ΤΕΙ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ
ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Πλήρης Οδηγός Εγκατάστασης και Παραμετροποίησης ενός Linux Server, για την υποστήριξη και παροχή με ασφάλεια υπηρεσιών WEB (Apache, PHP, MySQL, FTP, SMTP/POP)

Complete Guide of Linux Server Installation and Configuration, for the support and with safety provision of WEB services (Apache, PHP, MySQL, FTP, SMTP/POP)

Σπουδαστής: Γεωργόπουλος Νικόλαος

Εποπτεύων καθηγητής: Χόχολης Διονύσιος

Αμαλιάδα, Μάιος 2012

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Είναι αλήθεια ότι λόγω της πρωτοφανούς άνθησης του τομέα τεχνολογιών πληροφορίας που βιώνουμε τα τελευταία χρόνια, πλέον μας προσφέρεται απλόχερα η δυνατότητα πρόσβασης σε σχεδόν οποιαδήποτε πληροφορία, από σχεδόν οπουδήποτε στον κόσμο, με σχεδόν οποιαδήποτε συσκευή. Για να είναι υλοποιήσιμο αυτό, έχουν δημιουργηθεί νέες, διαδικτυακές εφαρμογές (web-based), οι οποίες σταδιακά αντικαθιστούν τις αντίστοιχες παραδοσιακές (desktop). Οι εφαρμογές αυτές βασίζονται στο μοντέλο πελάτη – εξυπηρετητή (client – server) και έτσι ο χρήστης δεν απαιτείται να είναι εφοδιασμένος με εξειδικευμένο υλικό ή/και λογισμικό, αφού όλος ο φόρτος εργασίας επιβαρύνει τον εξυπηρετητή. Συνεπώς, οι απαιτήσεις των διαδικτυακών εξυπηρετητών είναι ιδιαίτερα υψηλές και εξειδικευμένες, που όμως δεν έχουν καταφέρει να ανακόψουν την εξάπλωσή τους. Έτσι, τα συγκεκριμένα πληροφοριακά συστήματα πλέον χρησιμοποιούνται ευρέως, για να καλύψουν όχι μόνο τις ανάγκες μεγάλων, δύσκαμπτων οργανισμών και επιχειρήσεων, αλλά και αυτές των απλών, «οικιακών» χρηστών διαδικτυακών εφαρμογών.

Παράλληλα με την άνθηση των διαδικτυακών εφαρμογών, το λογισμικό ανοιχτού κώδικα φαίνεται να κερδίζει συνεχώς έδαφος απέναντι στο αντίστοιχο εμπορικό. Τέτοιου είδους λογισμικό έχει πλέον αναπτυχθεί και είναι διαθέσιμο για σχεδόν όλες τις κατηγορίες πληροφοριακών συστημάτων, μεταξύ των οποίων και ο τομέας των εξυπηρετητών διαδικτύου. Έτσι, οι υπεύθυνοι των τελευταίων έχουν επιτέλους στα χέρια τους μεγαλύτερη ελευθερία, περισσότερες δυνατότητες, με ελάχιστο ή ακόμα και μηδενικό κόστος απόκτησης και χρήσης. Ωστόσο, η υιοθέτηση ελεύθερου λογισμικού ορισμένες φορές οδηγεί σε περιορισμένη πρόσβαση σε βιβλιογραφία ή/και σε δυνατότητα εκπαίδευσης των χρηστών (για παράδειγμα υπάρχουν αμέτρητα βοηθήματα και σημεία εκπαίδευσης για την εμπορική σουίτα εφαρμογών γραφείου «Microsoft Office», ενώ ελάχιστα για την ελεύθερου λογισμικού «Libre Office»). Επιπροσθέτως, ορισμένες προσωποποιημένες εγκαταστάσεις και παραμετροποιήσεις ανοιχτού λογισμικού μπορεί να εξελιχθούν μη ομαλά, λόγω της έλλειψης πλήρους συμβατότητας μεταξύ των πακέτων που έχουν επιλεγεί για να αντιμετωπιστούν οι ιδιαιτερότητες της εκάστοτε περίστασης.

Παρά τις όποιες αντιξοότητες, η υφιστάμενη κατάσταση αποτελεί πρόκληση για πολλούς υπευθύνους πληροφοριακών συστημάτων υποστήριξης και παροχής υπηρεσιών

διαδικτύου και έτσι δεν είναι λίγες οι περιπτώσεις στις οποίες οι τελευταίοι στρέφονται σε υιοθετήσεις διαδικτυακών εξυπηρετητών χαμηλού κόστους, των οποίων οι εγκαταστάσεις και παραμετροποιήσεις βασίζονται εξ' ολοκλήρου σε ελεύθερο λογισμικό / λογισμικό ανοιχτού κώδικα. Η σχετική βιβλιογραφία, όπως αναφέρθηκε παραπάνω, είναι σαφώς περιορισμένη και οι λιγοστοί οδηγοί που έχουν αναρτηθεί σε διαδικτυακούς ιστοτόπους υπολείπονται κατάλληλης τεκμηρίωσης. Έτσι, λόγω της υψηλής εξειδίκευσης που απαιτείται, ο εκάστοτε υπεύθυνος εύλογα μπορεί να αισθανθεί αβεβαιότητα για τη λειτουργικότητα, αλλά κυρίως για την ασφάλεια του συστήματος.

Συνεισφέροντας στην κάλυψη του υφιστάμενου βιβλιογραφικού κενού, η παρούσα πτυχιακή εργασία επιδιώκει να αποτελέσει ένα σχετικό βοήθημα άμεσης αναφοράς στα χέρια όλων αυτών των υπευθύνων εγκατάστασης, παραμετροποίησης, αλλά και διαχείρισης των συγκεκριμένων πληροφοριακών συστημάτων. Αναλυτικότερα, η παρούσα εργασία στοχεύει:

- να απαντήσει, με την κατάλληλη επιχειρηματολογία, σε ερωτήματα που εγείρονται αναφορικά με την επιλογή του κατάλληλου λειτουργικού συστήματος, του λογισμικού που απαιτείται για την παροχή των υπηρεσιών διαδικτύου, καθώς και αυτού που θα πρέπει να χρησιμοποιηθεί για την εποπτεία και διαχείριση του διαδικτυακού εξυπηρετητή

- να παρουσιάσει μέσα από έναν βήμα προς βήμα περιγραφικό, αναλυτικό, αλλά πρωτίστως τεκμηριωμένο οδηγό τη διαδικασία εγκατάστασης καθώς και παραμετροποίησης όλου του εμπλεκόμενου λογισμικού που αναφέρθηκε παραπάνω

- να παραθέσει αδιάλειπτες παραπομπές σε σχετική «βιβλιογραφία», αξιοποιώντας, λόγω της απουσίας έντυπης τεκμηρίωσης, σχετικές αναφορές σε διαδικτυακούς πόρους, ώστε να είναι σε κάθε βήμα του οδηγού εύκολη και γρήγορη η άντληση επιπλέον πληροφοριών

- να μεριμνήσει σε όλα τα στάδια της διαδικασίας για τη διατήρηση της ασφάλειας του συστήματος στο υψηλότερο δυνατό επίπεδο

ABSTRACT

It is true that, due to the unprecedented boom in information technology that we have experienced in recent years, we are being generously offered the ability to access almost any information, from almost anywhere in the world, with almost any device. For that to be achievable, new web-based applications have been developed that are gradually replacing the traditional, desktop ones. These applications are based on the client - server model, hence the user does not need to be equipped with specialized hardware and / or software, since all the workload burdens only the server. Whilst the requirements of these servers are very demanding and specialized, they have failed to stem their spread. Thus, these information systems are now widely used to cover not only the needs of large, rigid organizations and businesses, but include those of simple, "home" users of web-based applications.

Along with the boom of web-based applications, open source software seems to be gaining ground against the proprietary one. Such software is now being developed and made available for almost all categories of information systems, including the area of the internet servers. Thus, internet server administrators finally have more freedom and options in their hands, with little or no cost of acquisition and use. However, the adoption of free software sometimes leads to poor access to bibliography and / or training for the end users (i.e. there are numerous books and training spots available for the commercial “Microsoft Office”, but only a few for the free “Libre Office” office suite). Furthermore, some customized installations and configurations of open source software may not develop smoothly, due to the lack of full compatibility between the packages that have been chosen to address the particular idiosyncrasies of each case.

Despite these setbacks, the current situation is a challenge for many administrators of information technology systems with regard to the support and provision of internet services and therefore, there are more than a few cases in which the latter turn to adopting low-cost internet servers, whose installations and configurations are based entirely on free and open source software. The relevant bibliography, as mentioned above, is clearly limited and the few guides that have been posted on internet sites fall short of adequate documentation. Thus, due to the high amount of specialization required, the administrator

of such a system may justifiably feel uncertain regarding the functionality and more importantly, the security of it.

In terms of contributing to filling the gap in the existing bibliography, this thesis seeks to provide a relevant direct reference document for all those administrators that are responsible for the installation, configuration, as well as the administration of these information systems. Specifically, this study aims:

- to answer, with the appropriate arguments, questions that are arise regarding the selection of the appropriate operating system and software required for the provision of the internet services, as well as the software that has to be used for the monitoring and administering of the internet server

- to present the installation and configuration process of all the software mentioned above, through a detailed step-by-step and exhaustively documented guide

- to present continual references to relevant "bibliography", using, in the absence of printed documentation, references to online resources, so that quick and easy access to additional information is supplied at each stage

- to ensure that the system’s security is maintained at the highest possible level at every stage of the process

ΕΙΣΑΓΩΓΗ

Στις αμέσως επόμενες, εισαγωγικές σελίδες της παρούσας εργασίας θα παρουσιαστούν παράμετροι, οι οποίες σήμερα περισσότερο από κάθε άλλη φορά καθιστούν απαραίτητη την υιοθέτηση των νέων τεχνολογιών πληροφορίας. Στη συνέχεια, αφού περιγραφούν οι νέες αυτές τεχνολογίες, θα δειχθεί η ανάγκη που πλέον υφίσταται για υιοθέτηση εξειδικευμένων πληροφοριακών συστημάτων, των εξυπηρετητών διαδικτύου. Ακολούθως, θα γίνει αναφορά και θα παρατεθεί σχετική σύγκριση των κατηγοριών λογισμικού που μπορεί να χρησιμοποιηθούν για την εγκατάσταση και παραμετροποίηση των εν λόγω συστημάτων. Τέλος, θα προσδιοριστούν οι στόχοι και το πλαίσιο της παρούσας πτυχιακής εργασίας.

Ηλεκτρονικό επιχειρείν

Σύμφωνα με την αναφορά «Το κατάστημα του μέλλοντος 2012-2015» [1], που προετοίμασε το Centre for Retail Research, ερευνώντας σε επτά ευρωπαϊκές χώρες για λογαριασμό της Visa Europe, μέχρι το 2012-15 περισσότεροι από το 71% των καταναλωτών είναι πιθανό να κάνουν έρευνα μέσω internet πριν προχωρήσουν σε αγορά προϊόντων, ενώ το 48% των εμπόρων αναμένεται να παρέχουν ηλεκτρονικές συσκευές για τους καταναλωτές στη μορφή ηλεκτρονικών περιπτέρων ή διαδραστικών υπολογιστών μέχρι το 2015.

Παράλληλα, η Cisco, που ειδικεύεται στον εξοπλισμό δικτύων, προβλέπει ότι μέχρι το 2015 ο συνολικός αριθμός των κάθε είδους μεγάλων και μικρών ηλεκτρονικών συσκευών, που θα είναι διασυνδεμένες στο διαδίκτυο, θα ξεπεράσει τα 15 δισεκατομμύρια (θα είναι δηλαδή κατά προσέγγιση διπλάσιος σε σχέση με τον πληθυσμό του πλανήτη).

Στη χώρα μας, σύμφωνα με έρευνα του τμήματος μελετών του «Παρατηρητηρίου για την Κοινωνία της Πληροφορίας» [2], το διαδίκτυο φαίνεται χρόνο με το χρόνο να μπαίνει σε ολοένα και περισσότερα σπίτια, έχοντας μάλιστα καλύψει σχεδόν το μισό του συνόλου (46%). Οι Έλληνες χρήστες του διαδικτύου προβαίνουν σήμερα σε ηλεκτρονικές συναλλαγές τάξης μεγέθους 1 δις ευρώ ετησίως και αυτό δε θα πρέπει να αφήσει αδιάφορο καμία σύγχρονη επιχείρηση, ανεξαρτήτως του μεγέθους αυτής.

Λόγω αυτής της αλματώδους επέκτασης του διαδικτύου, αλλά παράλληλα και των τεχνολογιών πληροφορίας, οι αποδέκτες των προϊόντων ή των υπηρεσιών μιας επιχείρησης που δραστηριοποιείται ηλεκτρονικά είναι πλέον σε θέση να έχουν πρόσβαση σε αυτή, όλες τις ώρες της ημέρας, όλες τις ημέρες του χρόνου, από οπουδήποτε στον κόσμο μπορούν να χρησιμοποιήσουν το διαδίκτυο. Μπορούν πλέον να εξυπηρετηθούν άμεσα μέσα από ένα «παράθυρο» συνομιλίας, οι πληρωμές να γίνουν σε απευθείας σύνδεση, τα προϊόντα να αποσταλούν, χωρίς αυτοί να χρειάζεται να μετακινηθούν από το χώρο στον οποίο βρίσκονται.

Οι καταναλωτές δεν είναι οι μόνοι ωφελημένοι από την υιοθέτηση των νέων τεχνολογιών. Οι συνεργάτες μιας τέτοιας επιχείρησης είναι σε θέση να ενημερώνονται με ιδιαίτερη ευκολία για τα νέα προϊόντα, τις τιμές ή τα χαρακτηριστικά αυτών, οποτεδήποτε, αλλά και από οπουδήποτε είναι σε θέση να αποκτήσουν πρόσβαση στο διαδίκτυο. Οι προμηθευτές είναι σε θέση να απολαμβάνουν νέες, βελτιωμένες παραγγελιοληψίες, οι οποίες μπορούν να γίνονται σε 24ωρη βάση, με άμεση ηλεκτρονική ενημέρωση για κάθε αλλαγή, με εξάλειψη των λαθών και των τηλεφωνικών διευθετήσεων στα οποία ήταν συνηθισμένοι μέχρι τώρα. Οι εργαζόμενοι είναι σε θέση να αποκτούν πρόσβαση σε όλα τα υποσυστήματα που καλύπτουν τους τομείς ενδιαφέροντός τους, από τη διαχείριση της αποθήκης (WHM), μέχρι και αυτή του πελατολογίου (CRM), για να ελέγξουν διεργασίες ή ακόμα και να προβούν σε ενέργειες, χωρίς να απαιτείται να βρίσκονται στο φυσικό χώρο της επιχείρησης.

Η ηλεκτρονική επέκταση της γεωγραφικής κάλυψης της επιχείρησης, καθώς και η βελτίωση των σχέσεών της με τους καταναλωτές, τους συνεργάτες και τους προμηθευτές αυτής, δεν οριοθετούν σε καμία περίπτωση τα οφέλη του ηλεκτρονικού επιχειρείν. Το ανταγωνιστικό πλεονέκτημα που προκύπτει από την απομάκρυνση όλων των χρονοβόρων, επισφαλών, απαρχαιωμένων διαδικασιών δεν είναι καθόλου ευκαταφρόνητο. Τα νέα πληροφοριακά συστήματα είναι αφενός απλά και εύκολα στη χρήση, αφετέρου προσφέρουν μεγάλη ταχύτητα στη διεκπεραίωση των λειτουργιών και καθιστούν εφικτή τη διαχείριση μεγάλου όγκου πληροφοριών, χωρίς λάθη ή καθυστερήσεις.

Με την υιοθέτηση των νέων τεχνολογιών πολλαπλασιάζονται άμεσα οι λειτουργικές, διοικητικές, αλλά και σχεδιαστικές δυνατότητες της επιχείρησης, έτσι ανεξαρτήτως του

μεγέθους της, αυτές αποτελούν μονόδρομο για οποιαδήποτε σύγχρονη επιχείρηση. Το ηλεκτρονικό επιχειρείν αποτελεί όχι μόνο στρατηγική διέξοδο για την αντιμετώπιση της οικονομικής ύφεσης που βιώνουμε, αλλά επιτακτική ανάγκη για τη διασφάλιση της επιχειρησιακής βιωσιμότητας στο σύγχρονο επιχειρείν.

Διαδικτυακές εφαρμογές

Παρά την αλματώδη επέκταση του διαδικτύου και των τεχνολογιών πληροφορίας, η δυνατότητα εύκολης πρόσβασης στον Παγκόσμιο Ιστό δεν είναι από μόνη της ικανή να εξασφαλίσει πρόσβαση στα υποσυστήματα εποπτείας ή/και διαχείρισης, ή ηλεκτρονικού εμπορίου μιας επιχείρησης που δραστηριοποιείται ηλεκτρονικά. Οι παραδοσιακές, desktop εφαρμογές σε πολλές περιπτώσεις απαιτούν εξειδικευμένο υλικό ή/και λογισμικό και για το λόγο αυτό δυσχεραίνουν τη χρήση τους εκτός των φυσικών ορίων της επιχείρησης. Για να ξεπεραστεί αυτός ο περιορισμός, έχει ήδη ξεκινήσει η ανάπτυξη εφαρμογών νέας τεχνολογίας, οι οποίες καλούνται διαδικτυακές (web-based) και στηρίζουν τη λειτουργία τους στο μοντέλο πληροφοριακών συστημάτων πελάτη - διακομιστή [3]. Οι συγκεκριμένες εφαρμογές χωρίζονται σε δύο μέρη, την εφαρμογή πελάτη (client), η οποία δεν παρουσιάζει εξειδικευμένες απαιτήσεις, ώστε να μπορεί να εκτελείται σε σχεδόν οποιαδήποτε συσκευή περιλαμβάνει έναν απλό περιηγητή διαδικτύου και την εφαρμογή διακομιστή ή εξυπηρετητή (server), η οποία έχοντας το πλεονέκτημα του εξειδικευμένου υλικού και λογισμικού του εξυπηρετητή, στον οποίο εκτελείται, επωμίζεται όλο το βάρος της επεξεργασίας της πληροφορίας.

Τα πολλαπλά οφέλη των εν λόγω εφαρμογών δεν περιορίζονται στη δυνατότητα που προσφέρουν στους χρήστες να ελέγχουν, ενημερώνονται, εκτελούν διεργασίες απομακρυσμένα. Πέρα από το ότι δεν απαιτείται εξειδικευμένο υλικό ή/και λογισμικό, το οποίο θα πρέπει να έχει κάθε φορά μαζί του ο χρήστης της εφαρμογής, συνήθως δεν απαιτούνται ή/και χρεώνονται άδειες χρήσης για τον εκάστοτε χρήστη αυτής. Το τελευταίο διατηρεί το συνολικό κόστος σε πολύ χαμηλότερα επίπεδα σε σχέση με τις αντίστοιχες desktop εφαρμογές. Παράλληλα, δεν απαιτείται προσαρμογή των χρηστών, αφού οι νέες εφαρμογές εκτελούνται σε μια οικεία επιφάνεια διεπαφής, αυτή του φυλλομετρητή διαδικτύου. Τέλος, τα δεδομένα σε αυτές τις υλοποιήσεις παραμένουν σε ένα κεντρικό σύστημα, γεγονός που αυξάνει την ασφάλεια και διευκολύνει τις διαδικασίες λήψης αντιγράφων ασφαλείας.

Χρησιμοποιώντας τη συγκεκριμένη τεχνολογία, ο καταναλωτής έχει τη δυνατότητα να προβεί σε έλεγχο τιμών, σύγκριση χαρακτηριστικών και αγορά προϊόντων, μέσα από έναν απλό φυλλομετρητή, από οπουδήποτε μπορεί να έχει πρόσβαση στο διαδίκτυο, σε οποιαδήποτε στιγμή της ημέρας ή νύχτας το επιθυμεί. Την ίδια στιγμή, ο διευθυντής πωλήσεων είναι σε θέση να έχει εικόνα για τις πωλήσεις, από την ξαπλώστρα της παραλίας, μέσα από μια απλή στη χρήση εφαρμογή πελάτη που εκτελείται στον υπερφορητό του υπολογιστή. Ταυτόχρονα, ο υπεύθυνος του πληροφοριακού συστήματος δε χρειάζεται να ανησυχεί για την επικαιροποίηση των συγκεκριμένων εφαρμογών, καθώς και τη λήψη αντιγράφων ασφαλείας σε όλα τα σημεία πρόσβασης, αφού όλα αυτά είναι αναγκαίο να πραγματοποιηθούν μόνο στον εξυπηρετητή των σύγχρονων διαδικτυακών εφαρμογών.

Εξυπηρετητές διαδικτύου

Το επίκεντρο ενδιαφέροντος μιας υλοποίησης πελάτη - διακομιστή προφανώς απομακρύνεται από τη συσκευή που θα φιλοξενήσει την εφαρμογή πελάτη, αφού εκεί οι μόνες απαιτήσεις αφορούν σε μια πρόσβαση στο διαδίκτυο, καθώς και ένα σύγχρονο φυλλομετρητή αυτού. Εύλογα, όλο το βάρος της υλοποίησης πέφτει στο διακομιστή ή εξυπηρετητή, ο οποίος λόγω της προσβασιμότητας μέσω του διαδικτύου που προσφέρει, καλείται εξυπηρετητής διαδικτύου (web server ή internet server) [4].

Στην Αγγλική, έχει άτυπα επικρατήσει το να χρησιμοποιείται ο όρος web server για αναφορές στους εξυπηρετητές Παγκοσμίου Ιστού και ο όρος internet server για τους εκτεταμένους διαδικτυακούς εξυπηρετητές, οι οποίοι μπορεί να είναι ένα ή και περισσότερα από τα παρακάτω παραδείγματα:

- Παγκόσμιου Ιστού (World Wide Web server, ή web server)
- Ηλεκτρονικού ταχυδρομείου (mail server)
- Εφαρμογών (application server)
- Βάσεων δεδομένων (database server)
- Αντιγράφων ασφαλείας (backup server)
- Αρχείων (file server)
- Μεταφοράς αρχείων (FTP server)

- Διαμεσολαβητής (proxy server)
- Ονομάτων τομέα (DNS server)
- Εκτυπωτών (printer server)
- Φαξ (fax server)
- Ροών δεδομένων (streaming server)

Σε κάθε περίπτωση, ένας διαδικτυακός εξυπηρετητής θα πρέπει να είναι σε θέση να «απαντά» σε αιτήσεις πελατών, ο αριθμός των οποίων μπορεί να είναι μονοψήφιος, μπορεί όμως να φτάνει και τις αρκετές χιλιάδες ταυτόχρονες συνδέσεις. Με δεδομένες τέτοιου είδους αυξημένες απαιτήσεις, το υλικό ενός διαδικτυακού εξυπηρετητή θα πρέπει να είναι εξειδικευμένο και συνήθως περιλαμβάνει περισσότερους του ενός πολυπηρυνικούς και πολυνηματικούς επεξεργαστές (multi core, multi thread CPUs), γρήγορους και μεγάλης χωρητικότητας σκληρούς δίσκους σε συστοιχία (RAID), ταχύτατες μνήμες με δυνατότητα διόρθωσης σφαλμάτων (ECC RAM). Πλέον αυτών, ένας εξυπηρετητής διαδικτύου συνήθως συνοδεύεται από σύστημα διπλής τροφοδοσίας (dual power supply) και από συσκευή παροχής αδιάλειπτης ενέργειας (UPS), ώστε να διασφαλίζεται αυξημένη αξιοπιστία στις παρεχόμενες υπηρεσίες του. Στον τομέα του λογισμικού υπάρχει πληθώρα επιλογών, εμπορικού και μη λογισμικού, που καλύπτει ολόκληρο το φάσμα των απαιτήσεων, από το λειτουργικό σύστημα, μέχρι και τις εφαρμογές εξυπηρέτησης. Εκτεταμένη αναφορά σε όλο το εμπλεκόμενο λογισμικό θα γίνει στο επόμενο κεφάλαιο.

Η εγκατάσταση ενός διαδικτυακού εξυπηρετητή δεν είναι απαραίτητο να πραγματοποιηθεί στο φυσικό χώρο της επιχείρησης. Λόγω της παρεχόμενης δυνατότητας απομακρυσμένης πρόσβασης, μπορεί να επιλεγεί και να χρησιμοποιηθεί κάποιο κέντρο δεδομένων (data center) το οποίο να βρίσκεται χιλιάδες χιλιόμετρα μακριά. Έτσι, τα πλεονεκτήματα και μειονεκτήματα των δύο λύσεων στην εκάστοτε περίπτωση υλοποίησης είναι αυτά που θα καθορίσουν την απόφαση διατήρησης ή μη ενός ιδιόκτητου κέντρου δεδομένων εντός του φυσικού χώρου της επιχείρησης. Η δυνατότητα άμεσης επικοινωνίας των πληροφοριακών υποσυστημάτων με τους εξυπηρετητές, καθώς και το προσωπικό απόρρητο των πληροφοριών που θα συγκεντρώνονται σε αυτούς, είναι δύο από τα πλεονεκτήματα που μπορεί να ωθήσουν μια επιχείρηση, στο να υιοθετήσει το δικό της κέντρο δεδομένων. Σε αυτή την περίπτωση θα πρέπει εκτός από το υψηλό κόστος προμήθειας, εγκατάστασης και παραμετροποίησης των πληροφοριακών συστημάτων, να απασχοληθεί και το αντίστοιχο εξειδικευμένο προσωπικό που θα εποπτεύει και

διαχειρίζεται καθ’ όλο το 24ωρο το κέντρο δεδομένων και αυτό δεν είναι εφικτό σε όλες τις περιπτώσεις.

Ανεξάρτητα με τη γεωγραφική τοποθέτηση του εξυπηρετητή ή τη σύνθεση του υλικού και λογισμικού που έχει χρησιμοποιηθεί, η πρόσβαση σε αυτόν θα πρέπει να παρέχεται είτε φυσικά, είτε μέσω του δικτύου ή/και διαδικτύου, ώστε να είναι εφικτή η εποπτεία και διαχείριση του συστήματος από το επιλεγμένο προσωπικό. Σε κάθε περίπτωση, είναι αυτονόητο ότι η πρόσβαση θα πρέπει να απαιτεί έλεγχο των κατάλληλων διαπιστευτηρίων, ενώ παράλληλα θα πρέπει να διασφαλίζεται το ότι δεν υπάρχουν κενά ασφαλείας στο λογισμικό, ούτως ώστε ο εξυπηρετητής να είναι επαρκώς προστατευμένος απέναντι σε διαδικτυακές λογικές απειλές.

Ελεύθερο και ιδιοταγές λογισμικό

Το λογισμικό που θα επιλεγεί να χρησιμοποιηθεί στη διαδικασία εγκατάστασης ενός διαδικτυακού εξυπηρετητή αφορά στο λειτουργικό σύστημα, αλλά και στις εφαρμογές που θα εξασφαλίζουν αφενός τις παρεχόμενες υπηρεσίες, αφετέρου τη δυνατότητα εποπτείας και διαχείρισης του συστήματος. Ανεξάρτητα με την επιμέρους επιλογή του κάθε πακέτου λογισμικού που θα χρησιμοποιηθεί, θα πρέπει αρχικά να καθοριστεί εάν συνολικά θα γίνει χρήση ελεύθερου λογισμικού (ανοιχτού κώδικα), ή ιδιοταγούς λογισμικού (κλειστού κώδικα), μιας και η κάθε κατηγορία παρουσιάζει, λόγω της φύσης της, τα δικά της πλεονεκτήματα και μειονεκτήματα.

Με τον όρο λογισμικό ανοικτού κώδικα καλείται το λογισμικό, του οποίου ο πηγαίος κώδικας διατίθεται ελεύθερα σε όσους θέλουν να τον εξετάσουν, τροποποιήσουν ή/και χρησιμοποιήσουν σε άλλες εφαρμογές. Η ελευθερία αυτή καθορίζεται στην άδεια χρήσης που συνοδεύει την εκάστοτε διανομή και μπορεί να περιλαμβάνει τη δυνατότητα τροποποίησης για προσωπική χρήση (επίπεδο 1), αντιγραφής και διανομής (επίπεδο 2), ή ακόμα και αναδημοσίευσης μιας τροποποιημένης - βελτιωμένης έκδοσης (επίπεδο 3). Το λογισμικό ανοικτού κώδικα δε σημαίνει κατ’ ανάγκη δωρεάν, αλλά, σύμφωνα με τον ορισμό που του δίνει το Ίδρυμα Ελεύθερου Λογισμικού, ούτε και ελεύθερο λογισμικό [5, 6].

Αντίστοιχα, το λογισμικό κλειστού κώδικα είναι αυτό που διανέμεται με τη μορφή δυαδικών, εκτελέσιμων αρχείων, τα οποία έχουν προκύψει μετά από μεταγλώττιση του πηγαίου τους κώδικα και τα οποία συνοδεύονται από άδεια χρήσης που δεν παρέχει τη δυνατότητα πρόσβασης στον κώδικα δημιουργίας τους. Παρά το μυστικισμό, καθώς και το πνεύμα εμπορικότητας που διέπει το ιδιοταγές λογισμικό, υπάρχουν και περιπτώσεις στις οποίες αυτό διατίθεται δωρεάν στους τελικούς αποδέκτες (πχ Adobe Reader).

Στη συντριπτική πλειοψηφία των περιπτώσεων, το κλειστό λογισμικό αναπτύσσεται με βασικό στόχο την κάλυψη μιας αυστηρά καθορισμένης απαίτησης χρήσης. Έτσι, πληρώνοντας συνήθως αδρά, ο αποδέκτης του μπορεί πέρα από το φιλικό περιβάλλον διεπαφής και τη λειτουργικότητα του λογισμικού, να προσδοκεί σε μια καλή τεκμηρίωση και υποστήριξη αυτού μετά την πώληση. Στην περίπτωση που αυτό δε συμβεί, ή στην περίπτωση που το λογισμικό δεν ταιριάζει στο διαφημιζόμενο προφίλ του, υπάρχει η διανέμουσα εταιρία, καθώς και η εταιρία ανάπτυξής του, εναντίων των οποίων μπορούν να κινηθούν νομικές διαδικασίες.

Στην άλλη πλευρά, το ανοιχτό λογισμικό δημιουργείται κατά κανόνα για ιδία χρήση, απευθυνόμενο πρωτίστως στους ίδιους τους προγραμματιστές του. Μάλιστα, δεν είναι λίγες οι φορές που οι απλοί χρήστες το βρίσκουν πολύπλοκο και δύσχρηστο. Για να αντιμετωπιστεί αυτό, δεν είναι λίγες οι περιπτώσεις στις οποίες έχουν δημιουργηθεί εταιρίες διανομής του συγκεκριμένου τύπου λογισμικού, οι οποίες αφού τροποποιήσουν τον πηγαίο του κώδικα, είναι σε θέση να προσφέρουν ένα πιο φιλικό στο χρήστη αποτέλεσμα (ένα καλό παράδειγμα αποτελούν οι διάφορες εταιρίες διανομής του λειτουργικού συστήματος Linux). Αντίθετα με το ιδιοταγές, το ανοιχτό λογισμικό συνήθως διανέμεται χωρίς να παρέχεται εγγύηση καλής λειτουργίας, τεκμηρίωσης ή ακόμα και υποστήριξής του.

Είναι προφανές ότι τα πλεονεκτήματα και μειονεκτήματα της κάθε πλευράς έχουν τις ρίζες τους στον τρόπο με τον οποίο οι δύο κατηγορίες λογισμικού διαφέρουν μεταξύ τους και αφορούν σε τομείς, οι οποίοι θα επηρεαστούν άμεσα ή έμμεσα από την υιοθέτηση της μίας ή της άλλης λύσης. Οι εμπλεκόμενες παράμετροι θα πρέπει εξεταστούν αναλυτικά, ώστε να είναι εφικτή η επιλογή της βέλτιστης σε κάθε περίπτωση λύσης:

Κόστος Το ολικό κόστος ιδιοκτησίας (Total Cost of Ownership), ανεξαρτήτως της επιλεγμένης λύσης, αφορά σε επιμέρους κόστη που αφορούν στην προμήθεια, εγκατάσταση, παραμετροποίηση, συντήρηση του λογισμικού, καθώς και εκπαίδευση του προσωπικού που θα το χρησιμοποιήσει. Ειδικά για την περίπτωση του ιδιοταγούς λογισμικού, θα πρέπει στο συνολικό κόστος να συνυπολογιστεί και η ειδική χρέωση που συνήθως συνοδεύει τις άδειες χρήσης και η οποία εξαρτάται από τον αριθμό των πληροφοριακών συστημάτων όπου θα εγκατασταθεί το λογισμικό, ή ακόμη και τον αριθμό των χρηστών αυτού. Μελέτες περιπτώσεων καθώς και συγκρίσεις που έχουν γίνει, δείχνουν ότι σε κάθε περίπτωση το συνολικό κόστος υιοθέτησης ανοιχτού λογισμικού είναι σαφώς μικρότερο από το αντίστοιχο κόστος υιοθέτησης κλειστού λογισμικού [7, 8, 9].

Αξιοπιστία Εντελώς αυθαίρετα, έχει στο παρελθόν προσαφθεί στο ανοιχτό λογισμικό η κατηγορία του λιγότερο αξιόπιστου λογισμικού. Για να διαπιστώσουν εάν αυτό αληθεύει, εργαζόμενοι στη Zdnet (διακεκριμένος ιστοχώρος ενδιαφέροντος πληροφορικής και τεχνολογίας) πραγματοποίησαν σχετική δοκιμή, η οποία περιλάμβανε πληροφοριακά συστήματα ίδιου υλικού, στα οποία εγκατέστησαν είτε το «κλειστό» λειτουργικό σύστημα Windows, είτε διανομή του «ανοιχτού» Linux [10]. Τα υπό έλεγχο συστήματα παρέμειναν σε λειτουργία καθ' όλο το διάστημα της δοκιμής και χρησιμοποιήθηκαν παράλληλα, ως εξυπηρετητές διαδικτύου, αρχείων, και εκτύπωσης. Η δοκιμή διήρκησε 10 μήνες και στη διάρκεια αυτών τα Windows «κράσαραν» κατά μέσο όρο μια φορά κάθε 6 εβδομάδες, ενώ το Linux ποτέ! Δηλαδή, όχι μόνο δε μπορεί να χαρακτηριστεί το ανοιχτό λογισμικό λιγότερο αξιόπιστο από το αντίστοιχο κλειστό, τουναντίον υπάρχουν περιπτώσεις όπου αποδεικνύεται ακριβώς το αντίθετο. Ένα ακόμη παράδειγμα απαντάται στο χώρο των εξυπηρετητών Παγκοσμίου Ιστού, όπου οι απαιτήσεις σε υλικό και λογισμικό είναι εξειδικευμένες και υψηλές. Στο συγκεκριμένο χώρο, το λογισμικό εξυπηρέτησης Παγκοσμίου Ιστού «Apache», έχει καθιερωθεί απόλυτα εκτοπίζοντας κάθε άλλο ανταγωνιστή και αυτό οφείλεται σε πολύ μεγάλο ποσοστό στην ευρέως παραδεκτή αξιοπιστία του!

Αποδοτικότητα Συγκριτικές δοκιμές, καθώς και μελέτες περιπτώσεων που έχουν γίνει για το σκοπό αυτό, έδειξαν ότι η ταχύτητα και αποδοτικότητα πολλών εφαρμογών ανοιχτού κώδικα υπερτερούν σε σχέση με τις αντίστοιχες ιδιοταγούς λογισμικού [11, 12, 13]. Αυτό έχει αποδοθεί στον ποιοτικότερο κώδικα του ανοιχτού λογισμικού (ο κώδικας

είναι ανά πάσα στιγμή προσβάσιμος από οποιονδήποτε), καθώς και τη μεγαλύτερη δυνατότητα ευελιξίας που απολαμβάνει ο χρήστης αυτού.

Ασφάλεια Οι εταιρίες ανάπτυξης κλειστού λογισμικού, προσπαθώντας να διατηρήσουν αμείωτο το ενδιαφέρον του αγοραστικού κοινού, συχνά προβαίνουν σε αναβαθμίσεις, ή/και διανομή νέων εκδόσεων του λογισμικού τους, χωρίς αυτές να έχουν αποσφαλματωθεί πλήρως. Αυτό έχει ως αποτέλεσμα το να επηρεάζεται αρνητικά αφενός η λειτουργικότητα, αφετέρου η ασφάλεια των πληροφοριακών συστημάτων στα οποία εγκαθίσταται το συγκεκριμένο λογισμικό. Στην περίπτωση του ανοιχτού λογισμικού, επειδή ο κώδικας είναι προσβάσιμος από οποιονδήποτε, τα τυχόν σφάλματα εντοπίζονται και διορθώνονται σε μικρό χρονικό διάστημα, αλλά και με διαφάνεια. Τέλος, επειδή το ανοιχτό λογισμικό απευθύνεται πρωτίστως σε πεπειραμένους χρήστες, στη φάση της ανάπτυξής του η ασφάλεια τοποθετείται πριν από την άνεση ή την ευκολία χρήσης. Έτσι, τα πακέτα ανοιχτού λογισμικού αποδεικνύονται στη χρήση πιο ασφαλή από τα αντίστοιχα εμπορικά.

Επεκτασιμότητα Αντίθετα με το κλειστό, το ανοιχτό λογισμικό είναι πολύ πιο ευέλικτο στη χρήση, αφού εξ' ορισμού επιτρέπει την επεκτασιμότητα της λειτουργικότητάς του. Βέβαια, αυτό προϋποθέτει σχετικές τροποποιήσεις στον πηγαίο του κώδικα, ο οποίος όμως είναι ανά πάσα στιγμή διαθέσιμος στο χρήστη. Σταδιακά, η επιθυμία βελτιστοποίησης της δυνατότητας επέκτασης του πρωτογενούς κώδικα έχει οδηγήσει τους προγραμματιστές αυτής της κατηγορίας λογισμικού στο να αναπτύσσουν τις εφαρμογές τους με την αρχιτεκτονική αρθρωμάτων (modules), τα οποία είναι ξεχωριστές λειτουργικές μονάδες και διευκολύνουν την προσθήκη επιπλέον λειτουργιών μετά την ολοκλήρωση του αρχικού κώδικα. Έτσι, αντίθετα με το κλειστό λογισμικό, στην περίπτωση του ελεύθερου κώδικα, ο τελικός χρήστης είναι σε θέση να ζητήσει επεκτάσεις ή τροποποιήσεις, οποτεδήποτε και αν αυτό απαιτηθεί.

Είναι προφανές ότι το χαμηλό ή ακόμα και μηδενικό κόστος αρχικής απόκτησης δεν είναι το μόνο πλεονέκτημα του ανοιχτού λογισμικού απέναντι στο αντίστοιχο κλειστό. Ο χρήστης του ελεύθερου κώδικα μπορεί πλέον να απολαμβάνει ένα αξιόπιστο και αποδοτικό λογισμικό, χωρίς να χρειάζεται να ανησυχεί για την παρεχόμενη ασφάλεια, ή να αισθάνεται εγκλωβισμένος σε μια επιλογή που άμεσα ή έμμεσα δεν θα είναι ικανοποιητικά προσωποποιημένη στις δικές του απαιτήσεις. Μειονέκτημα ορισμένες φορές ίσως να

αποτελεί ο «απευθύνομαι σε έμπειρους χρήστες» χαρακτήρας του, σε συνδυασμό με τη συχνά περιορισμένη βιβλιογραφία, καθώς και την όχι και τόσο προσβάσιμη από όλους δυνατότητα εκπαίδευσης (τη στιγμή που στο χώρο του κλειστού λογισμικού, λόγω του αυστηρά ελεγχόμενου περιβάλλοντος ανάπτυξης και διάθεσής του, αλλά και του εμπορικού του προσανατολισμού, η βιβλιογραφία και εκπαίδευση είναι ως επί το πλείστον περισσότερο πολυμορφικές, αλλά και διαδεδομένες).

Πλαίσιο και στόχοι πτυχιακής

Η πλεονεκτική θέση του ανοιχτού λογισμικού, έχει ως αποτέλεσμα η διάδοση και χρήση του να αποτελεί μια ισχυρή τάση της εποχής μας. Καθημερινά, όλο και περισσότεροι ιδιώτες, επιχειρήσεις και Δημόσιοι Οργανισμοί παγκοσμίως απολαμβάνουν τα οφέλη των εφαρμογών ανοιχτού κώδικα. Η διαδεδομένη χρήση του ελεύθερου λογισμικού δυστυχώς δεν έχει καταφέρει να εξαλείψει το φαινόμενο της περιορισμένης σχετικής βιβλιογραφίας. Οι εξυπηρετητές διαδικτύου είναι ένας από του τομείς που έχουν επηρεαστεί από το φαινόμενο αυτό και έτσι, ενώ ο ενδιαφερόμενος είναι σε θέση να εντοπίσει περιστασιακές αναφορές ή συνοπτικούς ατεκμηρίωτους οδηγούς εγκατάστασης λογισμικού, δε μπορεί να έχει στη διάθεσή του ένα αναλυτικό και τεκμηριωμένο σύνολο.

Με στόχο τη συνεισφορά στην κάλυψη του εν λόγω κενού, η τρέχουσα πτυχιακή εργασία θα παρουσιάσει ένα αναλυτικό και τεκμηριωμένο οδηγό εγκατάστασης και παραμετροποίησης του λειτουργικού συστήματος, του λογισμικού παροχής των υπηρεσιών διαδικτύου, καθώς και του λογισμικού εποπτείας και διαχείρισης του εξυπηρετητή. Με στόχο την απόλαυση των πλεονεκτημάτων του ελεύθερου λογισμικού, για όλα τα αυτά θα χρησιμοποιηθεί αποκλειστικά και μόνο λογισμικό ανοιχτού κώδικα και με στόχο το να αποφευχθούν τυχόν προβλήματα κατά την εγκατάσταση, αλλά και τη χρήση, οι επιλογές του λογισμικού θα γίνουν με πρωταρχικό στόχο τη μέγιστη δυνατή συμβατότητα μεταξύ των εμπλεκομένων πακέτων.

Από όλα τα εμπλεκόμενα πακέτα, σημαντικότερο είναι ο πίνακας ελέγχου και διαχείρισης του εξυπηρετητή, το λογισμικό δηλαδή που θα χρησιμοποιείται από τον υπεύθυνο του συστήματος για την εποπτεία και διαχείριση του συστήματος. Το συγκεκριμένο λογισμικό είναι αυτό που θα αλληλεπιδρά με το λειτουργικό σύστημα, αλλά και με το λογισμικό παροχής των υπηρεσιών του εξυπηρετητή, μεταφέροντας κάθε φορά

είτε τις επιθυμίες του διαχειριστή προς το σύστημα, είτε τα μηνύματα του συστήματος προς το διαχειριστή. Επειδή η έκταση αλληλεπίδρασης μεταξύ του πίνακα ελέγχου του εξυπηρετητή, του λειτουργικού συστήματος, καθώς και όλων των άλλων εμπλεκομένων πακέτων λογισμικού είναι πάρα πολύ μεγάλη, είναι βέλτιστο το να χρησιμοποιηθεί ένας δοκιμασμένος συνδυασμός, ώστε να αποφευχθούν τυχόν προβλήματα ασυμβατοτήτων.

Μέσα από αυτή τη λογική, θα επιλεγεί αρχικά το λογισμικό εποπτείας και διαχείρισης του εξυπηρετητή και στη συνέχεια να χρησιμοποιηθεί το λειτουργικό σύστημα στο οποίο γίνεται η ανάπτυξη αυτού, ενώ, για τις παρεχόμενες υπηρεσίες του εξυπηρετητή θα χρησιμοποιηθούν τα πακέτα λογισμικού που έχουν επιλεγεί για το συγκεκριμένο σκοπό από την ομάδα ανάπτυξης του λογισμικού εποπτείας και διαχείρισης του εξυπηρετητή. Τέλος, συγκεκριμένες τεχνικές που θα χρησιμοποιηθούν για να μεγιστοποιήσουν την ασφάλεια του συστήματος, έχουν δοκιμαστεί σε συστήματα παραγωγής, λειτουργούν απροβλημάτιστα και προτείνονται ανεπιφύλακτα για παρεμφερείς χρήσεις.

Η τεκμηρίωση σε κάθε στάδιο του οδηγού της παρούσας εργασίας θα περιλαμβάνει την απαραίτητη επιχειρηματολογία για την εκάστοτε επιλογή, ενώ παράλληλα, θα παρουσιάζονται σχόλια, παραδείγματα και θα παραθέτονται παραπομπές στην σχετική βιβλιογραφία. Επειδή, όπως ήδη αναφέρθηκε, στο συγκεκριμένο τομέα η βιβλιογραφία είναι περιορισμένη, οι παραπομπές θα είναι μεν αδιάλειπτες, θα γίνονται ωστόσο κατά κύριο λόγο σε διαδικτυακούς πόρους.

Με στόχο το να είναι στο μέγιστο του εφικτού περιγραφικός ο οδηγός, τα βήματά του θα παρουσιαστούν μέσα από στιγμιότυπα οθόνης τα οποία θα λαμβάνονται κατά τη διάρκεια της διαδικασίας. Για να είναι δυνατή η λήψη τους, η εγκατάσταση και παραμετροποίηση του εμπλεκόμενου λογισμικού θα πραγματοποιηθεί σε εικονικό υπολογιστή, ο οποίος θα δημιουργηθεί για το συγκεκριμένο σκοπό στη σχετική εφαρμογή ελεύθερου λογισμικού VirtualBox [14]. Με στόχο το να τονιστούν οι μικρότερες απαιτήσεις που υπάρχουν σε υλικό σχετικά με αντίστοιχους εξυπηρετητές, οι οποίοι λειτουργούν με κλειστό λογισμικό της εταιρίας Microsoft, στον εικονικό υπολογιστή θα παρασχεθούν ένας επεξεργαστής (CPU), 512MB μνήμης RAM και δίσκος χωρητικότητας 32GB. Βέβαια, σε επιχειρησιακά συστήματα (production systems), οι απαιτήσεις αναμένεται να είναι κάθε φορά διαφορετικές και να εξαρτώνται αφενός από τις παρεχόμενες υπηρεσίες, αφετέρου από τον αριθμό των χρηστών τους.

Ο οδηγός της παρούσας πτυχιακής εργασίας μπορεί να έχει εφαρμογή σε οποιαδήποτε επιχείρηση δραστηριοποιείται ηλεκτρονικά και παρέχει υπηρεσίες διαδικτύου, αποτελώντας ένα σημείο αναφοράς σχετικά με την εγκατάσταση, παραμετροποίηση, αλλά και διαχείριση του εξυπηρετητή των υπηρεσιών αυτών. Στο τμήμα Εφαρμογών Πληροφορικής στη Διοίκηση και Οικονομία της Σχολής Διοίκησης και Οικονομίας του ΑΤΕΙ Πάτρας, αλλά και κάθε άλλη παρόμοια σχολή τριτοβάθμιας (και όχι μόνο) εκπαίδευσης, ο οδηγός μπορεί να χρησιμοποιηθεί ως βοήθημα εγκατάστασης, παραμετροποίηση και διαχείρισης ενός εξυπηρετητή διαδικτύου, ο οποίος μπορεί να φιλοξενεί την ιστοσελίδα της σχολής, τη βάση δεδομένων των σπουδαστών, εκπαιδευτικών, προσωπικού γραμματειακής υποστήριξης και την εφαρμογή διαχείρισης αυτής, τον εξυπηρετητή ηλεκτρονικού ταχυδρομείου όλων των παραπάνω, τον εξυπηρετητή μεταφοράς αρχείων (FTP), κτλ.

Σε κάθε περίπτωση χρήσης του οδηγού είναι σημαντικό να λαμβάνεται υπόψη ότι νεότερες εκδόσεις των πακέτων του λογισμικού (από αυτές που έχουν χρησιμοποιηθεί στην παρούσα εργασία), μπορεί αφενός να παρουσιάζουν διαφοροποιήσεις στη διαδικασία εγκατάστασης και παραμετροποίησής τους, αφετέρου να παρουσιάσουν ασυμβατότητες με το υπόλοιπο λογισμικό.

ΚΕΦΑΛΑΙΟ 1

Στο παρών κεφάλαιο θα γίνει αναφορά στους πίνακες ελέγχου και διαχείρισης εξυπηρετητών διαδικτύου. Αφού αναλυθεί η φύση του συγκεκριμένου λογισμικού, θα παρουσιαστούν όλα τα σχετικά πακέτα λογισμικού που είναι υποψήφια για χρήση στον οδηγό της παρούσας εργασίας. Κατά τη διάρκεια της παρουσίασης, θα γίνεται σταδιακή απομάκρυνση όσων πακέτων δεν πληρούν βασικά κριτήρια υιοθέτησής τους, τα οποία και θα παρατίθενται σε κάθε βήμα της παρουσίασης. Τελικώς, θα πραγματοποιηθεί η επιλογή του βέλτιστου πακέτου και θα γίνει ανάλυση των όσων συμπαρασύρονται από τη συγκριμένη επιλογή, αναφορικά με το λειτουργικό σύστημα, καθώς και το λογισμικό παροχής των υπηρεσιών του εξυπηρετητή.

Λογισμικό ελέγχου - διαχείρισης εξυπηρετητών διαδικτύου

Η εποπτεία και διαχείριση ενός εξυπηρετητή διαδικτύου είναι μια πολύπλοκη διαδικασία, η οποία απαιτεί αφενός υψηλά εξειδικευμένο προσωπικό, αφετέρου χρονοβόρες και επισφαλείς διεργασίες. Με στόχο την απλοποίηση αυτής την επίπονης διαδικασίας έχουν πλέον σχεδιαστεί και αναπτυχθεί εφαρμογές, οι οποίες παρέχουν ένα κεντρικό πίνακα διαχείρισης, από όπου είναι εφικτή η εύκολη εποπτεία και ρύθμιση των υπηρεσιών που παρέχονται από τους εν λόγω εξυπηρετητές (web hosting control panels) [15]. Οι συγκεκριμένες εφαρμογές είναι διαδικτυακές, έχουν γραφικό περιβάλλον διεπαφής και έχουν υλοποιηθεί ούτως ώστε να παρέχουν αυτοματοποίηση των διαδικασιών ελέγχου και διαχείρισης των εξυπηρετητών διαδικτύου. Μερικές από τις πιο συνηθισμένες δυνατότητες που παρέχονται μέσω του λογισμικού αυτού στους υπεύθυνους των συγκεκριμένων συστημάτων είναι οι παρακάτω:

- Πρόσβαση στα αρχεία καταγραφής του εξυπηρετητή.
- Διαχείριση του διαθέσιμου και χρησιμοποιημένου χώρου αποθήκευσης, καθώς και του αντίστοιχου εύρους διαμεταγωγής (bandwidth) για τον κάθε χρήστη.
- Διαχείριση λογαριασμών ηλεκτρονικού ταχυδρομείου χρηστών.
- Διαχείριση λογαριασμών FTP χρηστών.
- Διαχείριση των βάσεων δεδομένων.

- Προβολή στατιστικών επισκεπτών με χρήση λογισμικού web log analysis.
- Δυνατότητα χρήσης διαδικτυακού περιηγητή αρχείων.

Σύγκριση πινάκων ελέγχου, επιλογή βέλτιστης λύσης

Σύμφωνα με σχετική ιστοσελίδα παρουσίασης των υπαρχόντων πινάκων ελέγχου εξυπηρετητών διαδικτύου της Wikipedia [16], οι διαθέσιμες επιλογές είναι οι παρακάτω:

Control panel	Άδεια χρήσης	Δωρεάν	Ανοιχτού κώδικα	Τελευταία έκδοση	BSD	Linux	Windows
Baifox	GPL	√	√	04/2009	X	√	X
cPanel	Proprietary	X	X	09/2011	√	√	Μερικώς
DirectAdmin	Proprietary	X	X	09/2011	√	√	X
Domain Technologie Control	GNU LGPL	√	√	09/2010	Μερικώς	√	X
Gnupanel	GPL	√	√	12/2009	X	√	X
H-Sphere	Proprietary	X	X	05/2011	√	√	√
HDE Controller X	Proprietary	X	X	11/2011	X	√	X
Hosting Controller	Proprietary	X	X	09/2011	X	√	√
i-MSCP	GPL	√	√	10/2011	X	√	X
InterWorx	Proprietary	X	X	11/2011	X	√	X
ISPConfig	BSD	√	√	11/2011	X	√	X
ispCP	GPL	√	√	11/2010	√	√	X
Kloxo (πρώην Lxadmin)	AGPL	√	√	11/2011	X	√	X
OpenPanel	GPL, Plugin API LGPL	√	√	07/2011	Σχεδιάζεται	√	Σχεδιάζεται
Plesk	Proprietary	X	X	07/2011	√	√	√
SysCP	GPL	√	√	05/2010	√	√	X
Froxlor	GPL	√	√	10/2011	√	√	X
Usermin	BSD style	√	√	10/2011	√	√	X
Virtualmin	GPL	√	√	10/2011	√	√	X
Virtualmin Pro	Proprietary	X	X	10/2011	√	√	X
Webmin	BSD style	√	√	10/2011	√	√	Μερικώς

Στην παρούσα πτυχιακή εργασία θα χρησιμοποιηθεί αποκλειστικά και μόνο ελεύθερο λογισμικό / λογισμικό ανοιχτού κώδικα, συνεπώς, οι εμπορικές εφαρμογές θα πρέπει να αφαιρεθούν από τον παραπάνω πίνακα. Έτσι, προκύπτει η παρακάτω λίστα:

Control panel	Frontend	Backend	Υποστήριξη πολλών εξυπηρετητών
Baifox	PHP	PHP, SQLite	--
Domain Technologie Control	PHP	--	--
Gnupanel	PHP	PHP	--
i-MSCP	PHP	Perl	X
ISPConfig	PHP	PHP, MySQL	√
ispCP	PHP	Perl	X
Kloxo (πρώην Lxadmin)	PHP	PHP, MySQL	√
OpenPanel	C++, AJAX	Core: C++, Modules: Any	Σχεδιάζεται
SysCP	PHP	PHP, MySQL	X
Froxlor	PHP	PHP, MySQL	Μερικώς
Usermin	--	--	--
Virtualmin	Perl	Perl	Μερικώς
Webmin	Perl	Perl	√

Πλέον, όλες οι επιλογές της παραπάνω λίστας αφορούν σε ελεύθερο λογισμικό / λογισμικό ανοιχτού κώδικα, εντούτοις, ορισμένες μόνο από αυτές υποστηρίζουν τον ταυτόχρονο έλεγχο και διαχείριση περισσοτέρων του ενός εξυπηρετητή. Το συγκεκριμένο χαρακτηριστικό είναι μείζονος σημασίας, αφού παρέχει τη δυνατότητα κεντρικού ελέγχου υπηρεσιών που έχουν διαμοιραστεί σε περισσότερα από ένα συστήματα, ώστε να ελαχιστοποιείται ο φόρτος αυτών. Επειδή δεν υπάρχουν αρνητικές επιπτώσεις από την υιοθέτηση μιας επιλογής που να παρέχει τη συγκεκριμένη δυνατότητα, μπορεί να χρησιμοποιηθεί αρχικά ένας τέτοιου είδους πίνακας ελέγχου και να παραμετροποιηθεί για χρήση ενός και μόνο εξυπηρετητή. Μελλοντικά, όταν και εάν αυτό απαιτηθεί, μπορούν να γίνουν οι κατάλληλες τροποποιήσεις στην παραμετροποίηση του λογισμικού, ώστε να γίνει διαμοιρασμός των υπηρεσιών σε περισσότερα συστήματα. Η επιλογή θα πρέπει να γίνει, συνεπώς, μεταξύ των εφαρμογών ανοιχτού κώδικα, που υποστηρίζουν εγγενώς τη συγκεκριμένη δυνατότητα:

Control panel	ISPConfig	Kloxo	Webmin
Plugin Support	√	--	√
IPV6 Support	√	--	√

FTP	√	√	√
Anonymous FTP	√	√	√
Terminal	SSH	Java Applet	SSH, Java Applet
File HTTP	√	√	√
Antivirus	√	--	√
Antispam	√	Προαιρετικά	√
Forwarders	√	√	√
Mailbox quota	√	--	√
DomainKeys	√	--	X
Lighttpd	√	√	√
Apache	√	√	√
PureFTPd	√	√	√
Vsftp	√	--	√
ProFTPd	√	--	√
Dovecot	√	--	√
Courier	√	√	√
Exim	X	--	--
Sendmail	X	--	√
Postfix	√	--	√
PostgreSQL	√	--	√
MySQL	√	√	√
PHP	√	√	√
Perl	√	√	√
Python	√	√	√

Με την εφαρμογή Kloxo να στερείται εγγενούς υποστήριξης προσθέτων (plugin), νέας γενιάς διευθυνσιοδότησης διαδικτύου (IPv6), καθώς και δυνατότητας έλεγχου των μηνυμάτων ηλεκτρονικού ταχυδρομείου για κακόβουλο λογισμικό (antivirus), η τελική επιλογή θα πρέπει να γίνει μεταξύ των πινάκων ελέγχου εξυπηρετητή διαδικτύου ISPConfig και Webmin.

Η αναζήτηση του βέλτιστου μεταξύ των δύο συγκεκριμένων πακέτων λογισμικού έχει απασχολήσει χρήστες πινάκων ελέγχου και διαχείρισης εξυπηρετητών, έχει αναρτηθεί σε σχετικά φόρα στο διαδίκτυο και έχει λάβει απαντήσεις όπως οι παρακάτω:

- «ISPConfig is more user-friendly, i.e., you don't need Linux knowledge. And you have 4 levels of administration: admin, resellers, customers, and users.» [17]

- «With Webmin, you can administrate nearly everything on your server, but you don't have these 4 levels like in ISPConfig, and you must have knowledge about what you do. Webmin isn't a tool I'd give to an end-user.» [18]

- «Webmin is more a general purpose control panel. You can configure nearly every service with it, but you need to know exactly what you are doing and how things work on linux.» [18]

- «ISPConfig is focused on webhosting (webserver, mailserver, DNS, FTP) and is more user friendly and easier to handle when you don’t have that much Linux knowledge.» [18]

Είναι γεγονός, ότι και οι δύο πίνακες ελέγχου είναι εξαιρετικά δυνατά εργαλεία διαχείρισης εξυπηρετητών. Η εφαρμογή Webmin είναι ένας γενικότερος πίνακας ελέγχου, μέσω του οποίου μπορεί κανείς να διαχειριστεί σχεδόν όλες τις υπηρεσίες ενός εξυπηρετητή με λειτουργικό σύστημα Linux, θα πρέπει όμως να γνωρίζει τον τρόπο με τον οποίο αυτές είναι δομημένες στο συγκεκριμένο λειτουργικό. Για τις απαιτήσεις της παρούσας εργασίας, ο πίνακας ελέγχου ISPConfig φαίνεται να είναι η καταλληλότερη επιλογή, μιας και είναι αφενός προσαρμοσμένος στους εξυπηρετητές διαδικτύου, αφετέρου πιο φιλικός στο χρήστη (δεν προϋποθέτει εξειδικευμένες γνώσεις πάνω στο λειτουργικό σύστημα για τη διεκπεραίωση του ελέγχου και των ρυθμίσεων).

Έτσι, στην παρούσα πτυχιακή εργασία θα χρησιμοποιηθεί ο πίνακας ελέγχου ISPConfig στην πλέον πρόσφατη έκδοσή του, την v3.0.4 [19], μαζί με ότι αυτό συμπαρασύρει αναφορικά με το λειτουργικό σύστημα, καθώς και το λογισμικό παροχής των υπηρεσιών του εξυπηρετητή. Οι επιμέρους επιλογές για όλο αυτό το εμπλεκόμενο λογισμικό θα αναλυθούν στο αμέσως επόμενο βήμα.

Σύμφωνα με την ομάδα ανάπτυξης της έκδοσης 3 του πίνακα ελέγχου εξυπηρετητή ISPConfig, αυτός είναι συμβατός με τα παρακάτω λειτουργικά συστήματα [20]:

- Debian 5 και 6 (συνιστάται)
- Ubuntu 8.10 - 11.10 (συνιστάται)
- CentOS 5.2 - 6.2
- Fedora 10 και 12-15
- OpenSuSE 11.1 - 12.1

Τα δύο πρώτα (και μόνο) λειτουργικά συστήματα της παραπάνω λίστας είναι συνιστώμενα από τους δημιουργούς της εφαρμογής ISPConfig για χρήση με το συγκεκριμένο λογισμικό. Αυτό συμβαίνει αφενός επειδή και οι δύο επιλογές αφορούν στο ίδιο κατά βάση λογισμικό (το Ubuntu είναι Debian derivative, βασισμένο δηλαδή στον αρχικό κώδικα του Debian), αφετέρου επειδή η ανάπτυξη του συγκεκριμένου πίνακα ελέγχου πραγματοποιείται στο περιβάλλον του λειτουργικού συστήματος Debian (έτσι είναι εξασφαλισμένη η μέγιστη συμβατότητα και ομαλή αλληλεπίδραση μεταξύ όλου του εμπλεκόμενου λογισμικού). Συνεπώς, το λειτουργικό σύστημα που αποτελεί τη βέλτιστη επιλογή και που θα χρησιμοποιηθεί στην παρούσα εργασία είναι το Debian GNU/Linux στην πλέον πρόσφατη έκδοση, την έκδοση v6.0.4, ή αλλιώς «Squeeze» [21].

Το λειτουργικό σύστημα δεν είναι το μόνο που εξαρτάται από την επιλογή του πίνακα ελέγχου. Ο τελευταίος αλληλεπιδρά σε σημαντικό βαθμό έκτασης και με ένα μεγάλο αριθμό πακέτων λογισμικού, μέσω των οποίων επιτρέπει στον υπεύθυνο του συστήματος να πραγματοποιεί την εποπτεία και διαχείριση όλων των παρεχομένων υπηρεσιών. Συνεπώς, θα πρέπει εκτός από την επιλογή του λειτουργικού συστήματος, να πραγματοποιηθεί αντίστοιχη επιλογή και του συγκεκριμένου λογισμικού. Με στόχο το να επιτευχθεί και στο σημείο αυτό η μέγιστη δυνατή συμβατότητα μεταξύ του ISPConfig και των εφαρμογών παροχής των υπηρεσιών του εξυπηρετητή, θα χρησιμοποιηθεί για τις τελευταίες, το λογισμικό που έχει επιλεγεί από τους δημιουργούς του εν λόγω πίνακα ελέγχου. Αναλυτικά, θα χρησιμοποιηθούν οι παρακάτω εφαρμογές για τις αντίστοιχες βασικές υπηρεσίες:

- Παγκοσμίου ιστού: Apache
- Ηλεκτρονικού ταχυδρομείου: Postfix
- Βάσεων δεδομένων: MySQL
- Μεταφοράς αρχείων: PureFTPd
- Ονομάτων τομέα: BIND

Εκτός από τις παραπάνω εφαρμογές, στον οδηγό της παρούσας πτυχιακής εργασίας θα χρησιμοποιηθεί επιπλέον λογισμικό για την παροχή δευτερευουσών υπηρεσιών (πχ λογισμικό παροχής δυνατότητας πρόσβασης στο λογαριασμό ηλεκτρονικού ταχυδρομείου των χρηστών μέσω ενός περιηγητή διαδικτύου), ή για τη διασφάλιση υψηλότερου επιπέδου ασφαλείας του εξυπηρετητή (πχ λογισμικό ανίχνευσης rootkit). Σε κάθε περίπτωση θα επιδιωχθεί η χρήση λογισμικού που συνιστάται από την ομάδα ανάπτυξης του πίνακα ελέγχου ISPConfig, ή αυτό που έχει δοκιμαστεί σε επιχειρησιακά συστήματα (production systems), χωρίς να έχουν παρουσιαστεί προβλήματα. Σε κάθε περίπτωση, η επιλογή θα συνοδεύεται από την αντίστοιχη τεκμηρίωση.

ΚΕΦΑΛΑΙΟ 2

Με την ολοκλήρωση της επιλογής του λογισμικού που θα χρησιμοποιηθεί στον οδηγό της παρούσας πτυχιακής εργασίας, δεν απομένει παρά να ξεκινήσει η διαδικασία εγκατάστασης και παραμετροποίησης αυτού.

Στο πρώτο στάδιο της συγκεκριμένης διαδικασίας, θα πραγματοποιηθεί η εγκατάσταση του λειτουργικού συστήματος του εξυπηρετητή (Debian GNU/Linux), το οποίο είναι διαθέσιμο σε περισσότερες από μία διανομές. Έτσι, πριν από την έναρξη εγκατάστασης αυτού, θα γίνει αναφορά στις εν λόγω διανομές, καθώς και επιλογή της καταλληλότερης.

Στη συνέχεια, θα παρατεθεί η βασική κατηγοριοποίηση των πακέτων λογισμικού που συνοδεύουν το συγκεκριμένο λειτουργικό σύστημα και θα αναλυθούν οι πιθανοί τρόποι προσβασιμότητας που είναι δυνατό να παρασχεθούν στον υπεύθυνο για την εγκατάσταση, παραμετροποίηση, αλλά και τον έλεγχο και διαχείριση του εξυπηρετητή.

Τέλος, θα διενεργηθεί η εγκατάσταση των πλέον απαιτούμενων πακέτων λογισμικού που αφορούν στο βασικό λειτουργικό σύστημα, καθώς και την υπηρεσία ασφαλούς απομακρυσμένης σύνδεσης (SSH), ώστε να μπορεί στο επόμενο κεφάλαιο να συνεχιστεί η παραμετροποίηση του λειτουργικού συστήματος, αλλά και η εγκατάσταση και παραμετροποίηση όλου του υπόλοιπου λογισμικού με τη μέγιστη δυνατή ασφάλεια.

Το λειτουργικό σύστημα Debian GNU/Linux

Το Debian GNU/Linux, ή απλά Debian, προέκυψε από την «ένωση» μεμονωμένων ατόμων, τα οποία είχαν την κοινή επιθυμία να δημιουργήσουν ένα δωρεάν λειτουργικό σύστημα. Το Debian GNU/Linux αποτελείται από ένα βασικό τμήμα κώδικα, το οποίο καλείται πυρήνας (kernel) και εκτελεί τις βασικές διεργασίες του συστήματος (όπως η διανομή της μνήμης μεταξύ των εφαρμογών και του χρόνου μεταξύ των διεργασιών), καθώς και από αρκετές χιλιάδες άλλα πακέτα λογισμικού, τα οποία αφορούν σε λειτουργικές διεργασίες, καθώς και εφαρμογές ή βοηθήματα που απευθύνονται στους τελικούς χρήστες.

Οι τελευταίοι μπορούν να απολαύσουν το Debian GNU/Linux σε τρεις διανομές, τη **stable**, την **testing** και την **unstable** (ή sid). Η πρώτη είναι η διανομή που περιέχει τις πλέον πρόσφατες σταθερές εκδόσεις λογισμικού και απευθύνεται για χρήση στα επιχειρησιακά συστήματα (production systems). Η δεύτερη διανομή είναι αυτή που περιέχει πακέτα λογισμικού που έχουν μεν γίνει αποδεκτά, όμως δεν έχουν ενσωματωθεί ακόμη στην πρώτη διανομή και συστήνεται σε όσους επιθυμούν τα πλεονεκτήματα των πλέον πρόσφατων εκδόσεων του λογισμικού. Τέλος, η τρίτη διανομή είναι αυτή που περιέχει τα υπό ανάπτυξη, μερικές φορές ασταθή πακέτα λογισμικού και συνήθως χρησιμοποιείται από τους προγραμματιστές για τη δοκιμή του λογισμικού, καθώς και από όσους θέλουν να δουν τι επιφυλάσσει το μέλλον.

Πέρα από το ίδιο το λειτουργικό σύστημα, τα πακέτα λογισμικού που συνοδεύουν το Debian GNU/Linux είναι και αυτά χωρισμένα σε τρεις κατηγορίες, τη **free**, τη **non-free** και την **contrib**. Η πρώτη κατηγορία περιλαμβάνει τα πακέτα που αφορούν σε δωρεάν λογισμικό, η δεύτερη σε μη δωρεάν και η τρίτη σε δωρεάν λογισμικό που βασίζεται πάνω σε μη δωρεάν πακέτα.

Επειδή το πληροφοριακό σύστημα του εξυπηρετητή αφορά σε επιχειρησιακό σύστημα, το οποίο και θα πρέπει να παρέχει την απόλυτη σταθερότητα και αξιοπιστία, στον οδηγό της παρούσας εργασίας θα χρησιμοποιηθεί η διανομή stable του λειτουργικού συστήματος Debian GNU/Linux. Αντίστοιχα, με στόχο την παραμονή στο χώρο του δωρεάν λογισμικού, θα χρησιμοποιηθεί η κατηγορία free των υπολοίπων πακέτων λογισμικού που θα εγκατασταθούν στα προσεχή βήματα του οδηγού.

Πρόσβαση στον εξυπηρετητή διαδικτύου

Για να πραγματοποιηθεί η εγκατάσταση του λειτουργικού συστήματος Debian GNU/Linux στον εξυπηρετητή, είναι αυτονόητο ότι θα πρέπει να παρέχεται κάποιου είδους πρόσβαση σε αυτόν! Η πρόσβαση μπορεί να είναι είτε φυσική (όπως στην περίπτωση μιας επιχείρησης που διατηρεί το δικό της κέντρο δεδομένων), είτε απομακρυσμένη (όπως στην περίπτωση που το υλικό του εξυπηρετητή αφορά σε πραγματικό ή εικονικό υπολογιστή, που βρίσκεται σε εξειδικευμένο κέντρο δεδομένων, οπουδήποτε στην υφήλιο). Σε κάθε περίπτωση, ο εξυπηρετητής θα είναι, λόγω της φύσης

του, προσβάσιμος απομακρυσμένα. Έτσι, με εξαίρεση τη μικρή διαφοροποίηση στον τρόπο εκκίνησης της διαδικασίας εγκατάστασης, η τελευταία μπορεί να εκτελεστεί απομακρυσμένα, εφαρμόζοντας τον παρών οδηγό ανεξαρτήτως από τον τρόπο πρόσβασης στον εξυπηρετητή (κονσόλα, VNC, eSSI, RTB).

Επιλογή του τύπου εγκατάστασης

Για την εκτέλεση της διαδικασίας εγκατάστασης του λειτουργικού συστήματος προσφέρεται από την ομάδα ανάπτυξης του Debian GNU/Linux πληθώρα λύσεων, η οποία περιλαμβάνει εγκατάσταση με χρήση οπτικού δίσκου CD (ή DVD), μινιμαλιστική εγκατάσταση μέσω δικτύου, απομακρυσμένη εγκατάσταση μέσω περιηγητή διαδικτύου, «ζωντανές» (live) εκδόσεις της κάθε διανομής που επιτρέπουν δοκιμή του λογισμικού πάνω στο υλικό πριν από την εγκατάσταση κτλ. Στην παρούσα πτυχιακή εργασία, επιδιώκοντας τη χρήση των πλέον πρόσφατων και ενημερωμένων εκδόσεων όλων των εμπλεκομένων πακέτων, θα γίνει εκμετάλλευση της εξ' ορισμού δυνατότητας πρόσβασης του εξυπηρετητή στο διαδίκτυο και θα χρησιμοποιηθεί ο τύπος της μινιμαλιστικής εγκατάστασης δικτύου [22].

Στο συγκεκριμένο τύπο εγκατάστασης του Debian GNU/Linux χρησιμοποιείται ένας οπτικός δίσκος με το εντελώς απαραίτητο λογισμικό που απαιτείται ώστε να ξεκινήσει η διαδικασία εγκατάστασης και ακολούθως, όλα τα υπόλοιπα απαιτούμενα πακέτα μεταφορτώνονται σταδιακά από το διαδίκτυο. Έτσι, μετά την ολοκλήρωση της εγκατάστασης, το σύστημα θα είναι αυτομάτως, πλήρως επικαιροποιημένο. Αυτό που απομένει λοιπόν, πριν την έναρξη της διαδικασίας εγκατάστασης είναι το να τοποθετηθεί ο παραπάνω οπτικός δίσκος στον αντίστοιχο οδηγό και να οριστεί εκκίνηση του συστήματος από αυτόν.

Στην περίπτωση φυσικής πρόσβασης στο σύστημα, η εν λόγω διαδικασία περιλαμβάνει τη μεταφόρτωση του αρχείου που περιέχει την εικόνα του οπτικού δίσκου εγκατάστασης [23], την εγγραφή αυτής σε κενό οπτικό δίσκο, την τοποθέτηση του τελευταίου στον οδηγό του συστήματος και, τέλος, εκκίνηση αυτού από το συγκεκριμένο οδηγό. Στην περίπτωση απομακρυσμένης πρόσβασης, θα πρέπει να ενημερωθεί το προσωπικό του κέντρου δεδομένων για τη συγκεκριμένη απαίτηση, ώστε να προβεί εκείνο στην παραπάνω διαδικασία. Σε ορισμένες περιπτώσεις εικονικού υπολογιστή (Virtual

Private Server), παρέχεται η δυνατότητα εκκίνησης από τον εικονικό οδηγό οπτικού δίσκου του συστήματος, στον οποίο μπορεί να προσαρτηθεί η εικόνα του δίσκου εγκατάστασης, είτε μεταφορτώνοντας το σχετικό αρχείο, είτε εισάγοντας τον κατάλληλο σύνδεσμο στις σχετικές ρυθμίσεις.

Εγκατάσταση βασικού συστήματος

Μετά την εισαγωγή του οπτικού δίσκου στον αντίστοιχο οδηγό του συστήματος και ρύθμιση εκκίνησης του τελευταίου από αυτόν, αρκεί το να τεθεί το σύστημα σε λειτουργία και η διαδικασία εγκατάστασης θα ξεκινήσει αυτόματα, παρουσιάζοντας το στιγμιότυπο οθόνης που φαίνεται στο πρώτο βήμα του οδηγού που ακολουθεί. Εάν απαιτηθεί επιπλέον βοήθεια, σημείο αναφοράς σχετικά με την όλη διαδικασία μπορεί να αποτελέσει η Ελληνική μετάφραση του επίσημου οδηγού εγκατάστασης του λειτουργικού Debian GNU/Linux, η οποία είναι διαθέσιμη σε απλό κείμενο [24], αλλά και σε μορφή υπερκειμένου [25]. Τέλος, έχουν υπάρξει περιπτώσεις, στις οποίες παρουσιάστηκαν προβλήματα κατά τη διαδικασία εγκατάστασης και έτσι είναι διαθέσιμη μια λίστα με την περιγραφή, καθώς και τις οδηγίες επίλυσης των γνωστότερων από αυτά [26].

Σημείωση: Κάποιες από τις ρυθμίσεις που θα χρησιμοποιηθούν κατά τη διαδικασία εγκατάστασης του οδηγού της παρούσας πτυχιακής εργασίας βρίσκονται συγκεντρωτικά στην παρακάτω λίστα. Οι αντίστοιχες πραγματικές θα πρέπει να καθοριστούν από τον υπεύθυνο του εκάστοτε συστήματος σε συνεργασία με το προσωπικό του κέντρου δεδομένων στον οποίο έχει εγκατασταθεί ο εξυπηρετητής:

- Όνομα υπολογιστή: server
- Όνομα τομέα: mydomain.gr
- Διεύθυνση IP: 192.168.204.134
- Subnet mask: 255.255.255.0
- Gateway: 192.168.204.1

Βήμα 1: Επιλογή μορφής οδηγού εγκατάστασης

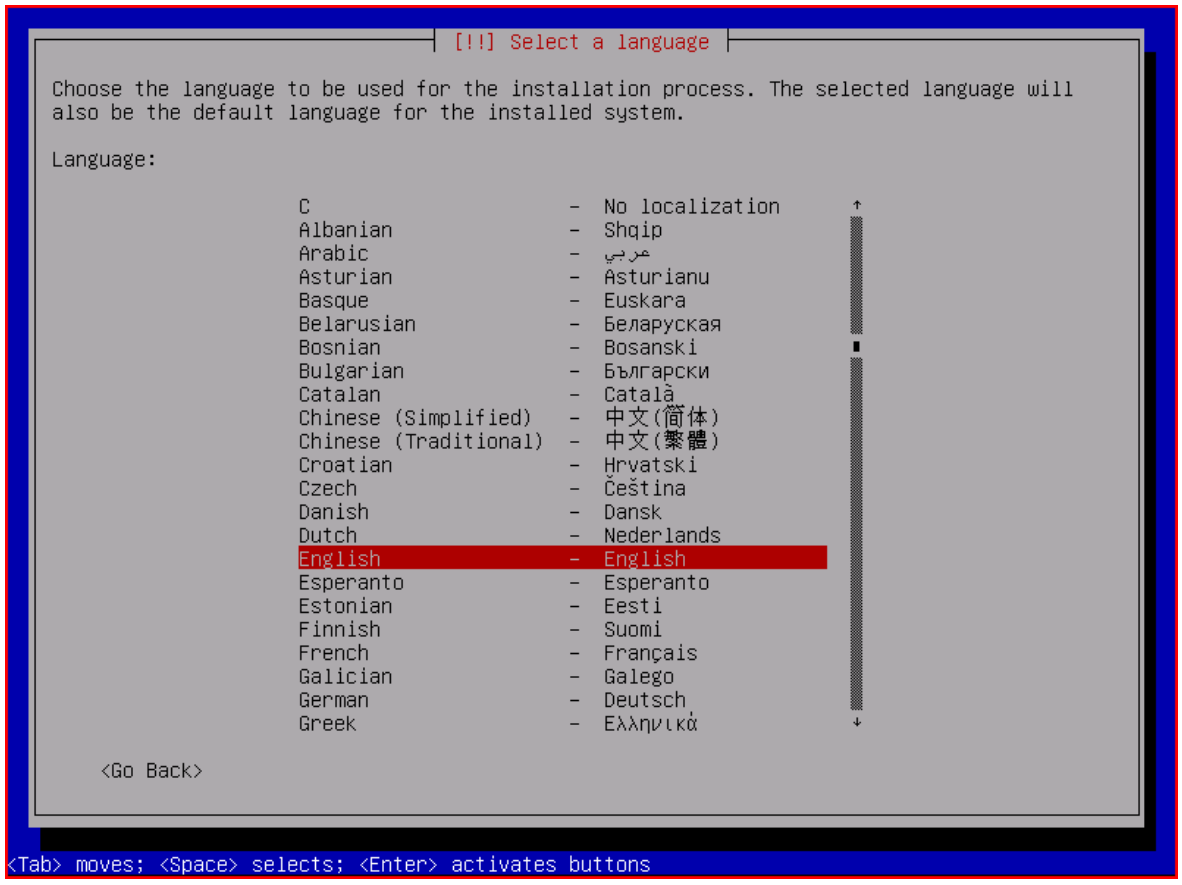
Πρώτο βήμα του οδηγού αποτελεί η διαδικασία επιλογής του τύπου εγκατάστασης. Οι δύο επιλογές είναι εγκατάσταση σε μορφή κειμένου και σε γραφικό περιβάλλον. Με στόχο την ελαχιστοποίηση του χρησιμοποιούμενου εύρους ζώνης δικτύου (bandwidth), στην παρούσα πτυχιακή εργασία θα χρησιμοποιηθεί ο οδηγός εγκατάστασης του Debian GNU/Linux στην πρώτη μορφή, τη μορφή απλού κειμένου (text mode).

Οδηγία: Επιλέγουμε «Install» για να εκκινήσουμε τον οδηγό εγκατάστασης σε μορφή κειμένου.

Βήμα 2: Επιλογή γλώσσας

Στο βήμα αυτό θα πρέπει να οριστεί η γλώσσα που θα χρησιμοποιηθεί στον οδηγό εγκατάστασης, η οποία όμως θα χρησιμοποιηθεί και για την αυτόματη ρύθμιση της προκαθορισμένης γλώσσας του συστήματος. Επειδή τα Ελληνικά είναι πιο πιθανό να δημιουργήσουν κάποιο πρόβλημα ασυμβατότητας από το να μας κάνουν να αισθανθούμε ότι εργαζόμαστε σε οικείο περιβάλλον, στο συγκεκριμένο βήμα θα επιλεγεί η Αγγλική γλώσσα.

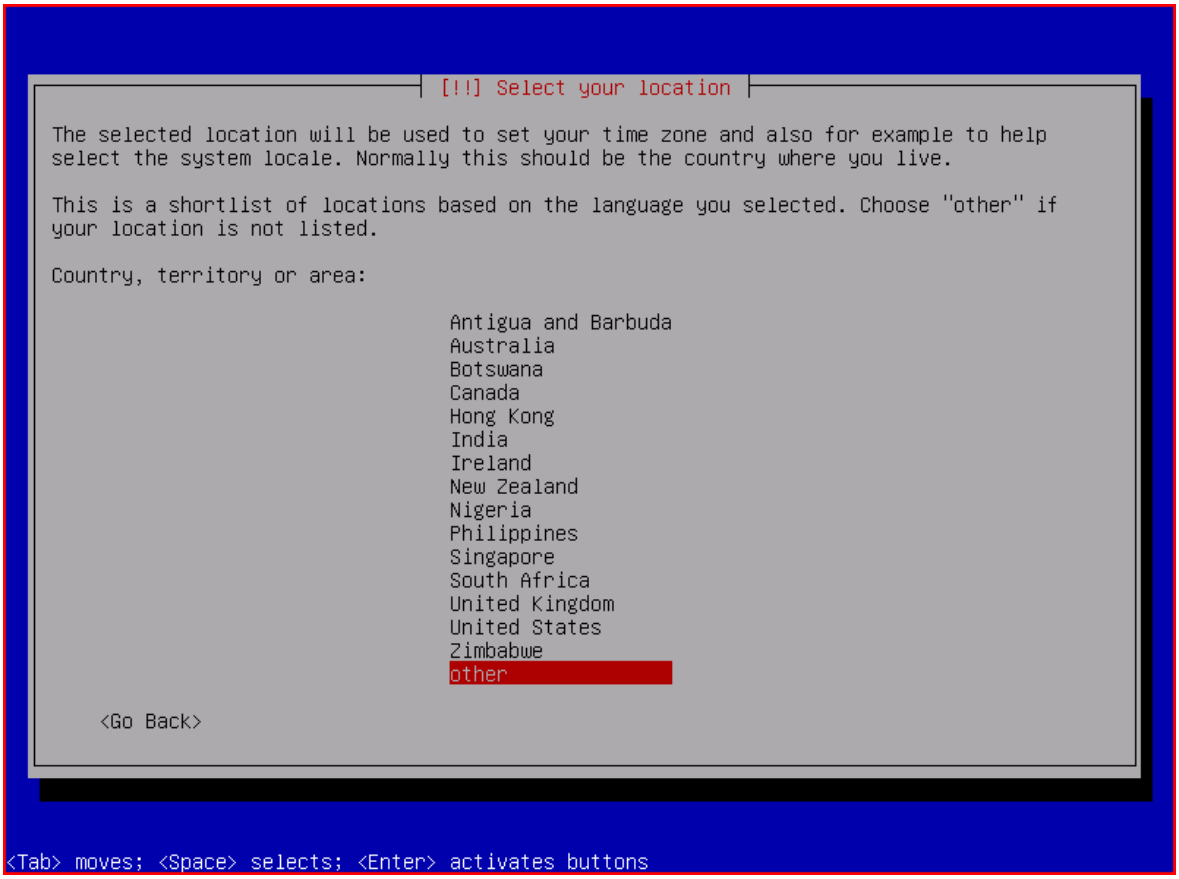
Οδηγία: Επιλέγουμε «English» για να εκτελέσουμε τον οδηγό εγκατάστασης στην Αγγλική γλώσσα, αλλά και να ορίσουμε αυτή εξ' ορισμού γλώσσα του συστήματος.

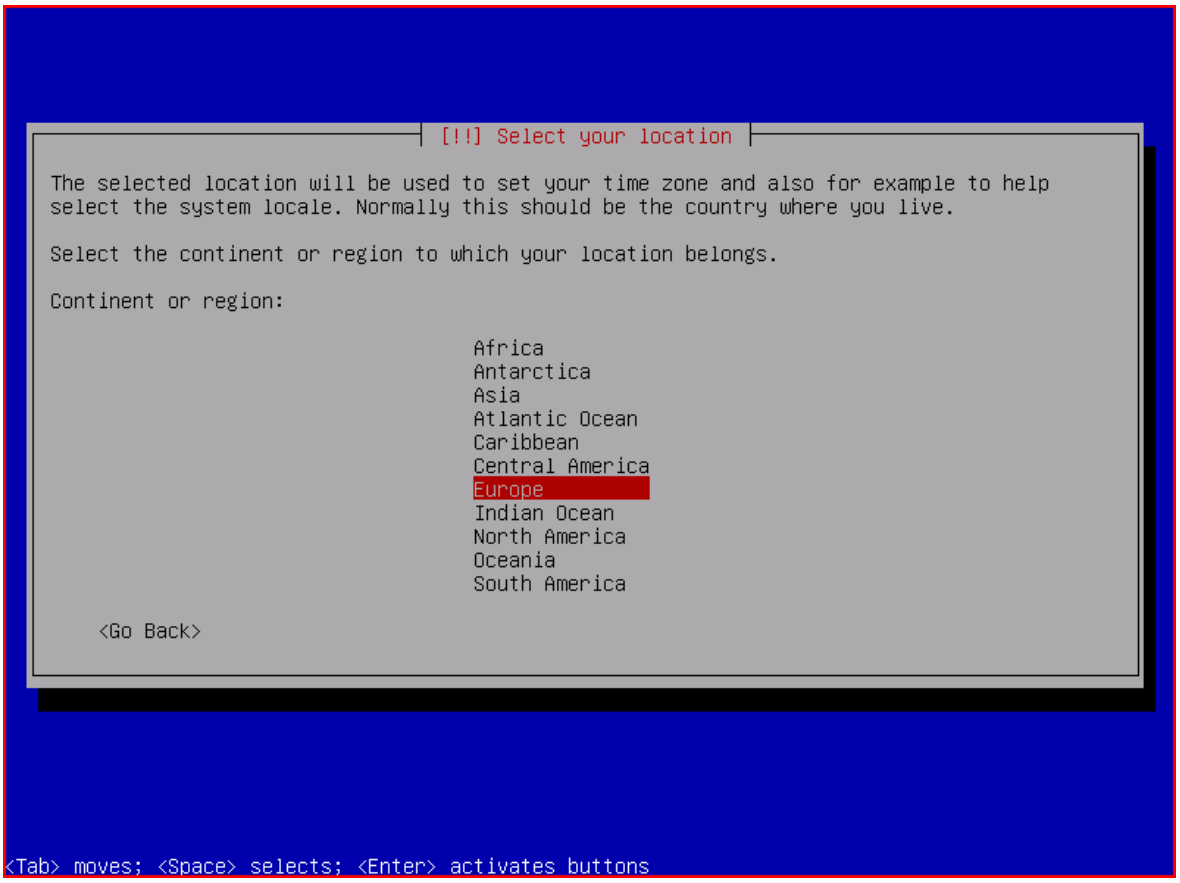


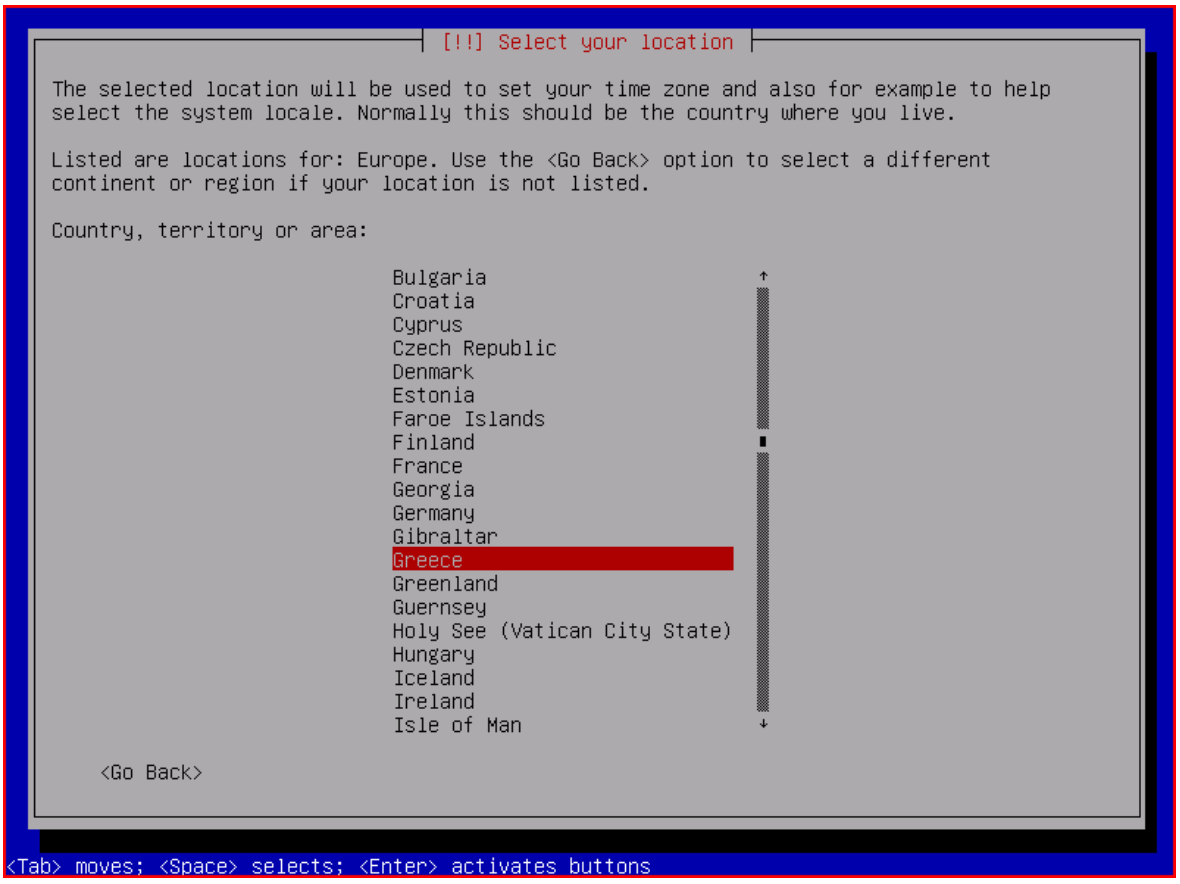
Βήμα 3: Επιλογή τοποθεσίας

Στο συγκεκριμένο βήμα θα πρέπει να οριστεί η γεωγραφική θέση (τοποθεσία) του εξυπηρετητή, η οποία και θα χρησιμοποιηθεί από τον οδηγό εγκατάστασης για τον καθορισμό της ζώνης ώρας και της παραμέτρου τοπικοποίησης του συστήματος. Η ζώνη ώρας του εξυπηρετητή είναι ιδιαίτερα σημαντική, επειδή σε επιλεγμένες ώρες, μη αιχμής, θα πραγματοποιούνται αυτοματοποιημένες διεργασίες συντήρησης του συστήματος. Η παράμετρος τοπικοποίησης συνήθως καθορίζεται αυτόματα από τον οδηγό εγκατάστασης βάσει της γλώσσας και της τοποθεσίας που έχουν επιλεγεί. Με τις αντίστοιχες όμως εισαγωγές που χρησιμοποιούνται στην παρούσα εργασία, αυτό δεν είναι εφικτό και έτσι, η συγκεκριμένη παράμετρος θα πρέπει να καθοριστεί χειρονακτικά στο αμέσως επόμενο βήμα.

Οδηγία: Επιλέγουμε διαδοχικά «other», «Europe» και «Greece», για να ορίσουμε ως τοποθεσία του συστήματος την Ελλάδα.



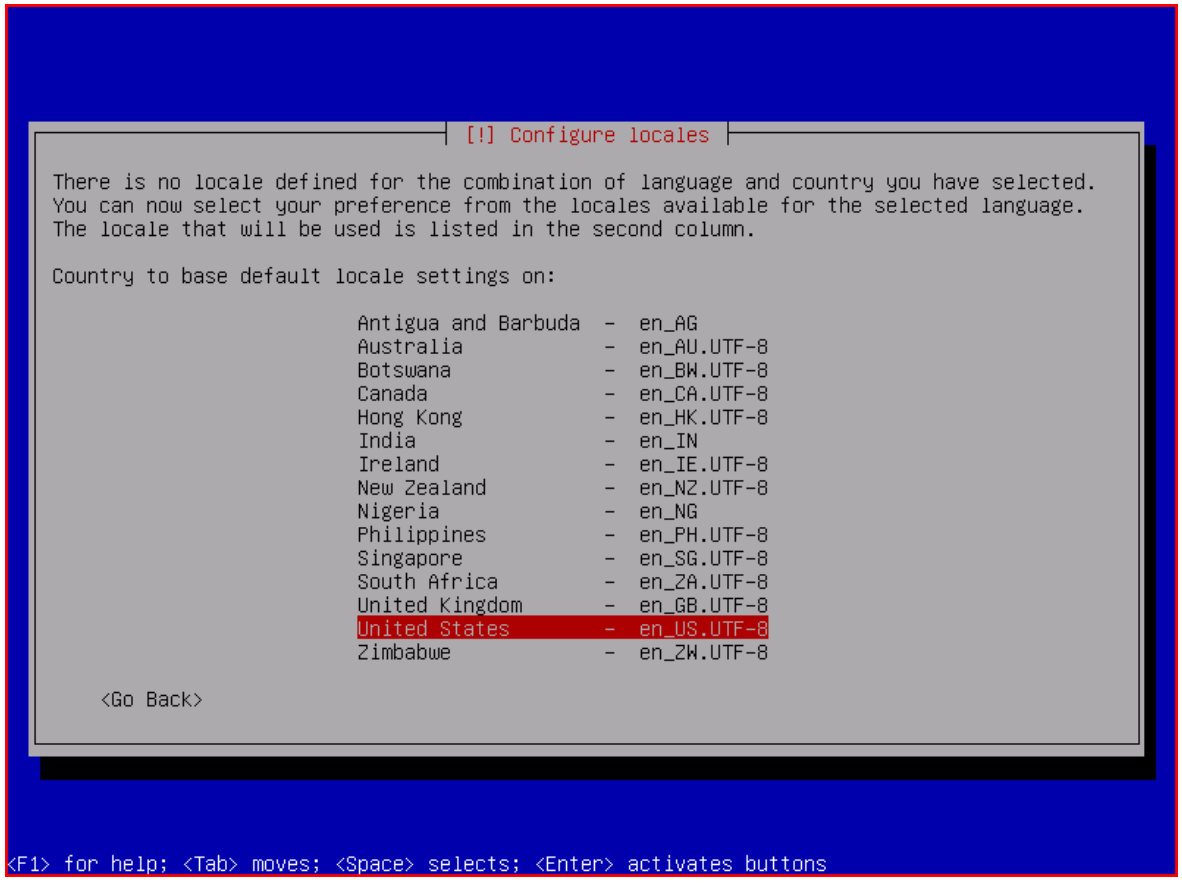

[!!] Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
Select the continent or region to which your location belongs.
Continent or region:
Africa
Antarctica
Asia
Atlantic Ocean
Caribbean
Central America
Europe
Indian Ocean
North America
Oceania
South America
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
Listed are locations for: Europe. Use the <Go Back> option to select a different continent or region if your location is not listed.
Country, territory or area:
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Faroe Islands
Finland
France
Georgia
Germany
Gibraltar
Greece
Greenland
Guernsey
Holy See (Vatican City State)
Hungary
Iceland
Ireland
Isle of Man
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

Βήμα 4: Ρύθμιση προκαθορισμένης παραμέτρου τοπικοποίησης

Η παράμετρος τοπικοποίησης (locale) είναι αυτή που καθορίζει κάποιες από τις τοπικές ρυθμίσεις του εγκατεστημένου συστήματος, όπως, για παράδειγμα, ο τρόπος εμφάνισης της ημερομηνίας και ώρας [27]. Στο Debian GNU/Linux υπάρχει η δυνατότητα καθορισμού περισσοτέρων της μιας παραμέτρου τοπικοποίησης, πάραυτα, μία και μόνο μπορεί να είναι η προκαθορισμένη παράμετρος τοπικοποίησης του συστήματος. Έτσι, με στόχο το να αποφευχθούν τυχόν ασυμβατότητες με το υπόλοιπο λογισμικό, που θα εγκατασταθεί αργότερα, θα χρησιμοποιηθεί ως προκαθορισμένη παράμετρος τοπικοποίησης η en_US.UTF-8.

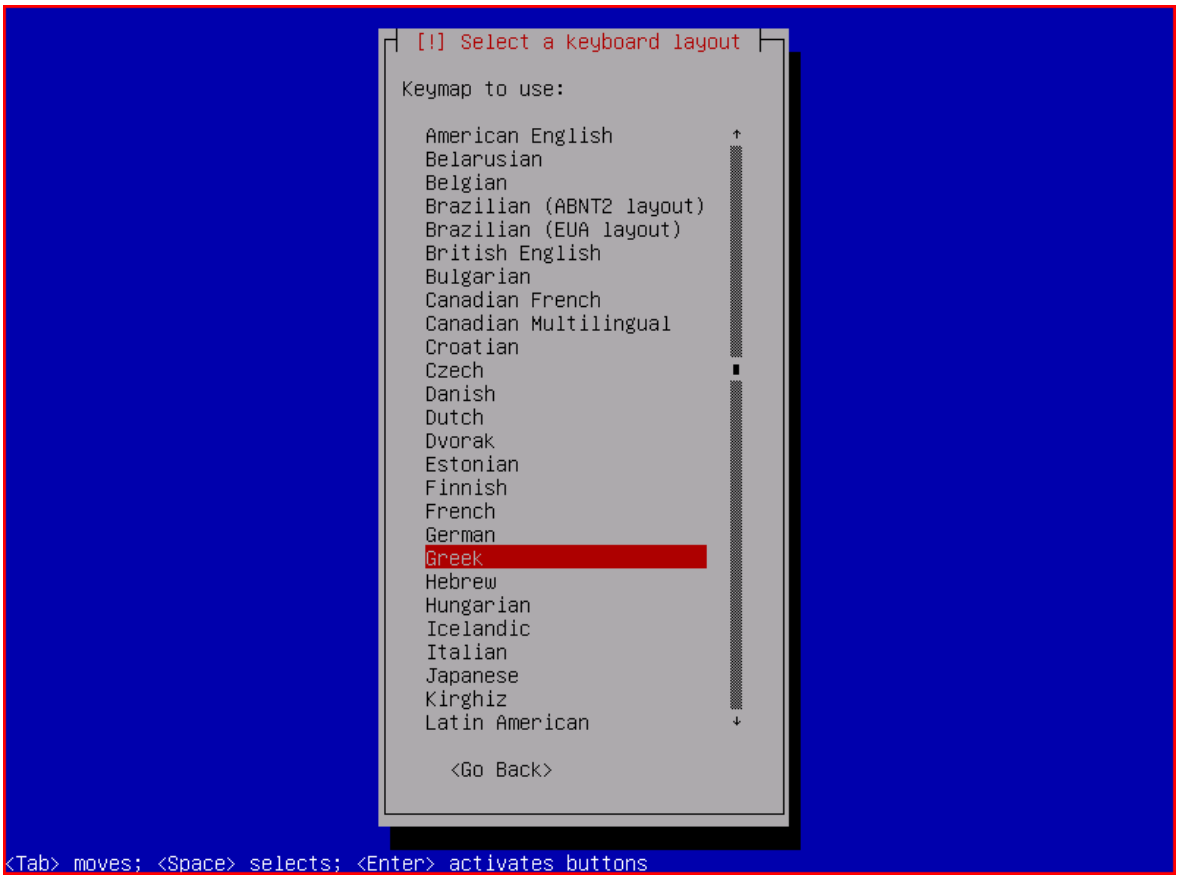
Οδηγία: Επιλέγουμε ως προκαθορισμένη παράμετρο τοπικοποίησης την «United States – en_US.UTF-8».



Βήμα 5: Επιλογή διάταξης πληκτρολογίου

Στο συγκεκριμένο βήμα θα πρέπει να επιλεγεί μια διάταξη που να ταιριάζει στο πληκτρολόγιο του συστήματος ή, εάν αυτό δεν είναι εφικτό, μια παραπλήσια με αυτή. Στο μεγαλύτερο ποσοστό των περιπτώσεων τα πληροφοριακά συστήματα που διατίθενται στην Ελληνική αγορά περιλαμβάνουν το τυπικό Ελληνικό πληκτρολόγιο και έτσι, η Ελληνική διάταξη πληκτρολογίου αποδεικνύεται ικανοποιητικότατη επιλογή. Σε διαφορετική περίπτωση θα πρέπει να επανακαθοριστεί η συγκεκριμένη παράμετρος μετά το πέρας της εγκατάστασης, όπου θα υπάρχει η δυνατότητα επιλογής από ένα σαφώς μεγαλύτερο εύρος διατάξεων πληκτρολογίου.

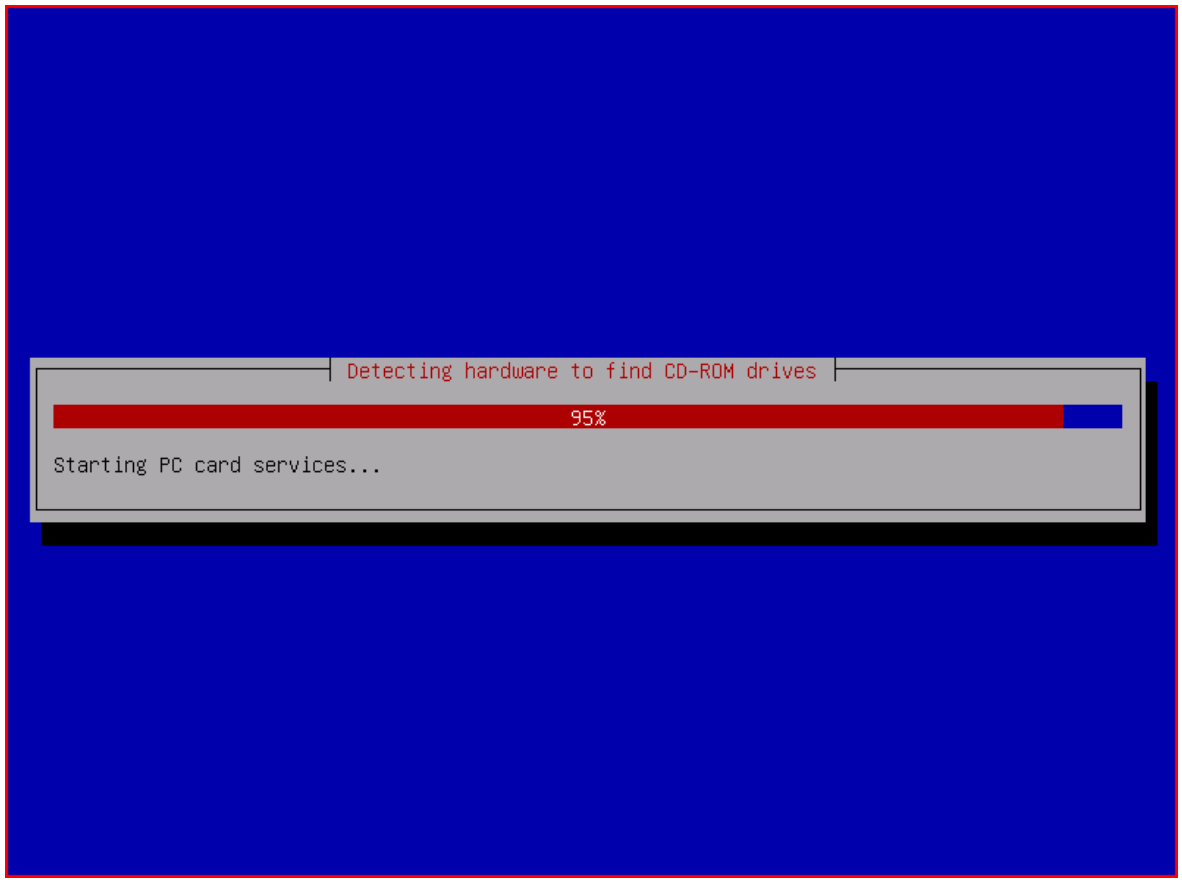
Οδηγία: Επιλέγουμε ως διάταξη πληκτρολογίου την Ελληνική «Greek».



Βήμα 6: Έλεγχος οπτικού δίσκου εγκατάστασης, υλικού, ρύθμιση δικτύου

Στο τρέχων βήμα ο οδηγός πραγματοποιεί έλεγχο του οπτικού δίσκου της εγκατάστασης, του υλικού στο οποίο θα πραγματοποιηθεί αυτή, καθώς και αυτόματο καθορισμό των ρυθμίσεων του δικτύου. Στην περίπτωση που ο τελευταίος αποτύχει (όπως όταν στο δίκτυο δε βρεθεί διακομιστής DHCP), γίνεται σχετική ερώτηση για επανάληψη της προσπάθειας αυτόματης ρύθμισης ή, εναλλακτικά, για χειροκίνητη ρύθμιση των παραμέτρων του δικτύου. Στη μη αυτόματη ρύθμιση, ο οδηγός υποβάλλει στο χρήστη ερωτήσεις για το δίκτυο και σύμφωνα με τις απαντήσεις πραγματοποιεί τις ανάλογες ρυθμίσεις αυτού (διεύθυνση IP, μάσκα δικτύου, πύλη δικτύου, διευθύνσεις εξυπηρετητών ονοματοδοσίας).

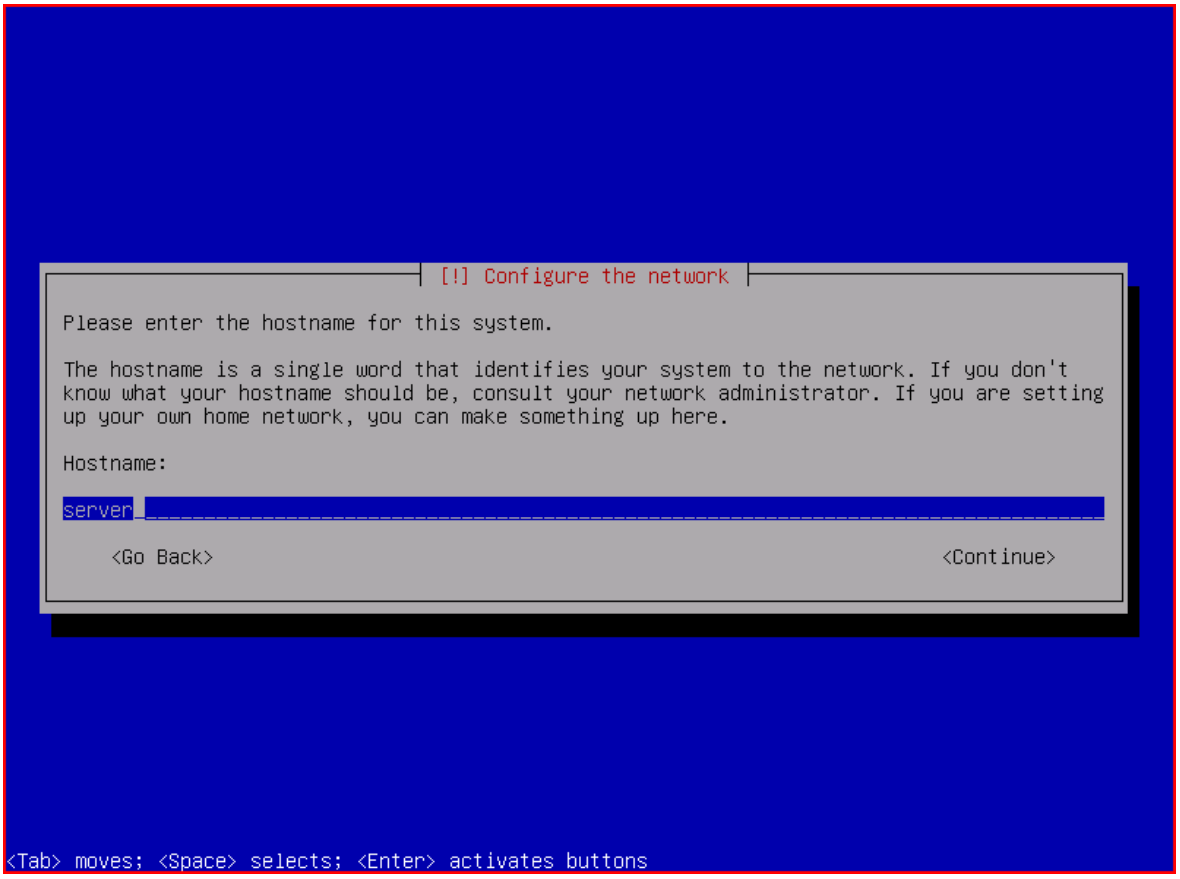
Οδηγία: Ο οδηγός εκτελεί έλεγχο του οπτικού δίσκου της εγκατάστασης, του υλικού στο οποίο θα πραγματοποιηθεί αυτή και τέλος, καθορισμό των ρυθμίσεων του δικτύου.



Βήμα 7: Καθορισμός ονόματος υπολογιστή

Σε αυτό το βήμα θα πρέπει να καθοριστεί το όνομα με το οποίο ο εξυπηρετητής θα είναι γνωστός στο δίκτυο. Οι περιορισμοί που ισχύουν σχετικά, έχουν καθοριστεί με τις προδιαγραφές RFC-952 και RFC-1123. Το όνομα θα πρέπει να είναι μια λέξη (χωρίς κενά) 1 έως 63 χαρακτήρων, οι οποίοι μπορεί να είναι χωρίς διάκριση πεζά ή κεφαλαία γράμματα του Αγγλικού αλφαβήτου ('a' έως 'z'), αριθμοί ('0' έως '9'), ή η παύλα ('-'), με την προϋπόθεση ότι αυτή δε θα είναι ο πρώτος ή ο τελευταίος χαρακτήρας στο όνομα. Ειδικής μνείας, χρίζει το ότι στις παλαιότερες προδιαγραφές RFC-952 δεν επιτρεπόταν η χρήση αριθμού στη θέση του πρώτου χαρακτήρα του ονόματος. Αυτό όμως έχει καταργηθεί και πλέον δεν ισχύει στις πιο πρόσφατες προδιαγραφές RFC-1123.

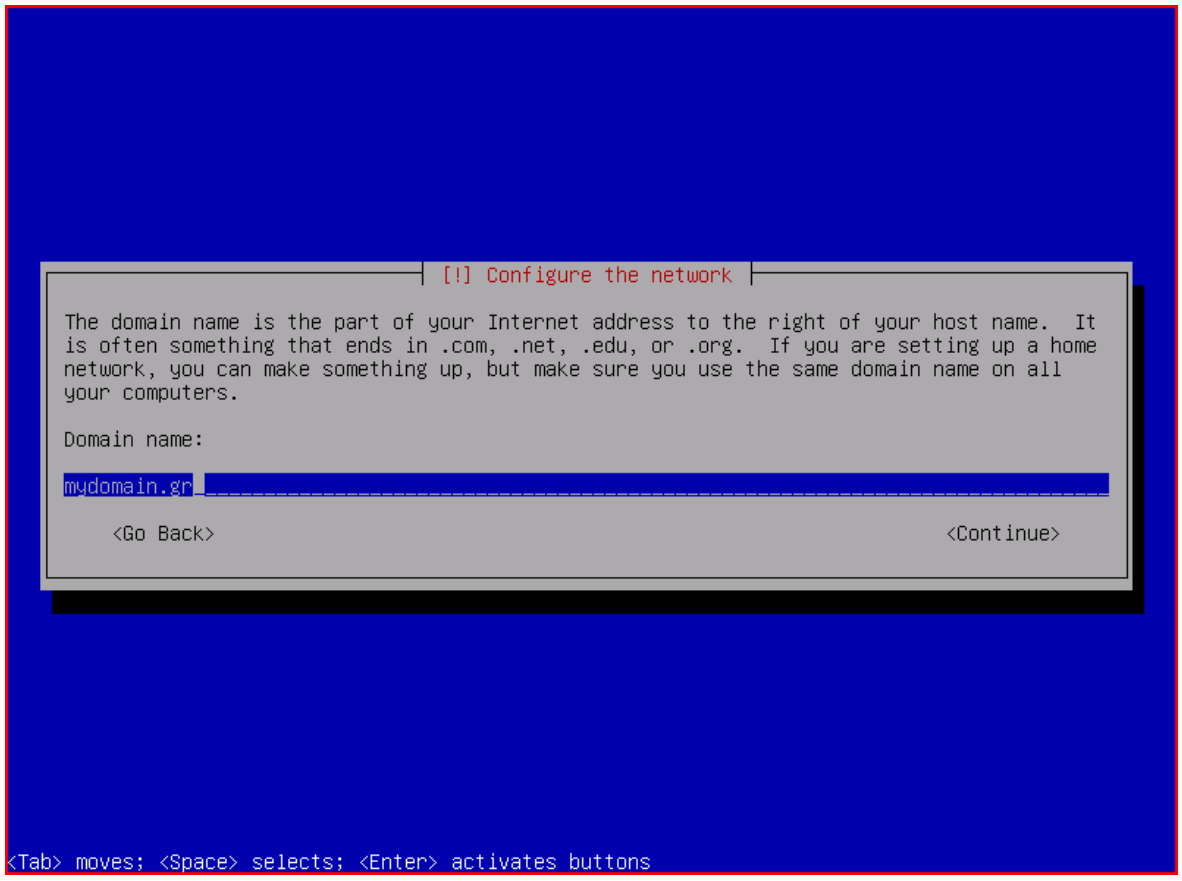
Οδηγία: Εισάγουμε το όνομα του εξυπηρετητή στο δίκτυο (hostname).



Βήμα 8: Καθορισμός ονόματος τομέα

Το παρών βήμα αφορά στον καθορισμό του ονόματος τομέα (domain name) στον οποίο ανήκει ο εξυπηρετητής. Ισχύουν και εδώ οι περιορισμοί που ισχύουν σχετικά με τον καθορισμό του ονόματος του συστήματος (προδιαγραφές RFC-952 και RFC-1123). Ο συνδυασμός του ονόματος τομέα και του ονόματος του εξυπηρετητή καθορίζει το fully qualified domain name (FQDN) αυτού, με το οποίο το σύστημα καθίσταται μοναδικό παγκοσμίως (δεν είναι εφικτό να υπάρχει το ίδιο ακριβώς όνομα σε περισσότερα από ένα συστήματα που ανήκουν στον ίδιο τομέα).

Οδηγία: Εισάγουμε το όνομα του τομέα (domain name), στον οποίο ανήκει ο εξυπηρετητής.



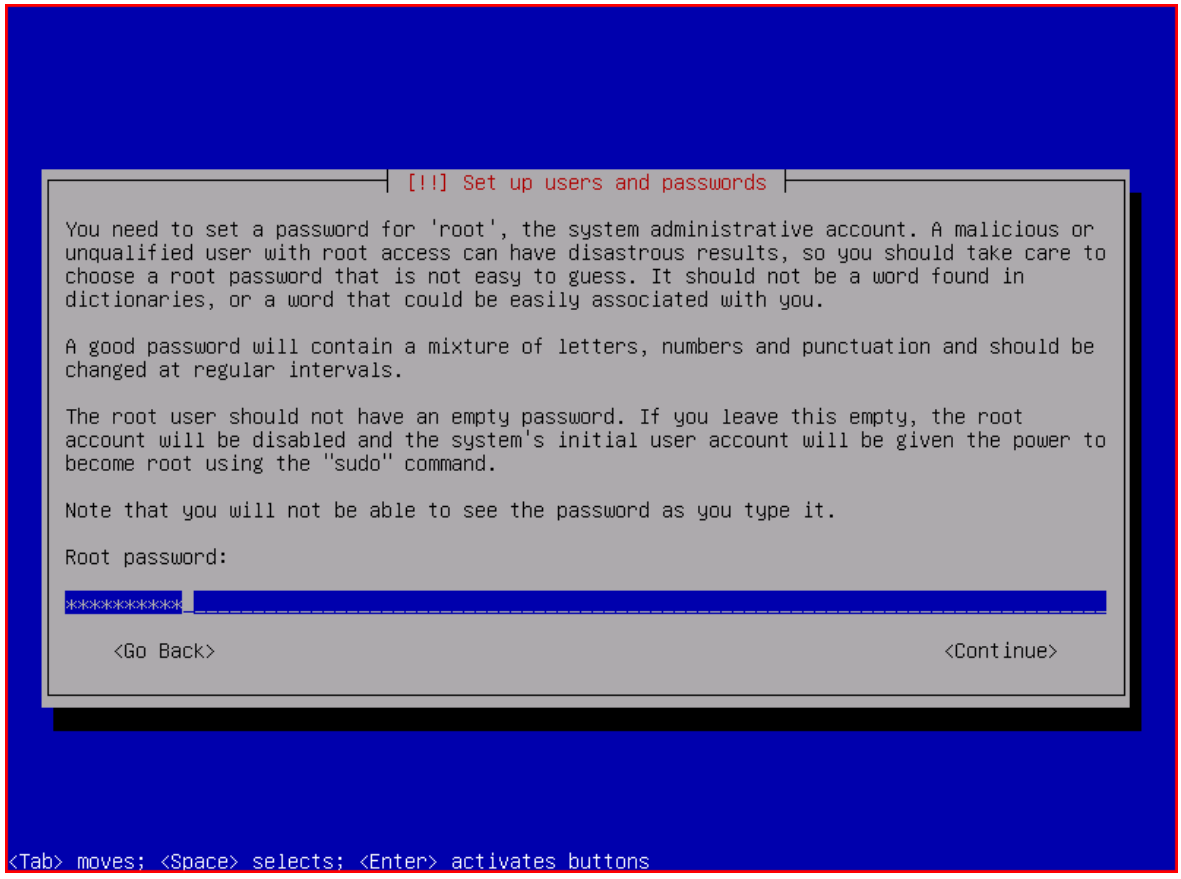
Βήμα 9: Καθορισμός κωδικού πρόσβασης διαχειριστή

Ο λογαριασμός του διαχειριστή του συστήματος, ή υπερχρήστη, ή root, είναι λογαριασμός με δυνατότητα πρόσβασης, η οποία παρακάμπτει κάθε προστασία ασφάλειας στο Debian GNU/Linux. Ο λογαριασμός αυτός θα πρέπει να είναι προσβάσιμος μόνο από εξουσιοδοτημένους χρήστες του εξυπηρετητή και να χρησιμοποιείται αποκλειστικά και μόνο για τη διαχείριση αυτού. Επιπλέον, ο κωδικός πρόσβασής του είναι πάρα πολύ σημαντικό να πληροί τις προδιαγραφές ενός ισχυρού κωδικού, έχοντας τα παρακάτω χαρακτηριστικά:

- να έχει ικανοποιητικό μήκος (τουλάχιστον 10 χαρακτήρες)
- να περιέχει συνδυασμό πεζών και κεφαλαίων γραμμάτων, αριθμών, καθώς και συμβόλων στίξης
- να μην υφίσταται ως λέξη σε οποιαδήποτε γλώσσα
- να μη βασίζεται σε προφανή στοιχεία όπως ημερομηνίες, ονόματα κτλ

Ένας τρόπος ελέγχου της ισχύος του κωδικού πρόσβασης παρέχεται δωρεάν στην ιστοσελίδα www.passwordmeter.com, όπου εκτός από βαθμολόγηση της πολυπλοκότητάς του, γίνεται ανάλυση των πλεονεκτημάτων, καθώς και μειονεκτημάτων του. Σε κάθε περίπτωση είναι ιδιαίτερα σημαντικό να τονίζεται το ότι η χρήση ισχυρών κωδικών μπορεί να μειώνει τον κίνδυνο παραβίασης της ασφάλειας του συστήματος, δεν είναι όμως σε θέση να εξαλείψει την ανάγκη για περαιτέρω ελέγχους.

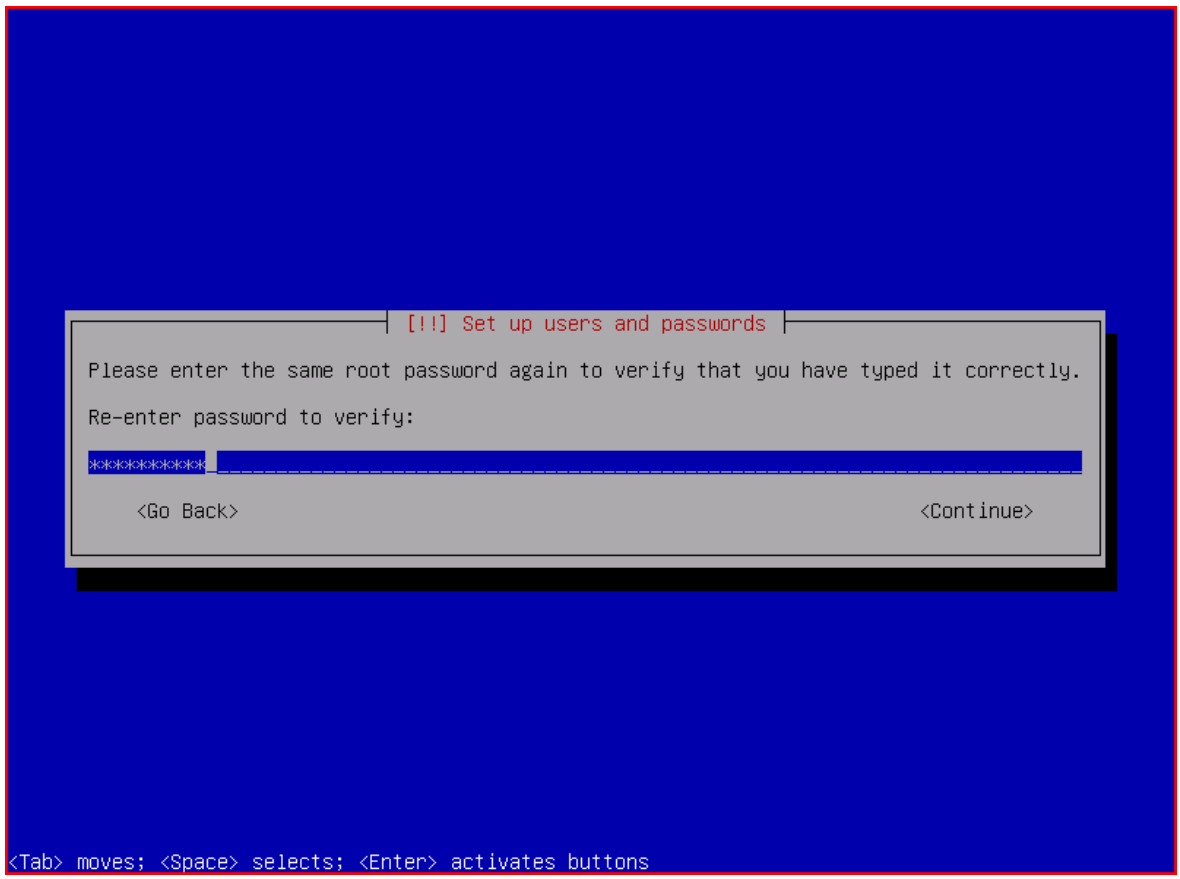
Οδηγία: Εισάγουμε τον επιθυμητό κωδικό για το διαχειριστή του εξυπηρετητή.



Βήμα 10: Επιβεβαίωση ορθής εισαγωγής κωδικού διαχειριστή

Για την αποφυγή τυχόν σφαλμάτων πληκτρολόγησης ζητείται η εκ νέου εισαγωγή του κωδικού πρόσβασης που έχει επιλεγεί για το χρήστη root.

Οδηγία: Επανεισάγουμε τον επιθυμητό κωδικό πρόσβασης για το χρήστη root.



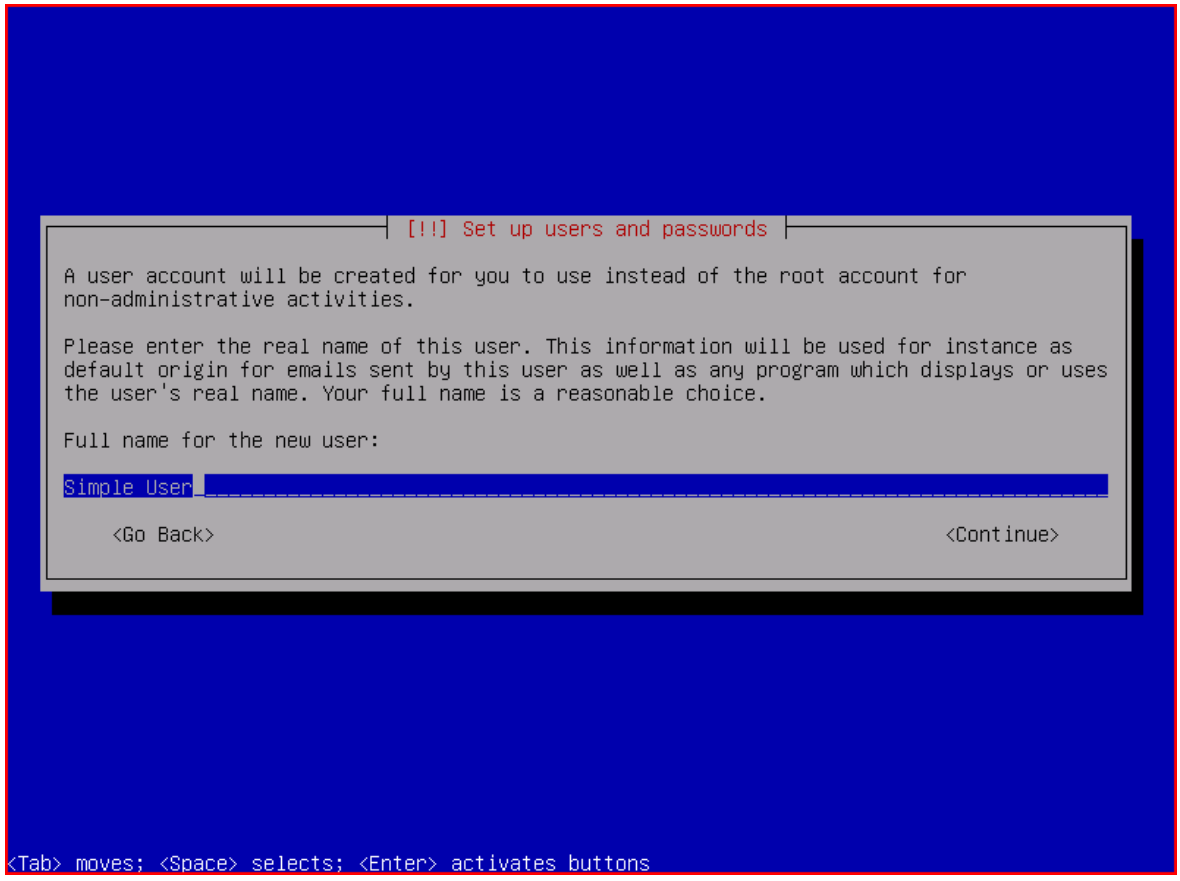
Βήμα 11: Καθορισμός πλήρους ονόματος απλού χρήστη

Εκτός από τον παραπάνω λογαριασμό του διαχειριστή θα πρέπει να δημιουργηθεί ένας ακόμη λογαριασμός, ο οποίος δε θα έχει ειδικά δικαιώματα πρόσβασης στο σύστημα. Η χρησιμότητα αυτής της ενέργειας ίσως αμφισβητηθεί εάν αναλογιστεί κανείς ότι η αλληλεπίδραση με τον εξυπηρετητή (σε αυτό το επίπεδο), θα πρέπει να αφορά αποκλειστικά στη διαχείριση αυτού, κάτι που εξ' ορισμού απαιτεί «ανεβασμένα» δικαιώματα. Έτσι, εκτός από το να αναρωτηθεί εάν πραγματικά απαιτείται ο συγκεκριμένος λογαριασμός του απλού χρήστη, κάποιος μπορεί εύλογα να ανησυχήσει για πιθανή υποβάθμιση του επιπέδου ασφαλείας του συστήματος.

Αντιθέτως, ο λογαριασμός του απλού χρήστη όχι μόνο δεν είναι περιττός και δε θα μειώσει το επίπεδο ασφάλειας του συστήματος, αλλά θα είναι ιδιαίτερα χρήσιμος στην αύξηση αυτού. Η τεχνική που θα ακολουθηθεί στον οδηγό της παρούσας εργασίας για να επιτευχθεί αυτό είναι η παρακάτω: στο χρήστη «root» θα απαγορευτεί η δυνατότητα απομακρυσμένης σύνδεσης στο σύστημα. Έτσι, ακόμα και με το σωστό κωδικό πρόσβασης, δε θα είναι σε θέση κάποιος κακόβουλος χρήστης να αποκτήσει απομακρυσμένη πρόσβαση στο λογαριασμό του υπερ-χρήστη. Ο εξουσιοδοτημένος διαχειριστής θα πρέπει αρχικά να χρησιμοποιήσει το όνομα και τον κωδικό πρόσβασης του απλού χρήστη για να συνδεθεί απομακρυσμένα με τον εξυπηρετητή και στη συνέχεια να αιτηθεί την εκχώρηση των ανεβασμένων δικαιωμάτων, παρέχοντας φυσικά τα απαιτούμενα διαπιστευτήρια (το δικό του κωδικό πρόσβασης). Συνεπώς, κάποιος μη εξουσιοδοτημένος χρήστης, που επιδιώκει να αποκτήσει απομακρυσμένη πρόσβαση, θα πρέπει να «μαντέψει» τον όνομα και τον κωδικό του απλού χρήστη και ακολούθως τον κωδικό πρόσβασης του διαχειριστή, προτού να είναι σε θέση να βλάψει σημαντικά το σύστημα.

Για τη δημιουργία του λογαριασμού του απλού χρήστη, θα πρέπει αρχικά να καθοριστεί το κανονικό, πραγματικό όνομα αυτού, το οποίο μπορεί να είναι το πλήρες ονοματεπώνυμό του με τη μορφή «Επώνυμο Όνομα».

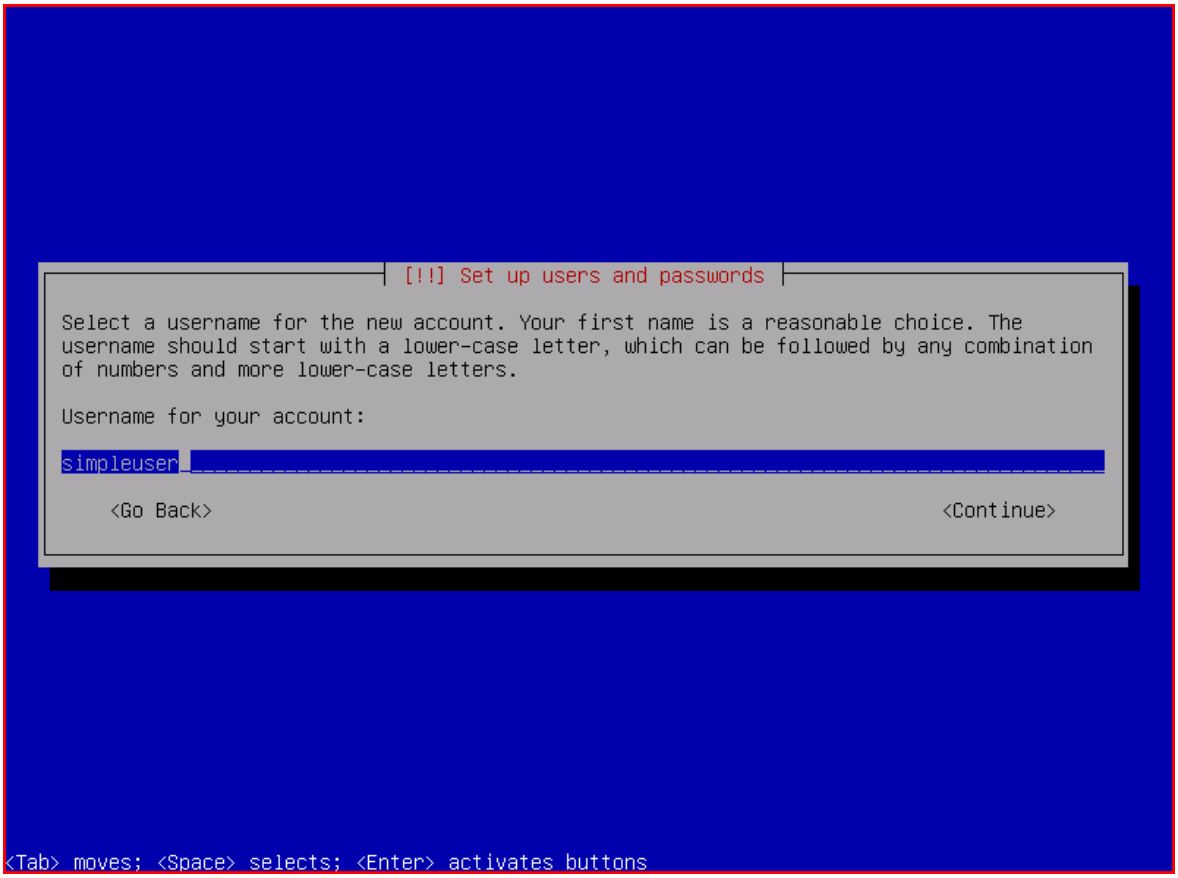
Οδηγία: Εισάγουμε το πλήρες όνομα για τον απλό χρήστη του εξυπηρετητή.



Βήμα 12: Καθορισμός ονόματος χρήστη απλού χρήστη

Στο συγκεκριμένο βήμα θα πρέπει να καθοριστεί το όνομα χρήστη (username ή userid) με το οποίο θα συνδέεται ο απλός χρήστης στο σύστημα. Σύμφωνα με το εγχειρίδιο του adduser, που χρησιμοποιείται για την προσθήκη νέων χρηστών στα συστήματα Debian GNU/Linux, το όνομα χρήστη θα πρέπει να αρχίζει από Αγγλικό πεζό χαρακτήρα και να ακολουθείται από οποιονδήποτε συνδυασμό Αγγλικών πεζών γραμμάτων και αριθμών. Επιπλέον, στο εγχειρίδιο της εντολής useradd (που κρύβεται πίσω από το script adduser) προβλέπεται ότι το μέγιστο μήκος του ονόματος χρήστη δε μπορεί να υπερβαίνει τους 32 χαρακτήρες. Τέλος, θα πρέπει να αναφερθεί ότι είναι δεσμευμένο από το σύστημα και δε μπορεί να χρησιμοποιηθεί το όνομα χρήστη «admin» [40].

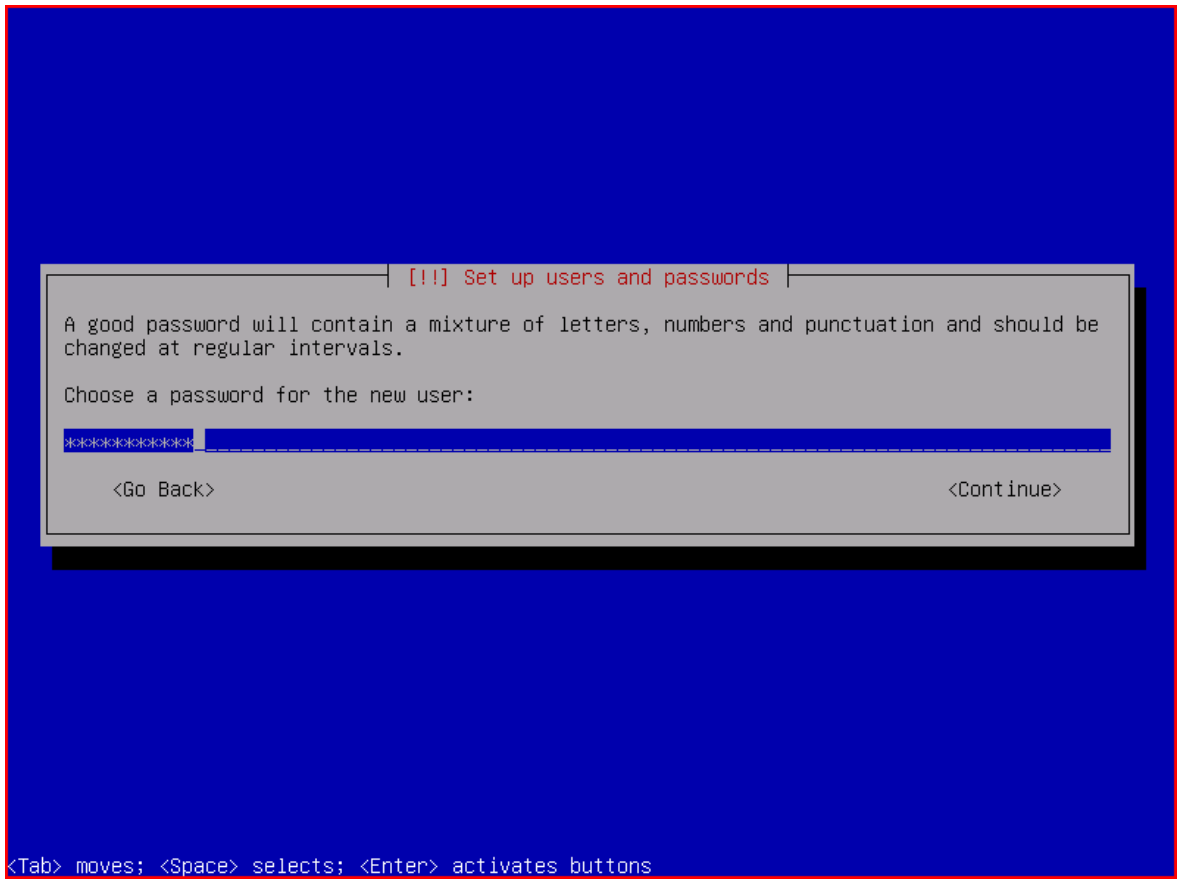
Οδηγία: Εισάγουμε το επιθυμητό όνομα χρήστη για τον απλό χρήστη.



Βήμα 13: Καθορισμός κωδικού πρόσβασης απλού χρήστη

Στο τρέχων βήμα θα πρέπει να καθοριστεί ο κωδικός πρόσβασης για το λογαριασμό του απλού χρήστη. Εκτός του ότι ισχύουν και εδώ τα όσα ισχύουν σχετικά με τον κωδικό του διαχειριστή, είναι αυτονόητο ότι για τη διατήρηση υψηλότερου επίπεδου ασφάλειας του συστήματος θα πρέπει να χρησιμοποιηθεί για τον απλό χρήστη διαφορετικός κωδικός από αυτόν που χρησιμοποιήθηκε για το διαχειριστή.

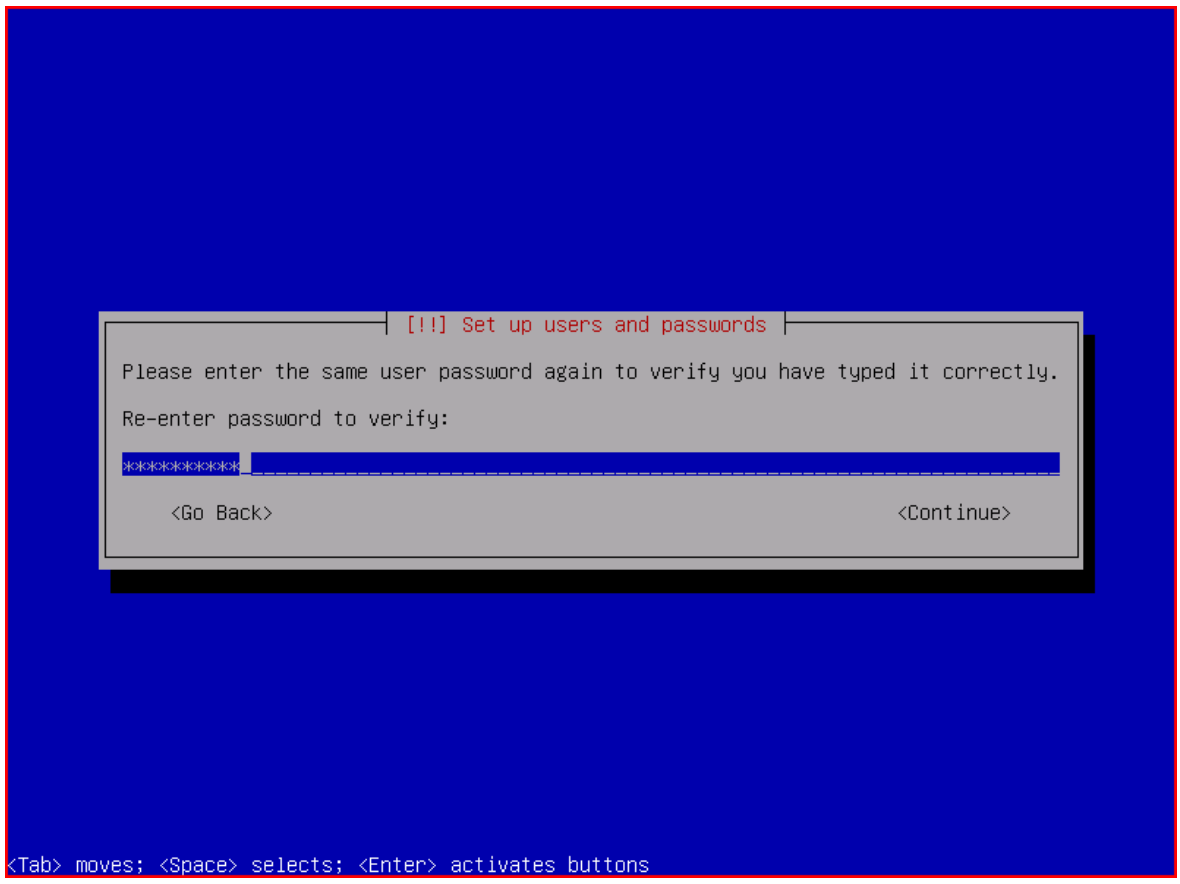
Οδηγία: Εισάγουμε τον επιθυμητό κωδικό για τον απλό χρήστη.



Βήμα 14: Επιβεβαίωση ορθής εισαγωγής κωδικού απλού χρήστη

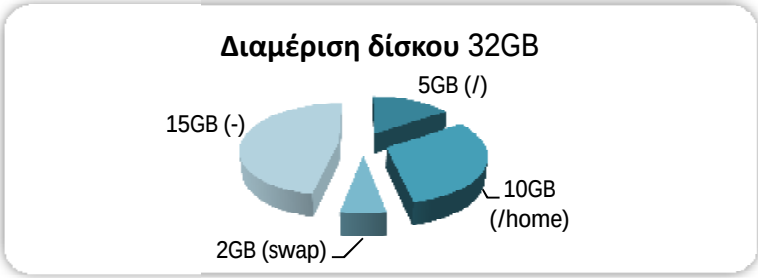
Για την αποφυγή τυχόν σφαλμάτων πληκτρολόγησης ζητείται η εκ νέου εισαγωγή του κωδικού πρόσβασης που έχει επιλεγεί για τον απλό χρήστη.

Οδηγία: Επανεισάγουμε τον επιθυμητό κωδικό πρόσβασης για τον απλό χρήστη.



Βήμα 15: Διαμέριση και επιλογή σημείων προσάρτησης

Στο συγκεκριμένο βήμα του οδηγού εγκατάστασης, δίδεται στο χρήστη η δυνατότητα για διαμέριση των δίσκων, δημιουργία συστημάτων αρχείων και απόδοση σημείων προσάρτησης. Είναι πάρα πολλές οι πιθανές περιπτώσεις χρήσης και δεν είναι εφικτό να καλυφθούν όλες από την παρούσα εργασία. Έτσι, έχει επιλεχθεί ως παράδειγμα η ύπαρξη ενός και μόνο δίσκου συνολικής χωρητικότητας 32GB, ο οποίος και θα διαμεριστεί, χωρίς την αυτόματη καθοδήγηση, στις παρακάτω πρωτεύουσες (primary) κατατμήσεις:



Κατάτμηση	Χωρητικότητα	Σύστημα αρχείων	Σημείο προσάρτησης
1	5GB	ext4	/
2	10GB	ext4	/home
3	2GB	swap	swap
4	15GB	ext4	- (μη προσαρτημένο)

Όπως φαίνεται στον παραπάνω πίνακα, στην πρώτη κατάτμηση θα αφιερωθούν 5GB από το χώρο του δίσκου και εκεί θα προσαρτηθεί ολόκληρος ο ριζικός φάκελος (/), εξαιρουμένου του φάκελου χρηστών (/home), ο οποίος και θα προσαρτηθεί ξεχωριστά, στη δεύτερη, μεγέθους 10GB κατάτμηση. Στην τρίτη κατάτμηση, που θα έχει μέγεθος 2GB, θα προσαρτηθεί η εικονική μνήμη (swap) και ο υπόλοιπος χώρος του δίσκου θα διαμορφωθεί, όμως δε θα προσαρτηθεί.

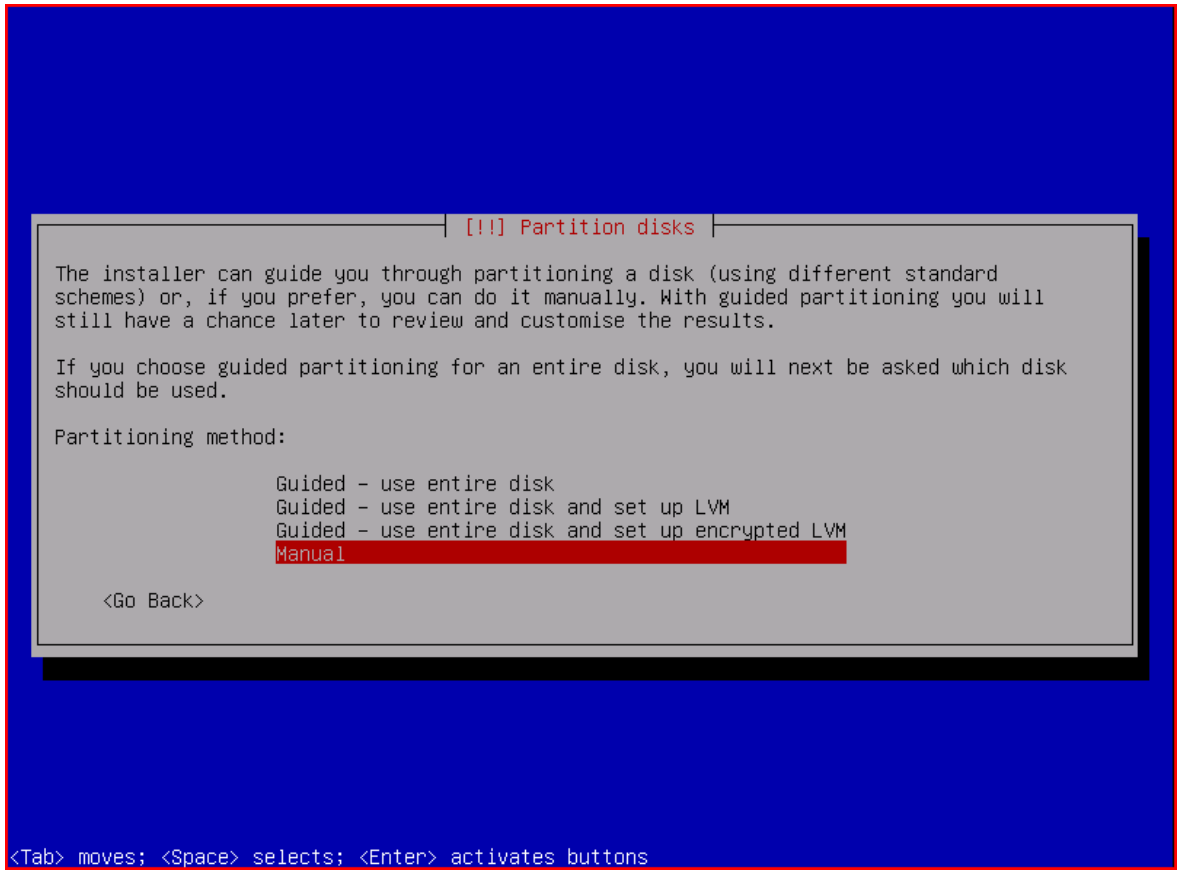
Ο συγκεκριμένος τρόπος διαμέρισης του δίσκου και προσάρτησης των κατατμήσεων, επιτρέπει τη μεμονωμένη άντληση αντιγράφου ασφαλείας του λειτουργικού συστήματος του εξυπηρετητή, την τοποθέτηση αυτού στη μη χρησιμοποιούμενη κατάτμηση, με τελικό αποτέλεσμα να υπάρχουν δύο πανομοιότυπα λειτουργικά

συστήματα, τα οποία, μετά τις κατάλληλες ρυθμίσεις, θα μπορούν να λειτουργούν εκ περιτροπής με «κοινόχρηστο» το φάκελο χρηστών. Αυτό σημαίνει ότι, για την επιδιόρθωση κάποιου σοβαρού προβλήματος δε θα απαιτηθεί επανεγκατάσταση του λειτουργικού συστήματος, αλλά ο εξυπηρετητής θα είναι σε θέση να λειτουργήσει και πάλι μετά από ελάχιστα λεπτά, μετά δηλαδή από μια απλή επανεκκίνηση, στην οποία θα επιλεγεί η εκκίνηση του συστήματος από την εικόνα αντιγράφου (περαιτέρω ανάλυση και υλοποίηση της συγκεκριμένης τεχνικής θα γίνει σε επόμενο κεφάλαιο). Τέλος, ο επιπλέον χώρος της τελευταίας, μη προσαρτημένης κατάτμησης θα χρησιμοποιηθεί σε μεταγενέστερο βήμα του οδηγού για την αυτοματοποιημένη λήψη συμπιεσμένων αντιγράφων ασφαλείας του φακέλου χρηστών.

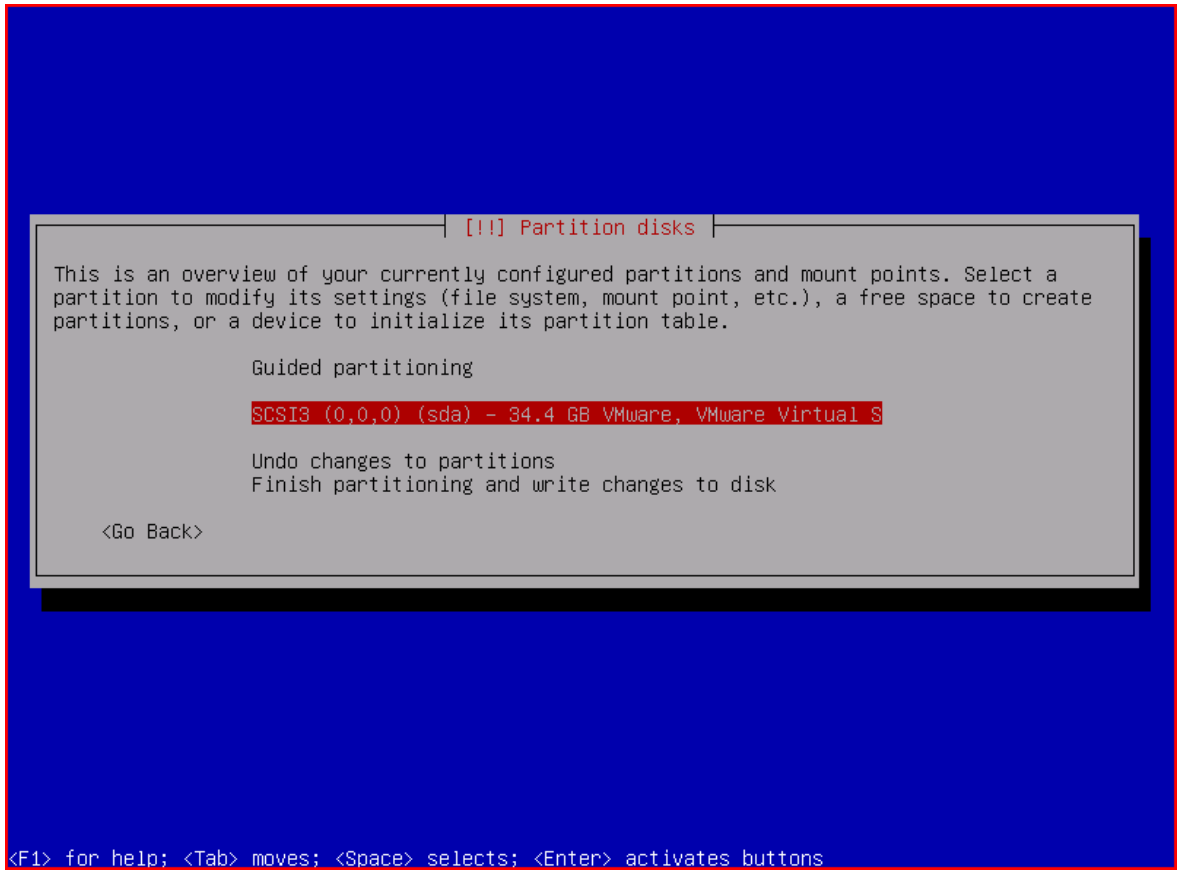
Με εξαίρεση την εικονική μνήμη, η διαμόρφωση όλων των κατατμήσεων έχει επιλεγεί να γίνει με το σύστημα αρχείων ext4, λόγω των αυξημένων επιδόσεων και αξιοπιστίας που αυτό παρουσιάζει σε σύγκριση με το προγενέστερο ext3. Τα προβλήματα που εμφανίστηκαν το πρώτο διάστημα χρήσης του και σχετιζόταν με την εν δυνάμει απώλεια δεδομένων, αφενός δεν είχαν άμεση σχέση με το ίδιο το σύστημα αρχείων, αφετέρου έχουν ξεπεραστεί από την έκδοση πυρήνα 2.6.30 και μετά [29]. Όλες οι κατατμήσεις έχουν γίνει πρωτεύουσες και όχι λογικές επειδή έτσι θα είναι πολύ πιο εύκολο να υλοποιηθεί μια πιθανόν απαιτούμενη αλλαγή μεγέθους οποιασδήποτε από αυτές στο μέλλον.

Όπως αναφέρθηκε παραπάνω, το συγκεκριμένο βήμα του οδηγού εγκατάστασης περιλαμβάνει πληθώρα περιπτώσεων χρήσης. Έτσι, εάν αυτό απαιτείται, η δημιουργία κατατμήσεων μπορεί να μελετηθεί επιπλέον στο παράρτημα C του οδηγού εγκατάστασης Debian GNU/Linux [30].

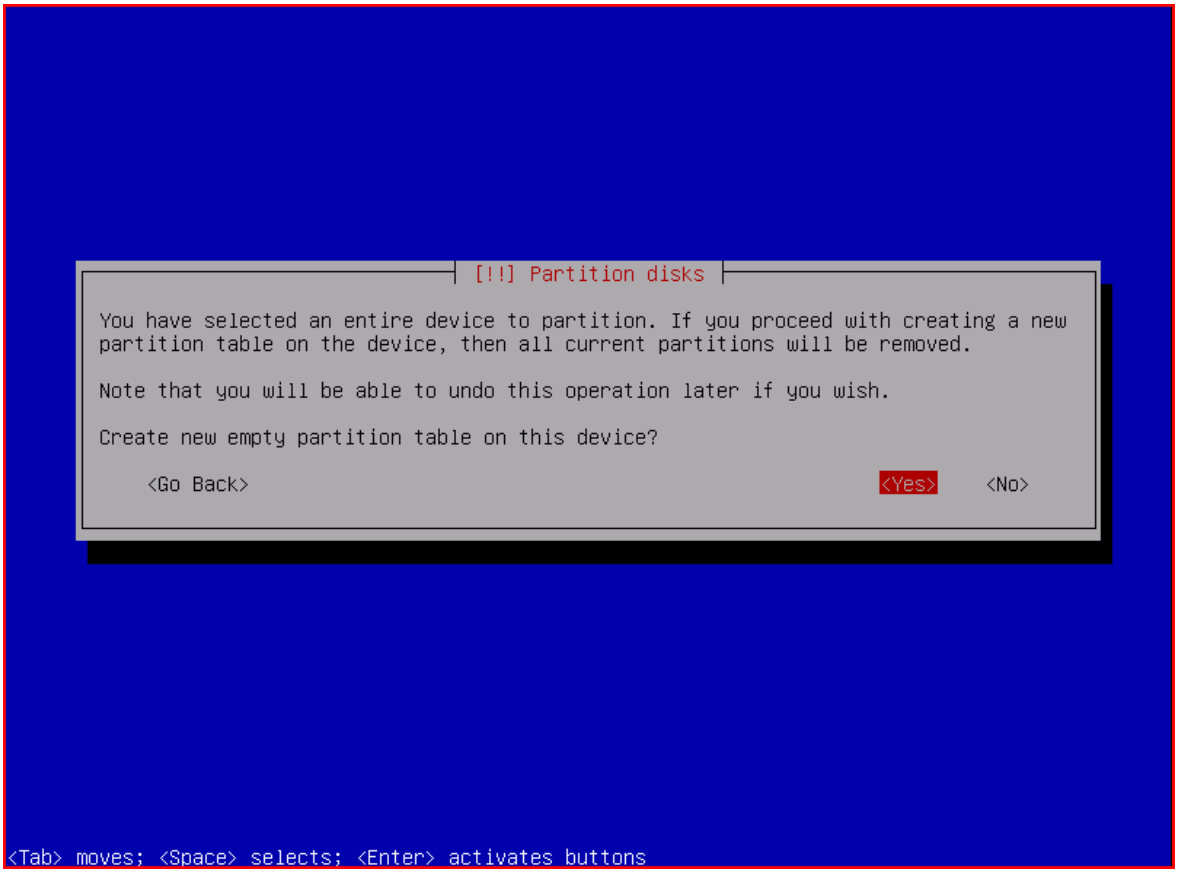
Οδηγία: Επιλέγουμε τη διαμέριση του δίσκου χωρίς τη χρήση του οδηγού (Manual).



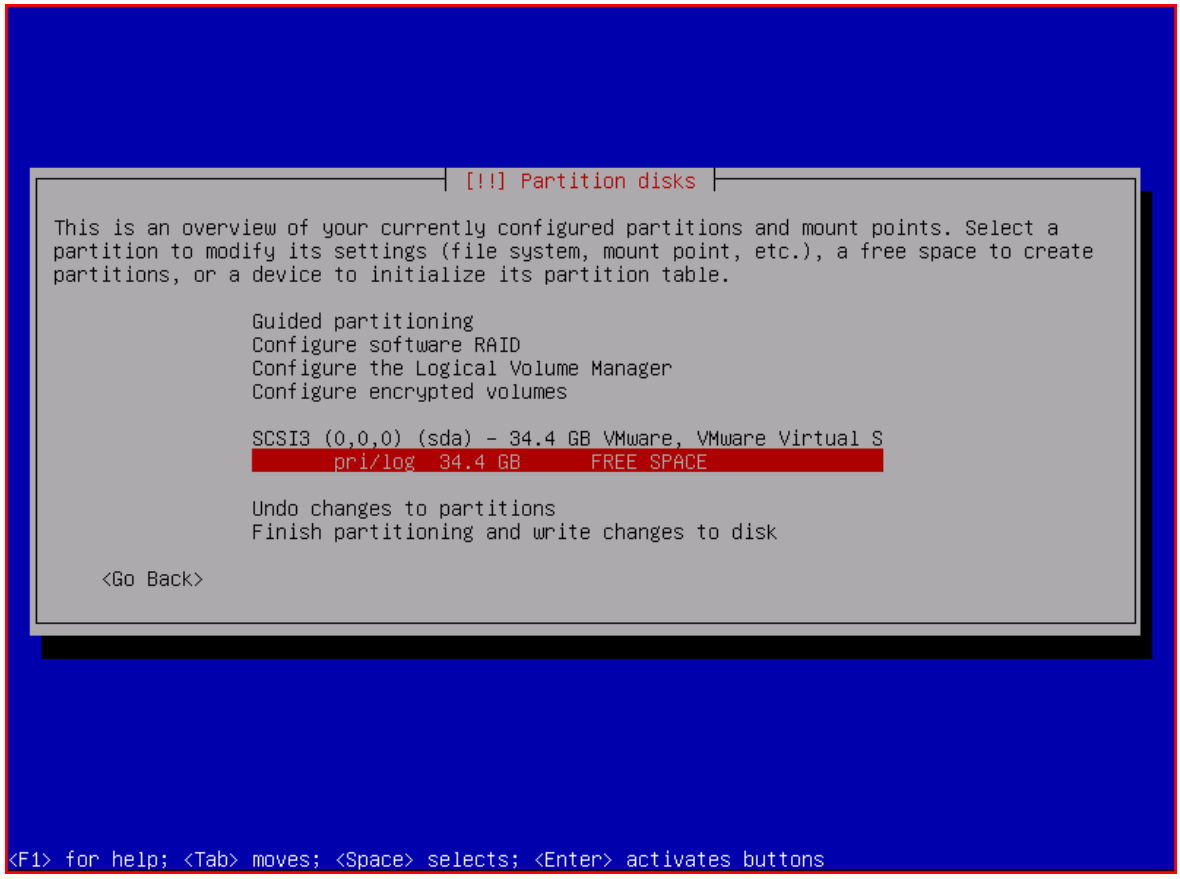
Οδηγία: Επιλέγουμε τον προς διαμέριση δίσκο.



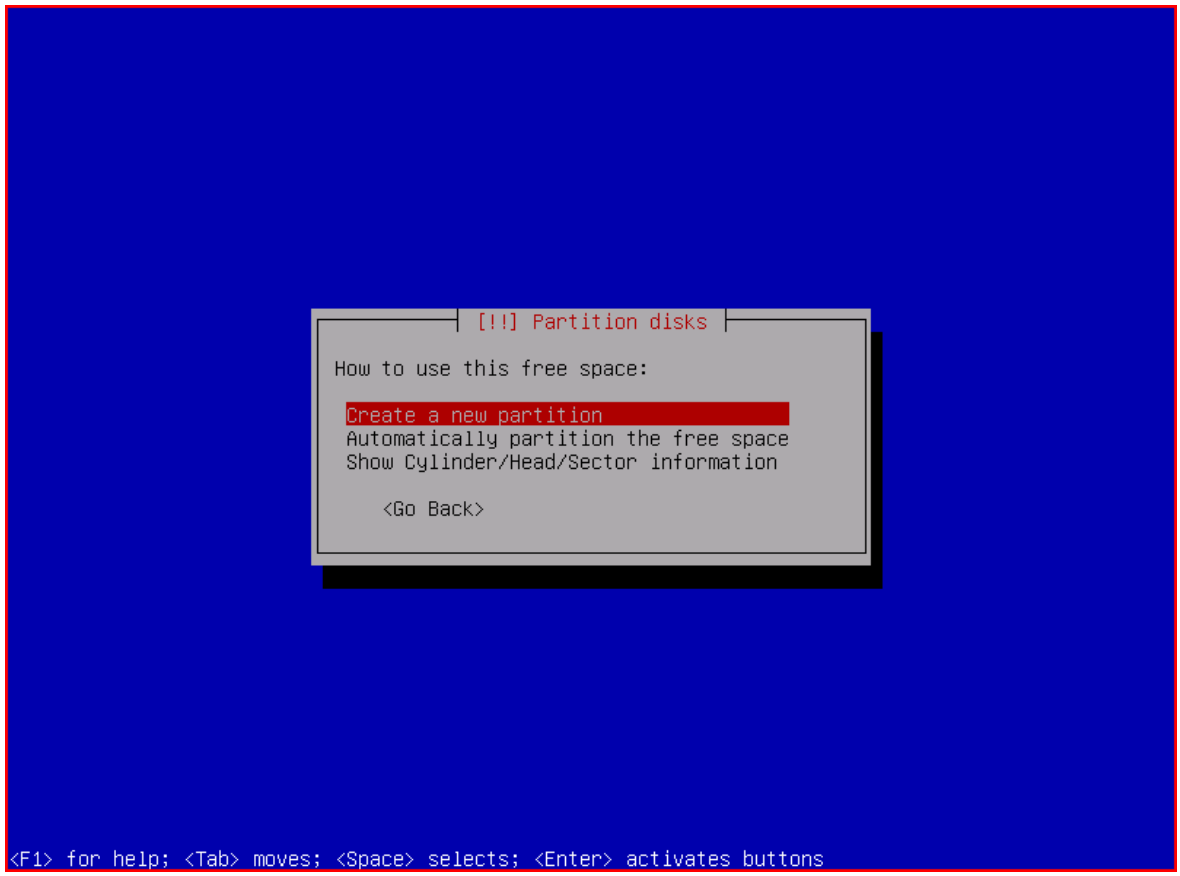
Οδηγία: Επιλέγουμε «Yes» για να δημιουργηθεί πίνακας κατατμήσεων στο δίσκο.



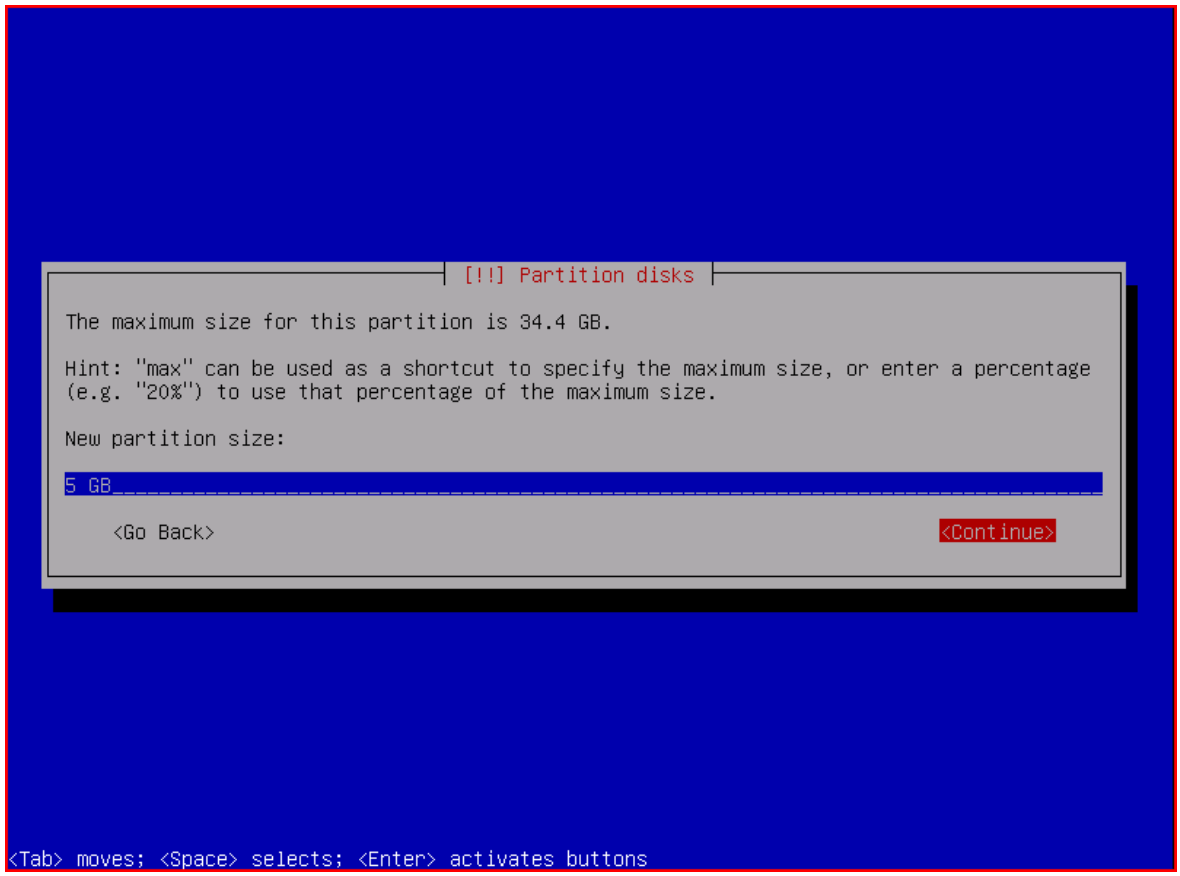
Οδηγία: Επιλέγουμε τον άδειο, προς χρήση χώρο του δίσκου.



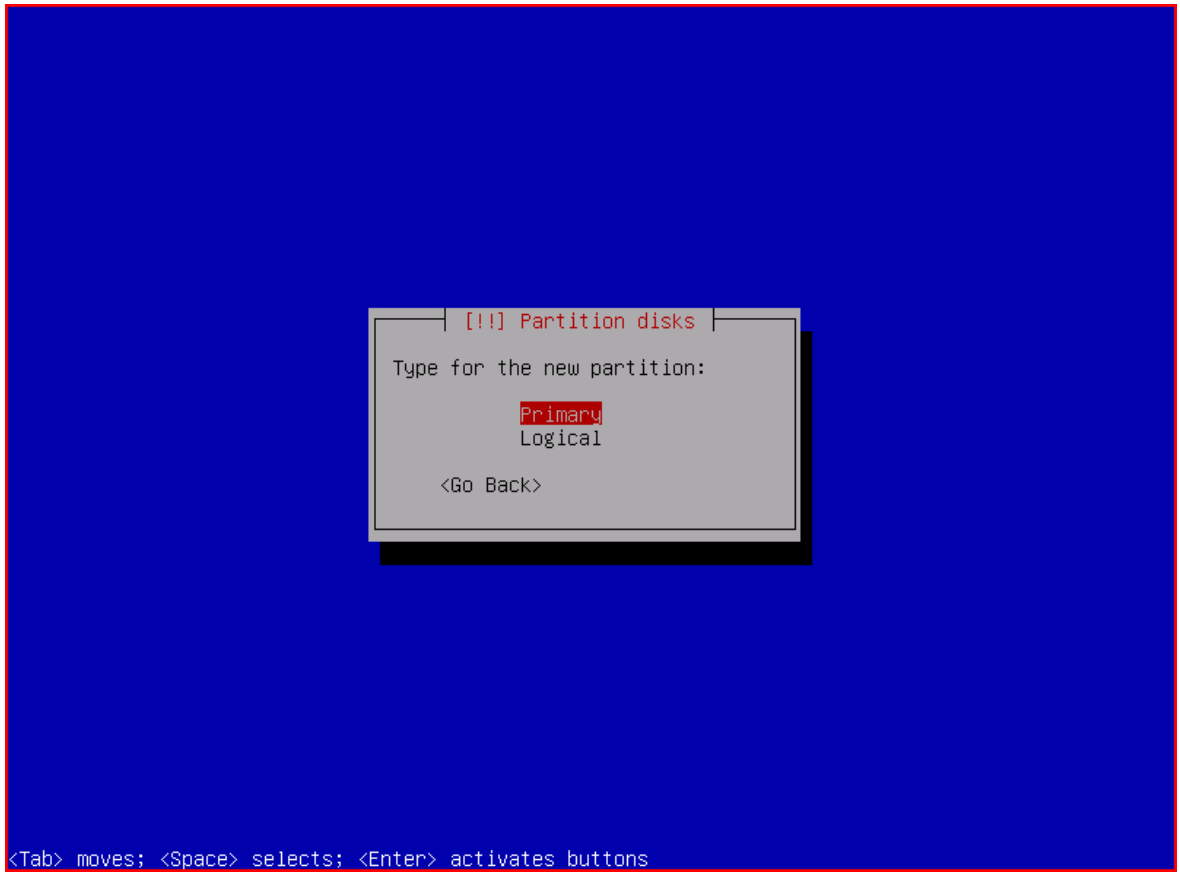
Οδηγία: Επιλέγουμε να χρησιμοποιήσουμε τον κενό χώρο του δίσκου για τη δημιουργία νέας κατάτμησης.



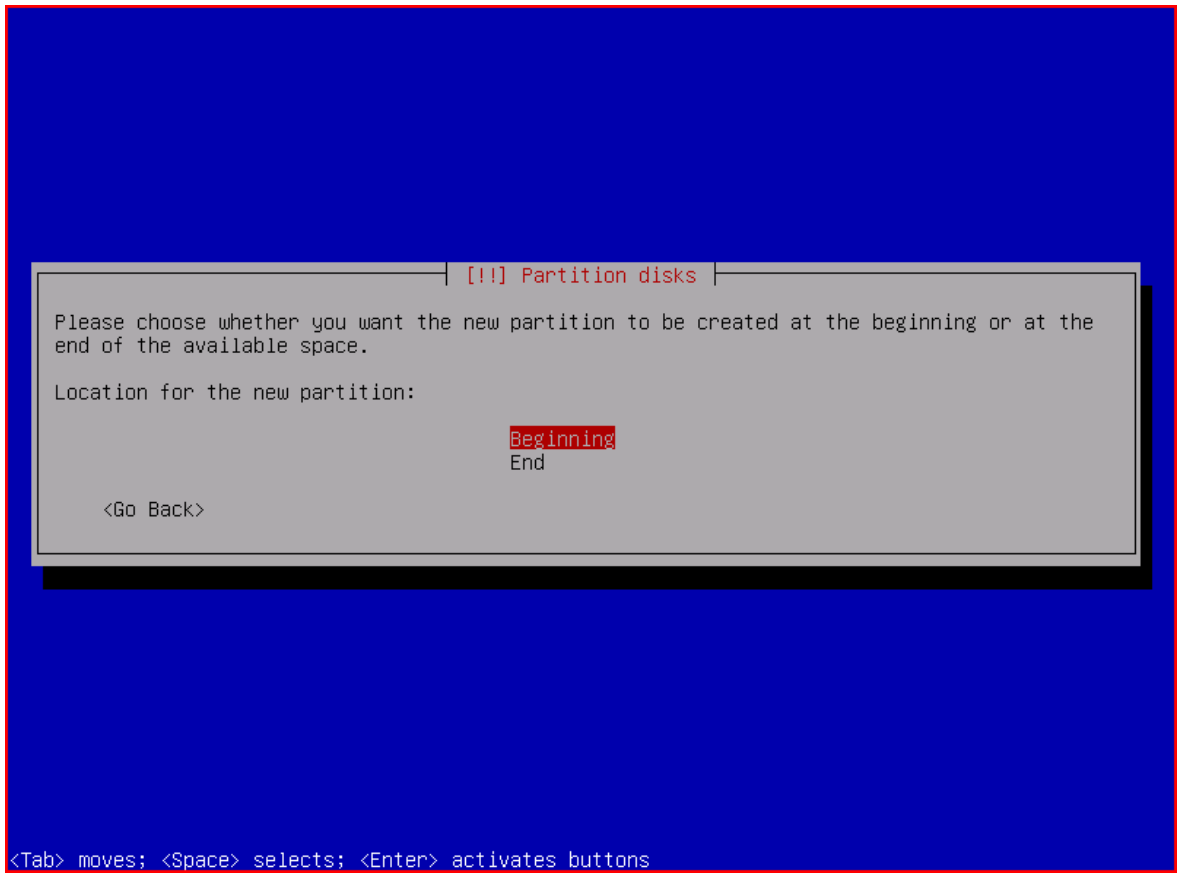
Οδηγία: Καθορίζουμε το μέγεθος της νέας κατάτμησης (στο παράδειγμα φαίνεται το μέγεθος των 5GB που αφορά στην πρώτη κατάτμηση).



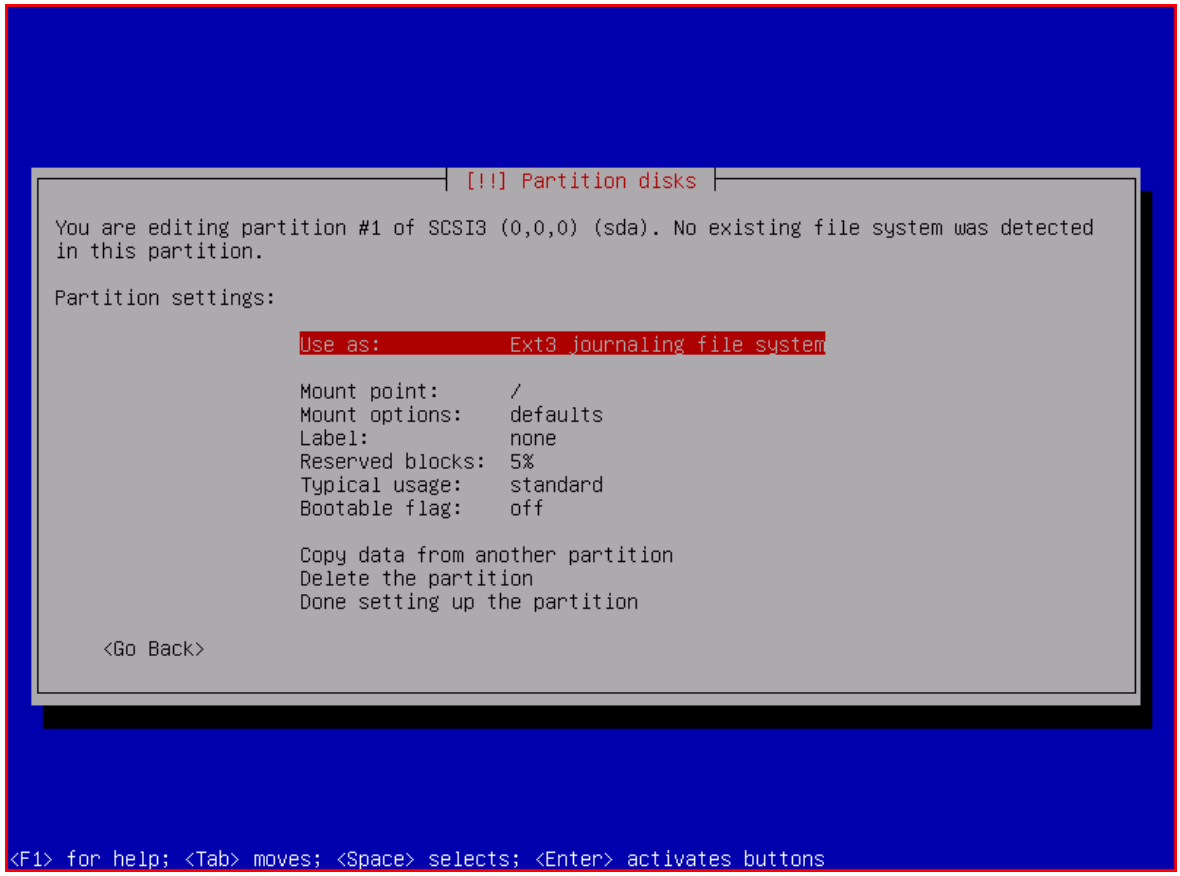
Οδηγία: Επιλέγουμε η κατάτμηση να είναι πρωτεύουσα και όχι λογική.



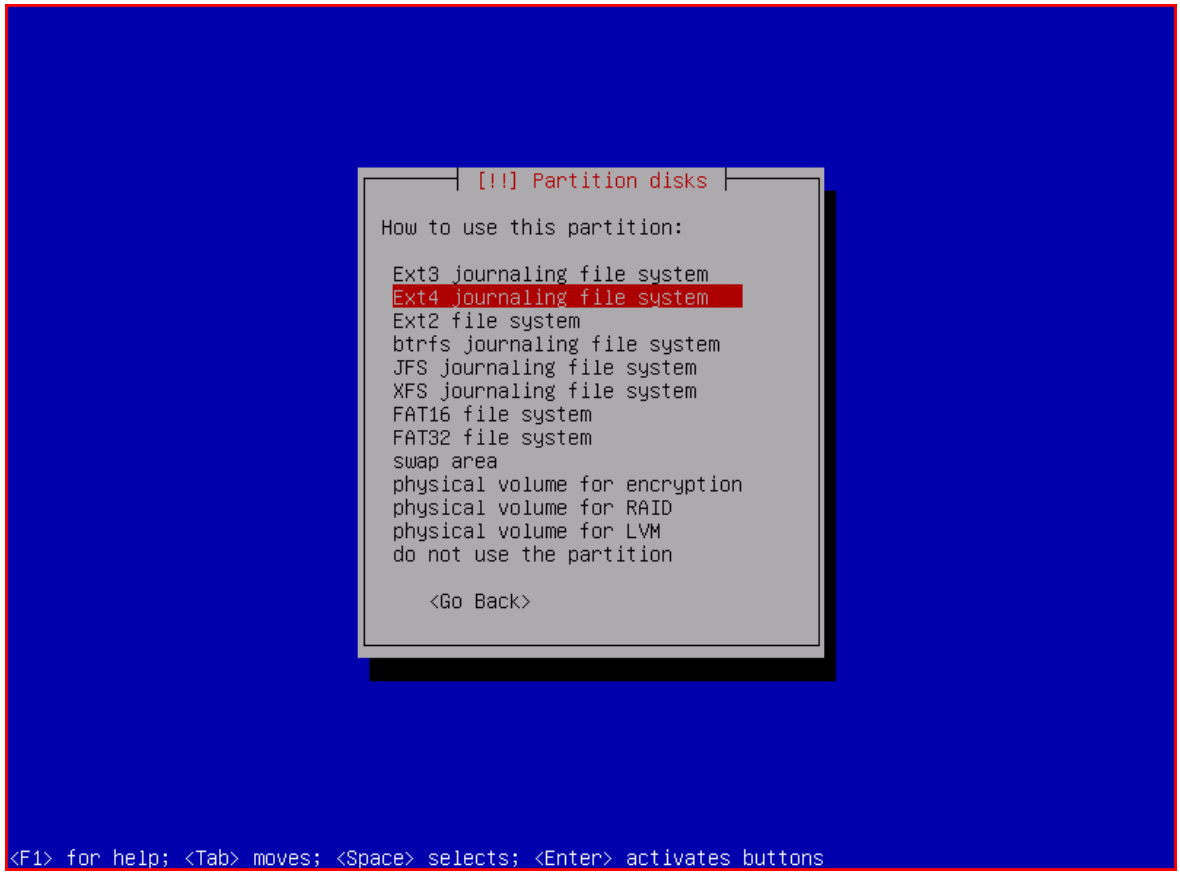
Οδηγία: Επιλέγουμε η νέα κατάτμηση να δημιουργηθεί στην αρχή του διαθέσιμου χώρου στο δίσκο.



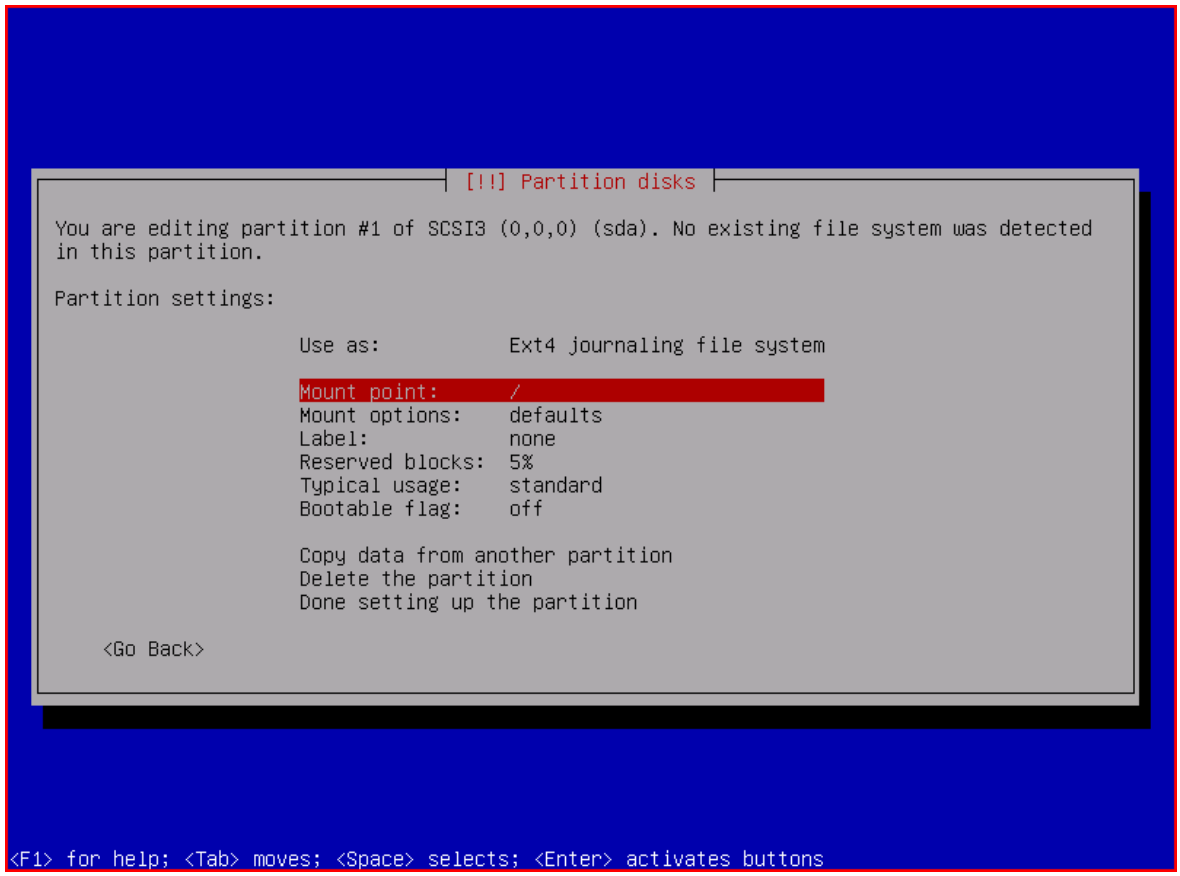
Οδηγία: Επιλέγουμε το σύστημα αρχείων για τη νέα κατάτμηση.

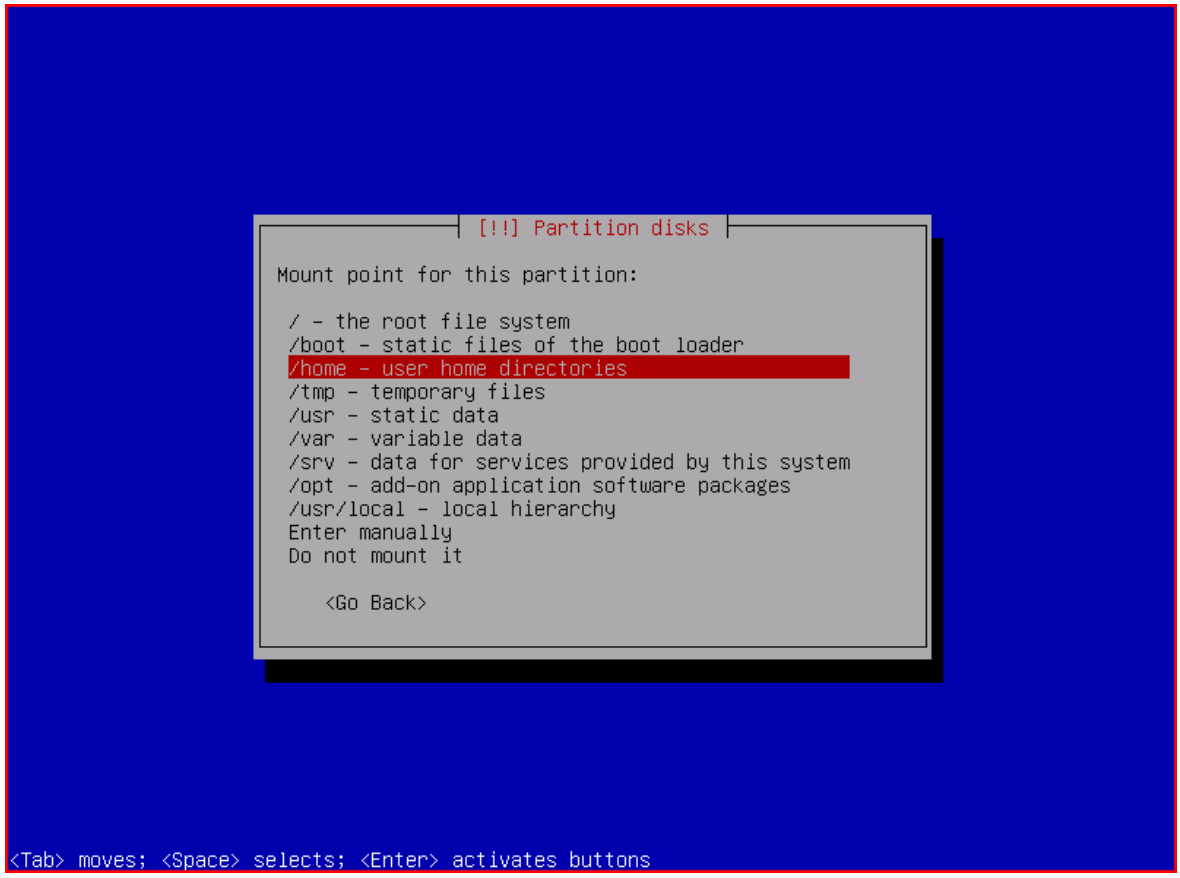


Οδηγία: Επιλέγουμε το σύστημα αρχείων της νέας κατάτμησης να είναι Ext4.

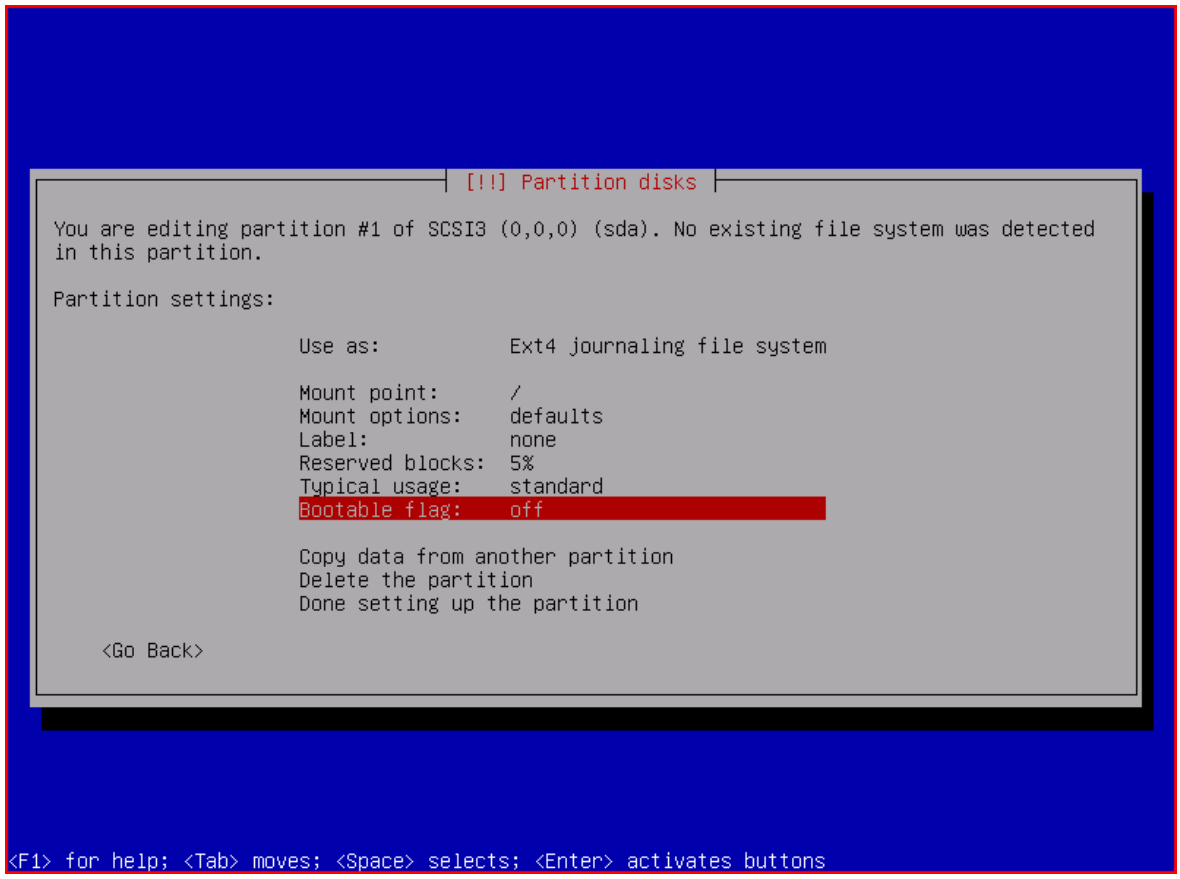


Οδηγία: Εάν αυτό απαιτείται, τροποποιούμε το ήδη καθορισμένο σημείο προσάρτησης, επιλέγοντας από τον πίνακα που εμφανίζεται για το σκοπό αυτό.

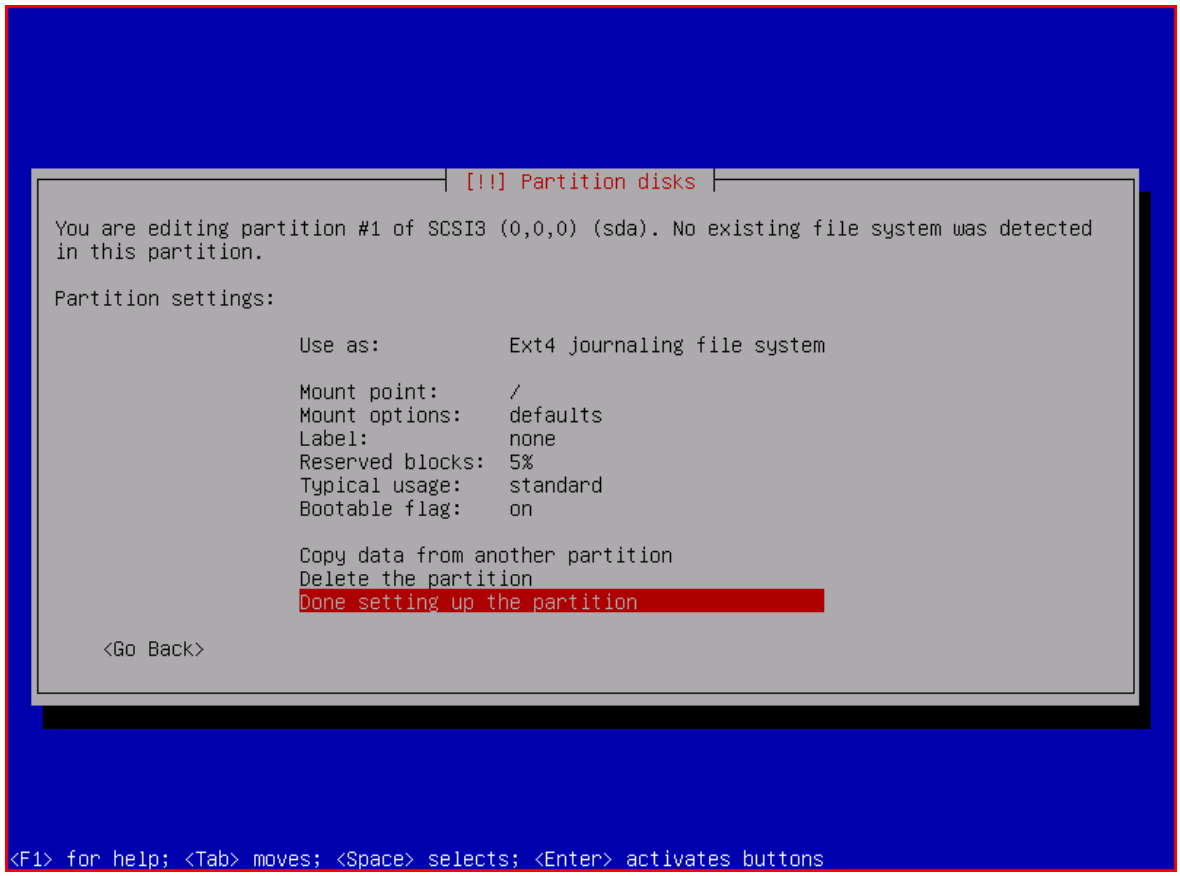




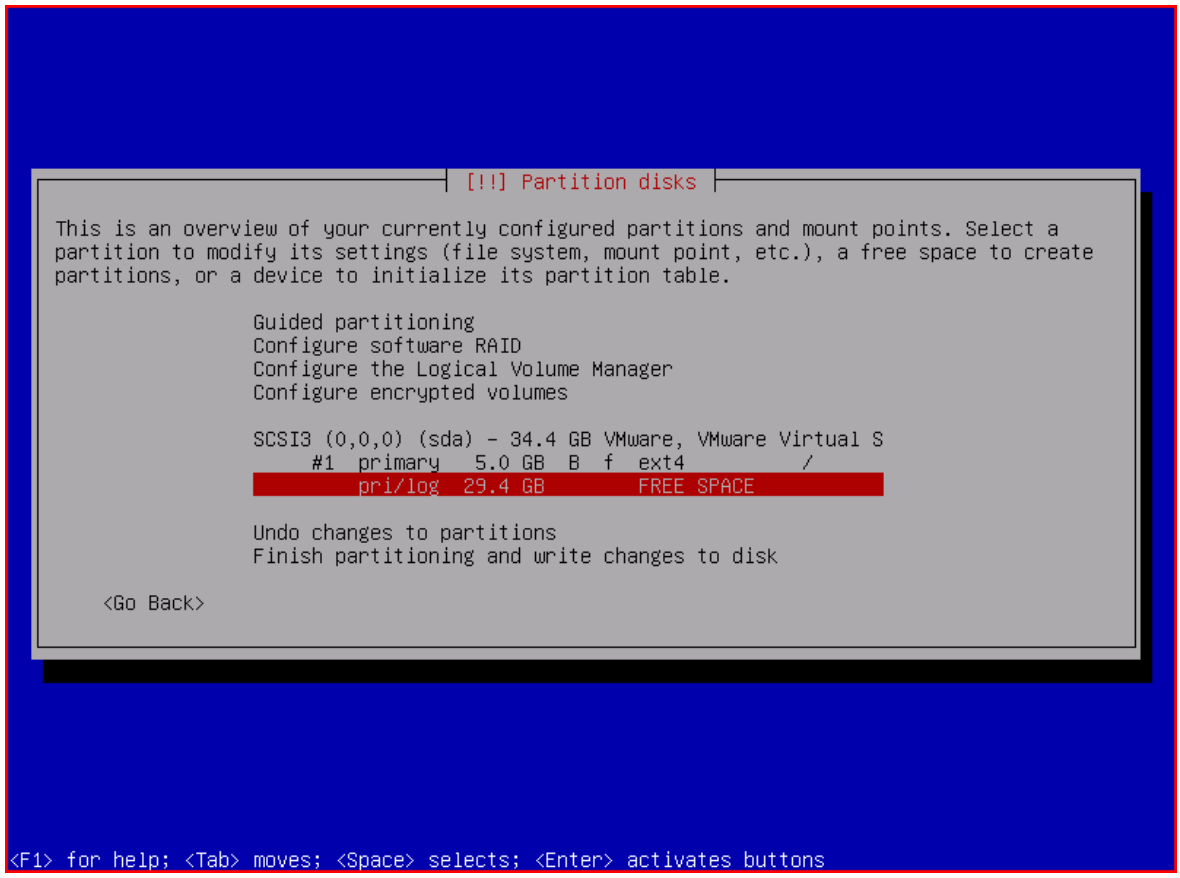
Οδηγία: Μόνο στην περίπτωση της πρώτης κατάτμησης, με σημείο προσάρτησης το ριζικό φάκελο, θέτουμε το Bootable flag από off σε on (αυτή θα είναι η μόνη εκκινήσιμη κατάτμηση).



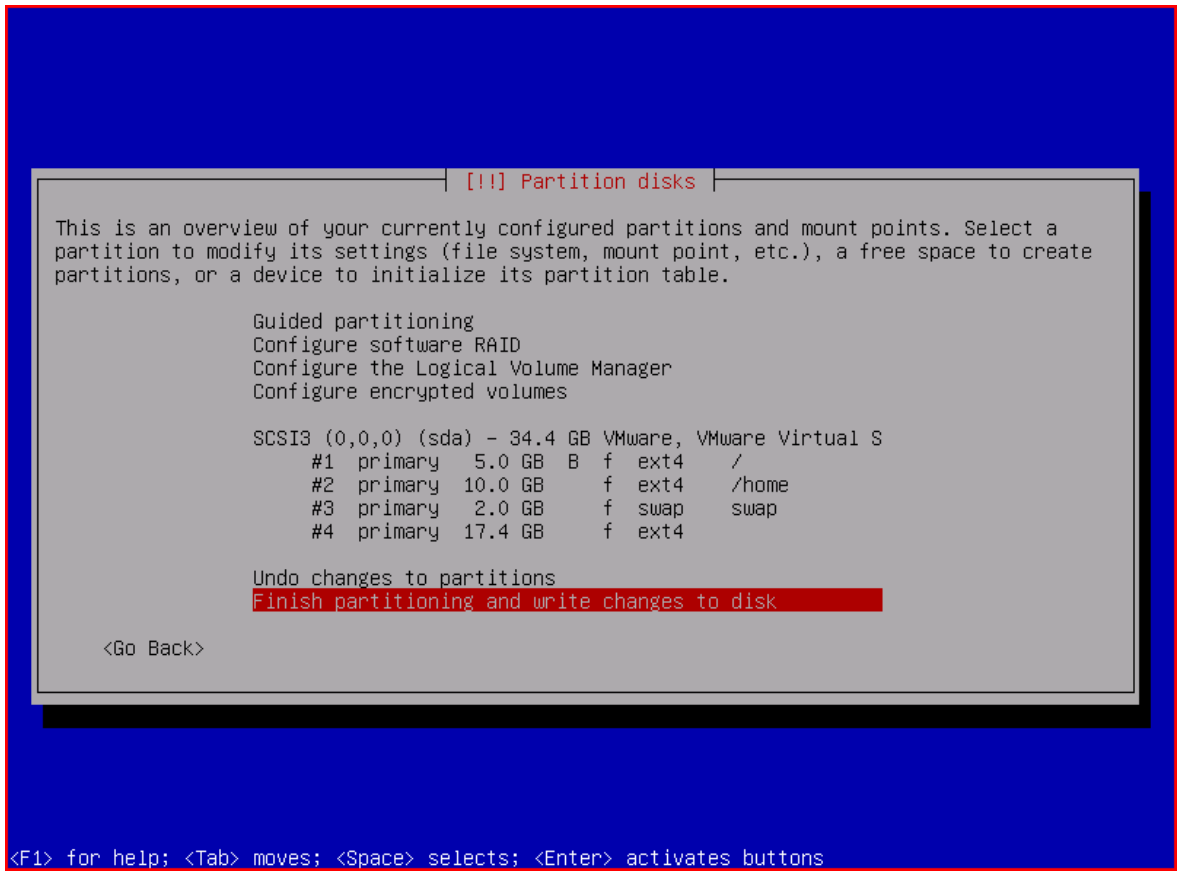
Οδηγία: Όταν ολοκληρώσουμε τον καθορισμό των επιθυμητών ρυθμίσεων για την εκάστοτε κατάτμηση, επιλέγουμε ολοκλήρωση των ρυθμίσεων.



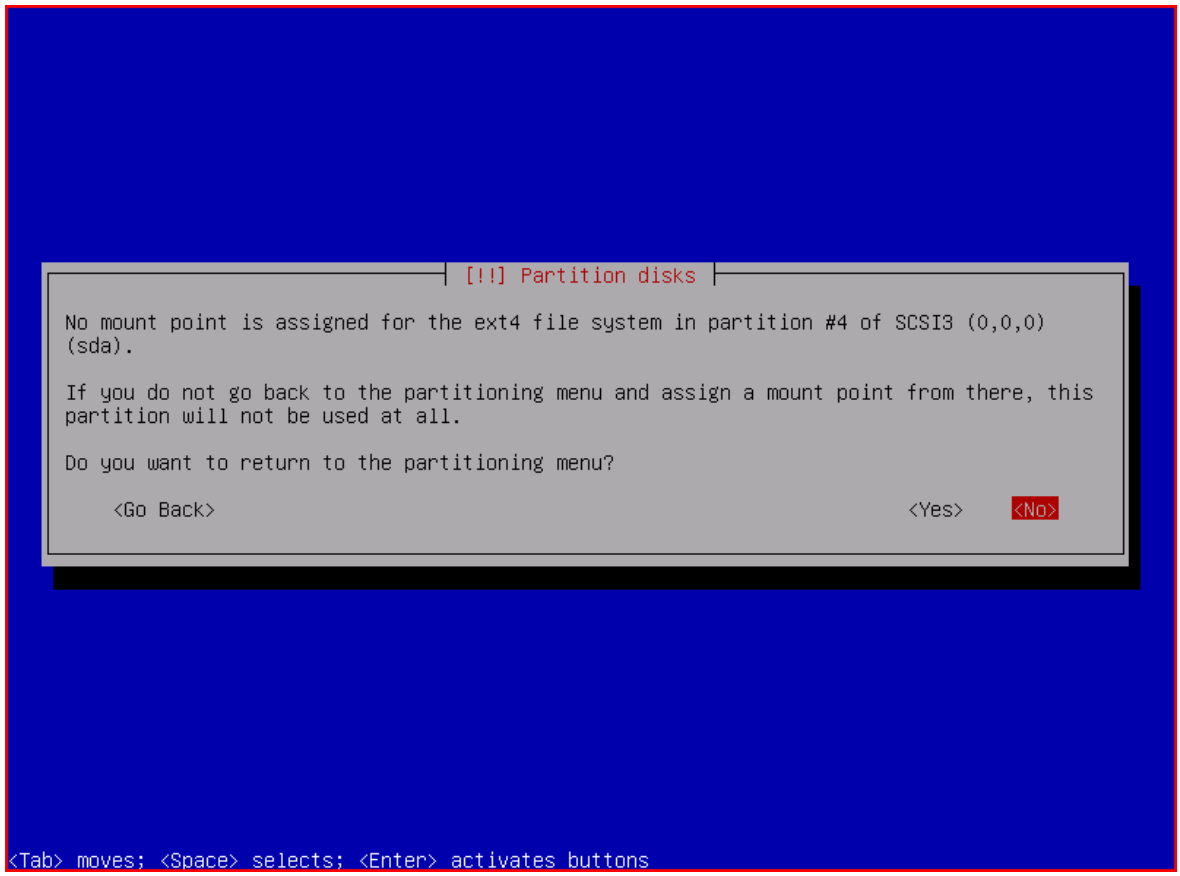
Οδηγία: Επαναλαμβάνουμε τη διαδικασία μέχρι να ολοκληρώσουμε τη ρύθμιση όλων των εμπλεκομένων κατατμήσεων.



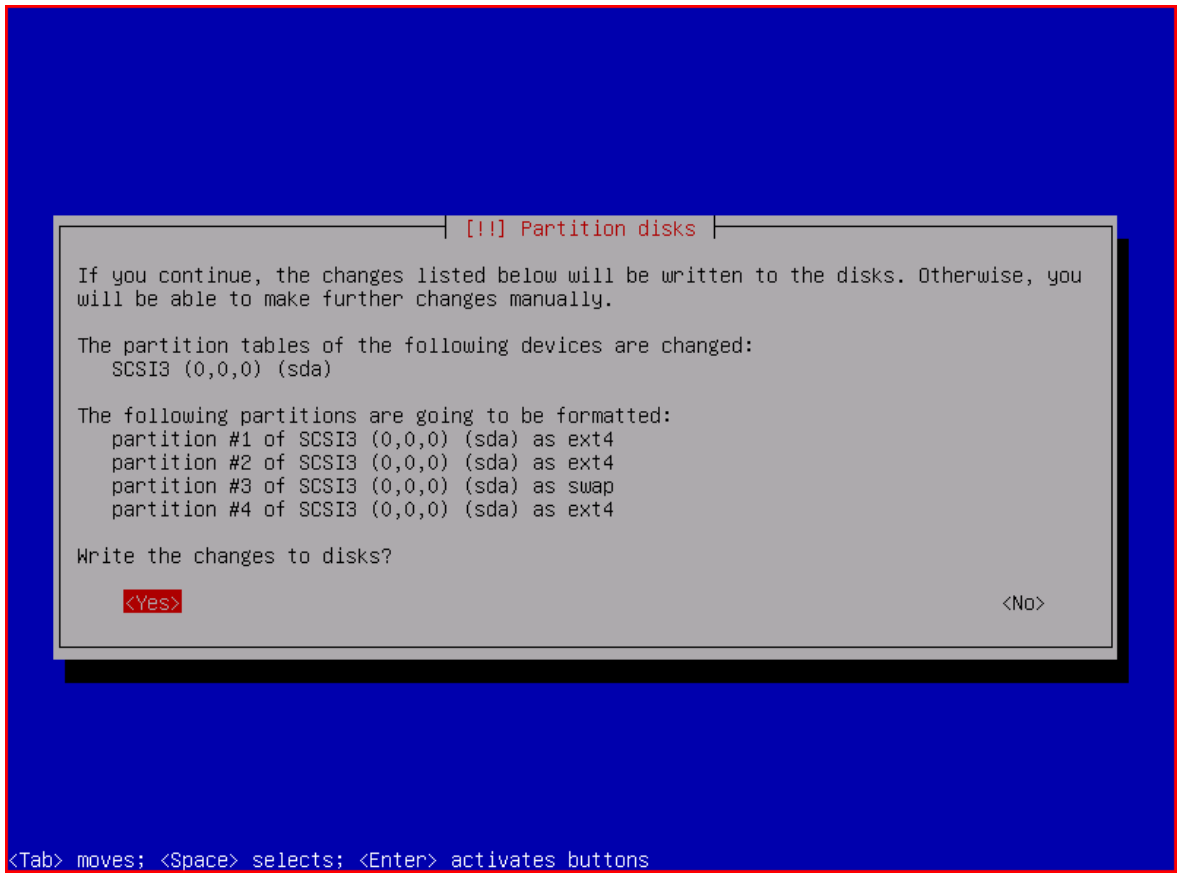
Οδηγία: Έχοντας ολοκληρώσει τον καθορισμό των ρυθμίσεων για όλες τις κατατμήσεις, ελέγχουμε την ορθότητα αυτών και επιλέγουμε ολοκλήρωση της διαδικασίας διαμέρισης και εγγραφή των αλλαγών στο δίσκο.



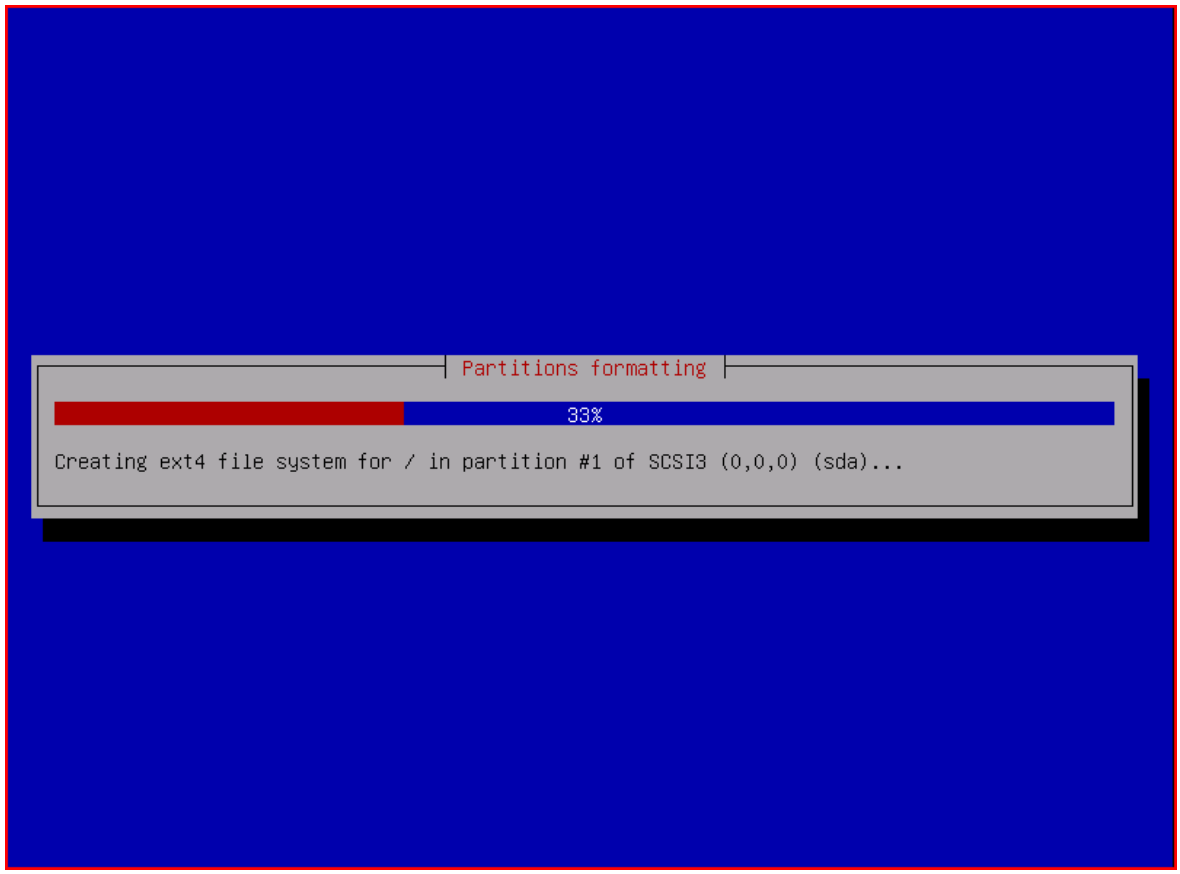
Οδηγία: Ο οδηγός εγκατάστασης μας προειδοποιεί για την έλλειψη σημείου προσάρτησης για την τελευταία κατάτμηση. Αυτό είναι επιθυμητό, συνεπώς επιλέγουμε «No» για να μην επιστρέψουμε στο μενού διαμέρισης.



Οδηγία: Ο οδηγός εγκατάστασης μας ενημερώνει για τις αλλαγές που θα γίνουν στο δίσκο. Πραγματοποιούμε ένα τελευταίο έλεγχο και επιλέγουμε «Yes» για να προβούμε στις αλλαγές.



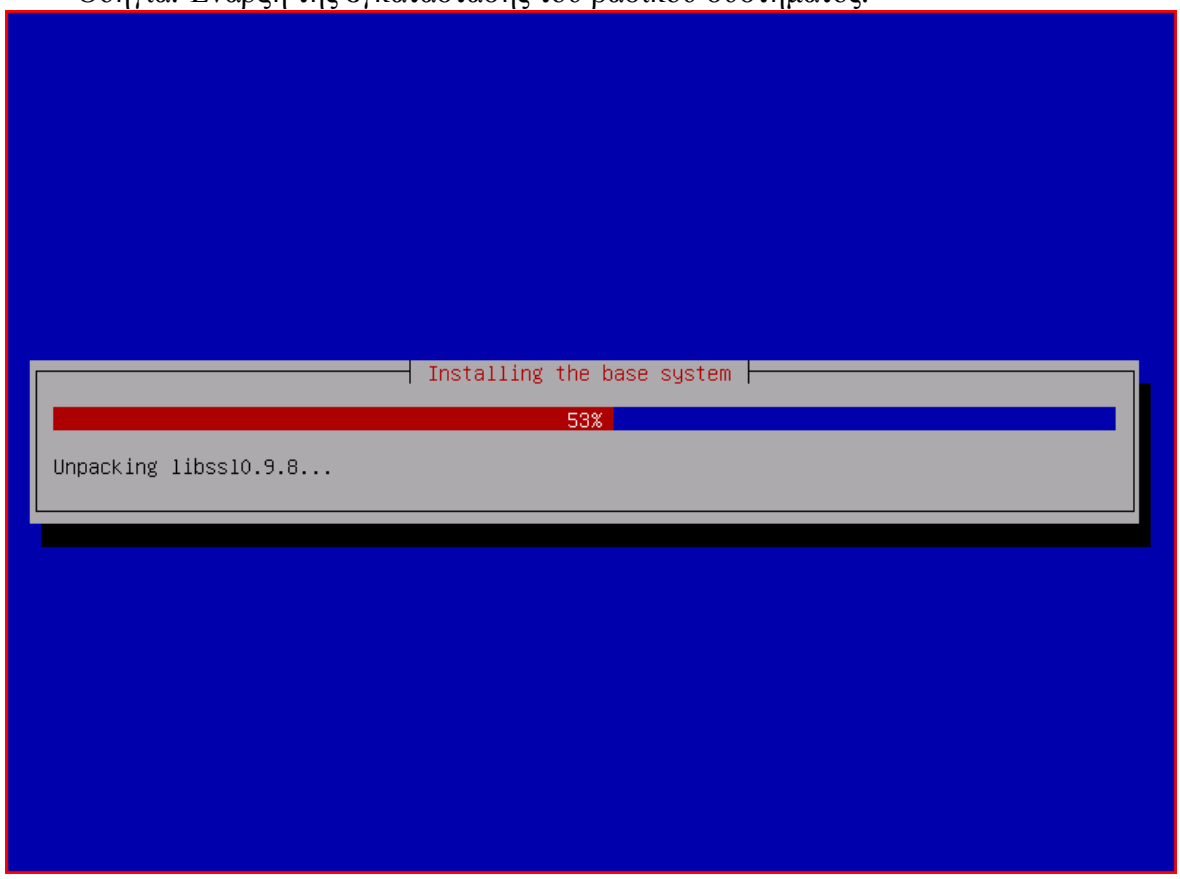
Οδηγία: Γίνεται η διαμέριση του δίσκου με εφαρμογή όλων των ρυθμίσεων που επιλέξαμε.



Βήμα 16: Έναρξη εγκατάστασης βασικού συστήματος

Στο τρέχων βήμα του οδηγού εγκατάστασης, ξεκινά η εγκατάσταση του βασικού συστήματος του Debian GNU/Linux.

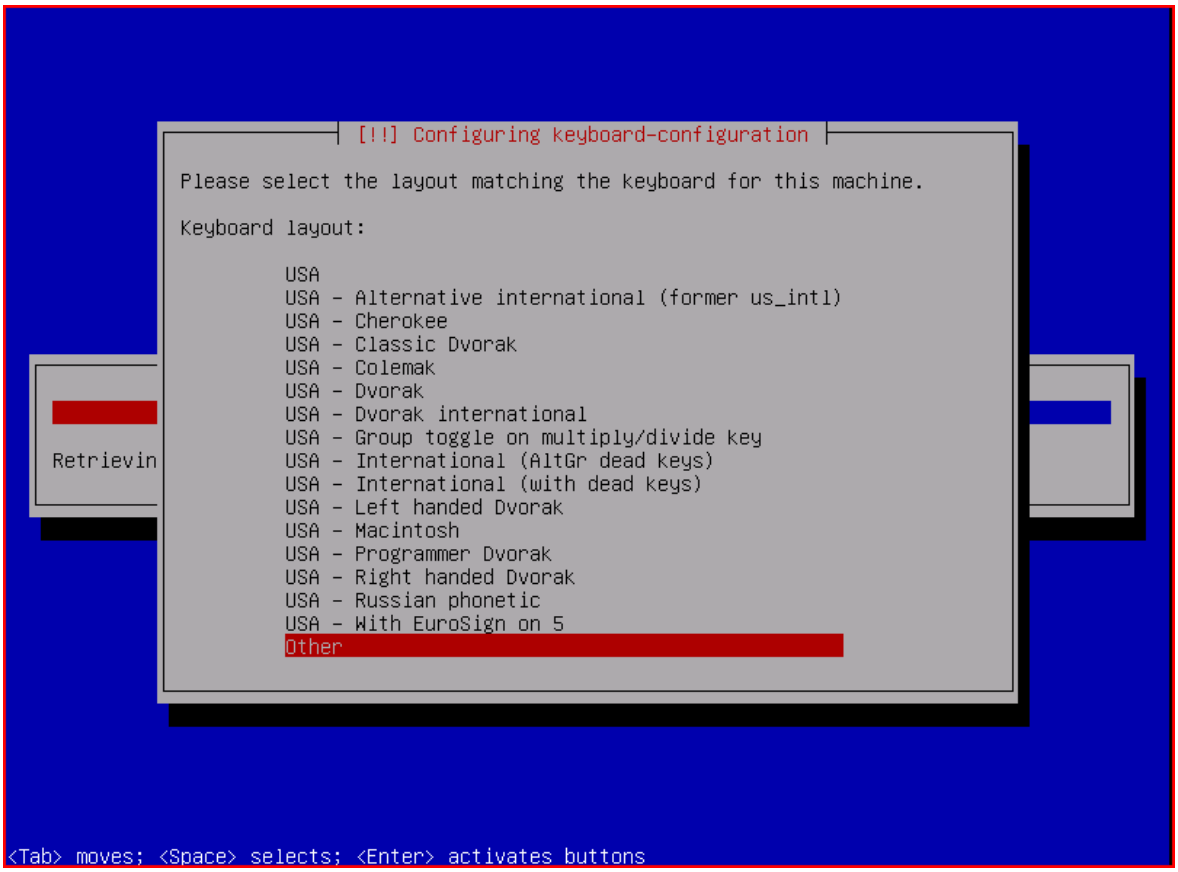
Οδηγία: Έναρξη της εγκατάστασης του βασικού συστήματος.

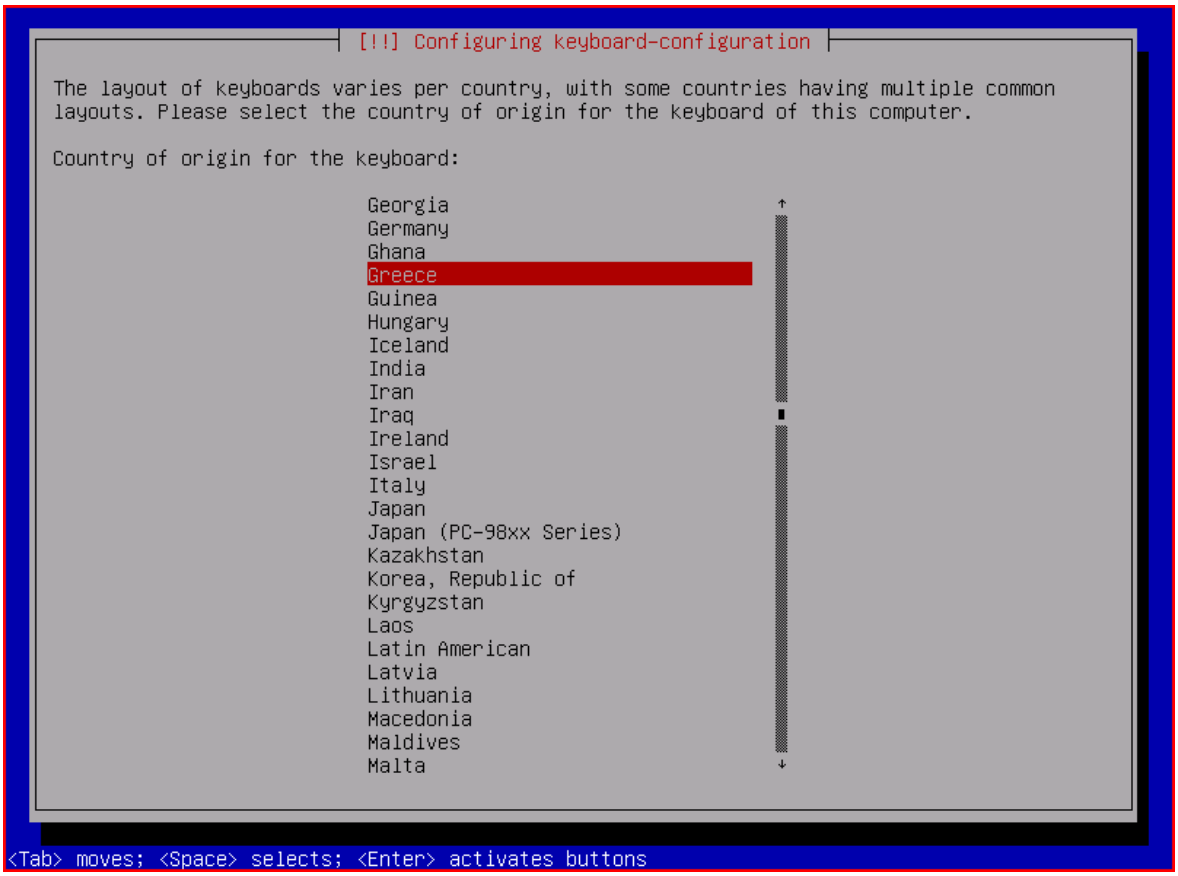


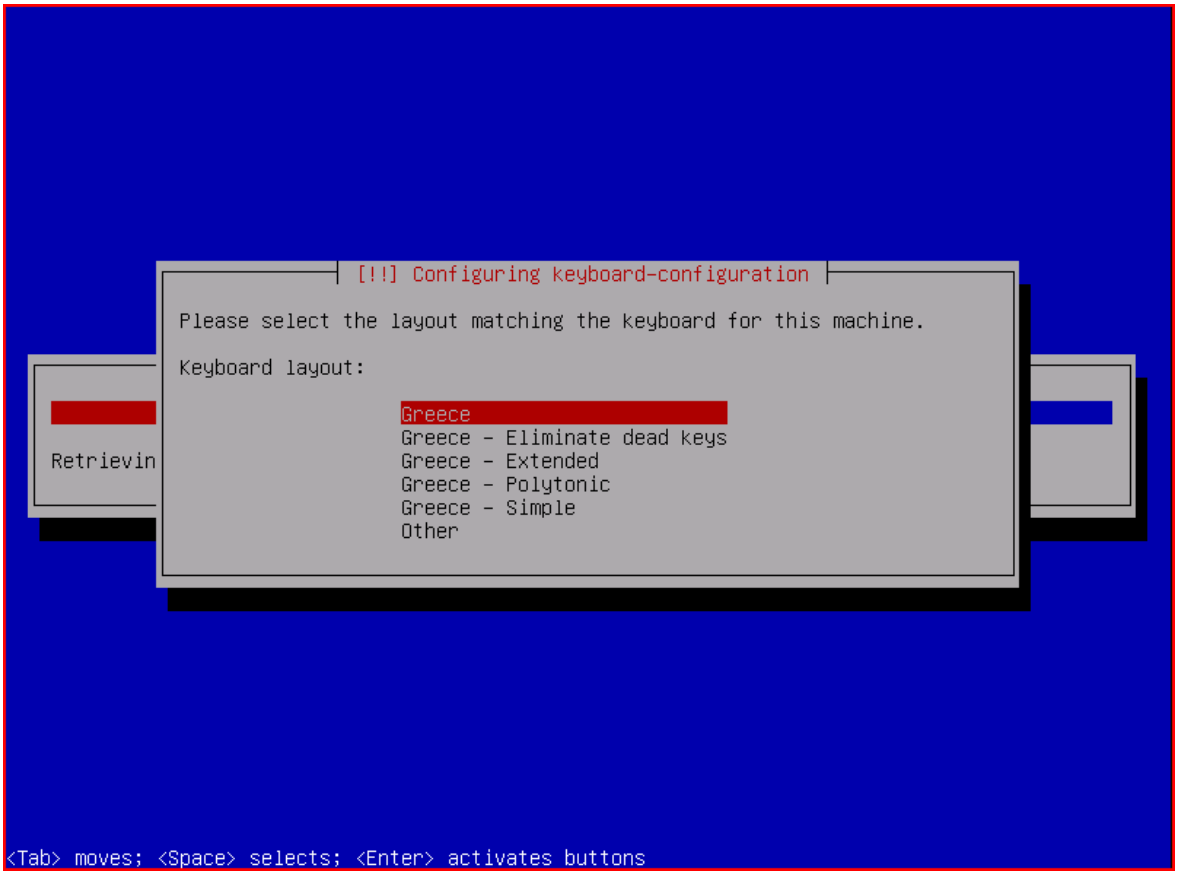
Βήμα 17: Ρυθμίσεις διάταξης πληκτρολογίου

Για το Ελληνικό πληκτρολόγιο, που επιλέχθηκε στο βήμα 5, υπάρχουν διαθέσιμες περισσότερες από μία διατάξεις. Έτσι, θα πρέπει στο παρών βήμα να πραγματοποιηθεί λεπτομερής καθορισμός της συγκεκριμένης παραμέτρου και επιπλέον, να καθοριστεί ο συνδυασμός πλήκτρων με τον οποίο θα γίνεται εναλλαγή μεταξύ της τοπικής και της προκαθορισμένης, Λατινικής διάταξης πληκτρολογίου.

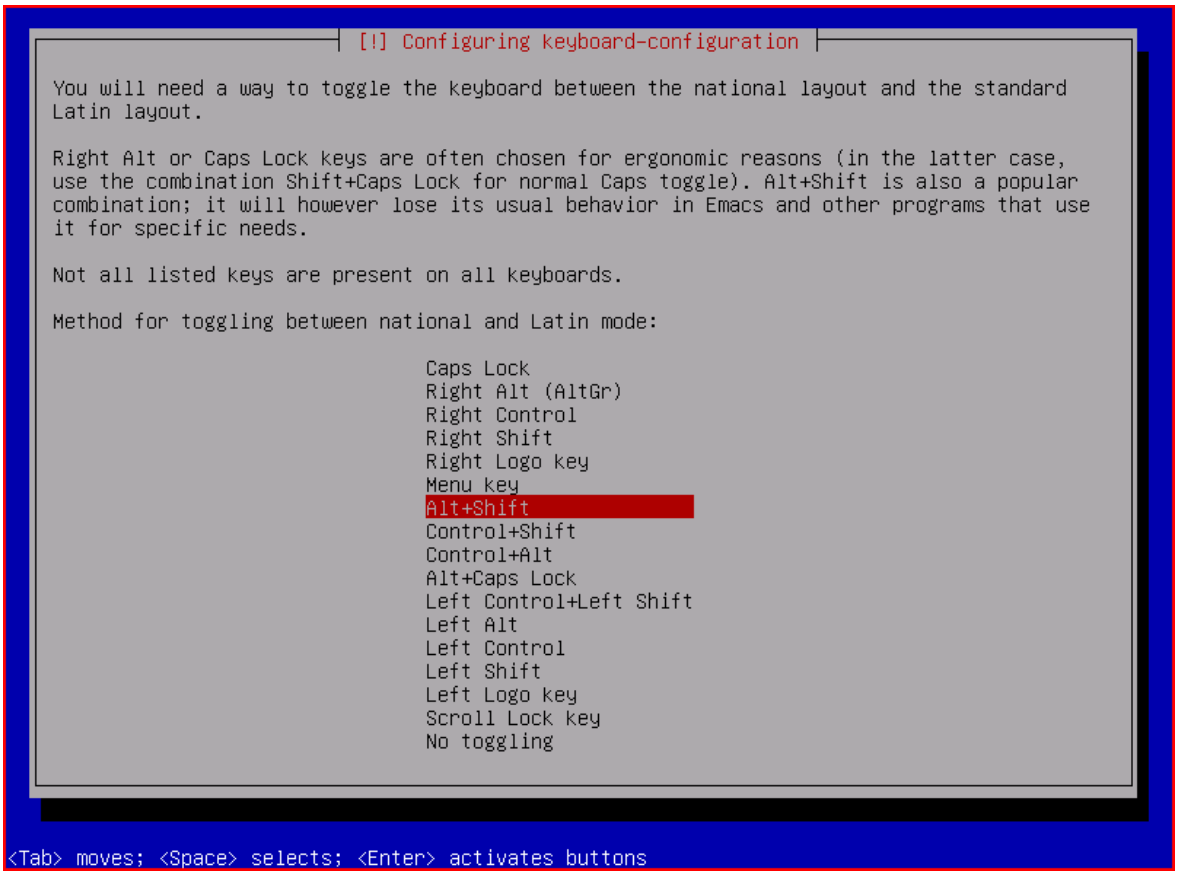
Οδηγία: Επιλέγουμε διαδοχικά «Other» – «Greece» – «Greece».




[!!] Configuring keyboard-configuration
The layout of keyboards varies per country, with some countries having multiple common layouts. Please select the country of origin for the keyboard of this computer.
Country of origin for the keyboard:
Georgia
Germany
Ghana
Greece
Guinea
Hungary
Iceland
India
Iran
Iraq
Ireland
Israel
Italy
Japan
Japan (PC-98xx Series)
Kazakhstan
Korea, Republic of
Kyrgyzstan
Laos
Latin American
Latvia
Lithuania
Macedonia
Maldives
Malta
<Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Configuring keyboard-configuration
Please select the layout matching the keyboard for this machine.
Keyboard layout:
Greece
Greece - Eliminate dead keys
Greece - Extended
Greece - Polytonic
Greece - Simple
Other
Retrievin
<Tab> moves; <Space> selects; <Enter> activates buttons

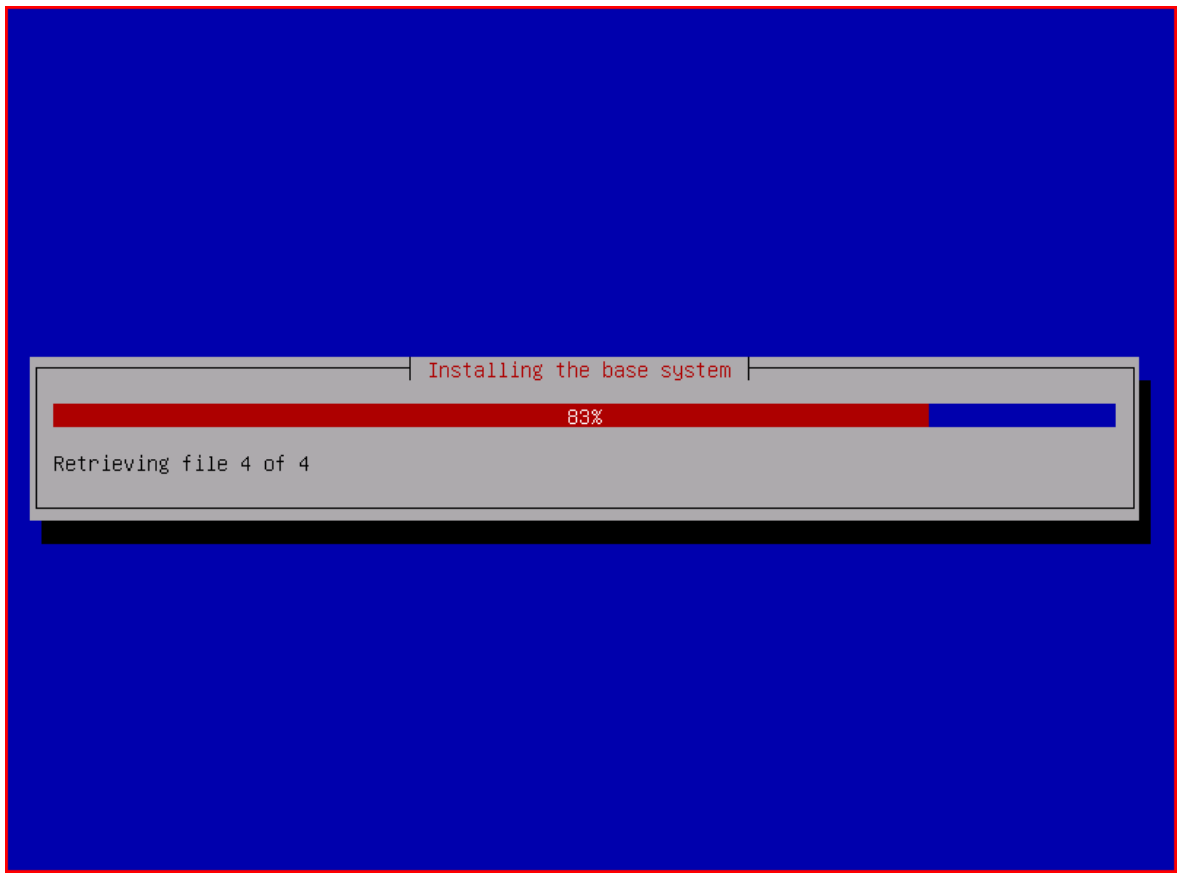
Οδηγία: Επιβεβαιώνουμε την προκαθορισμένη επιλογή του συνδυασμού πλήκτρων «Alt+Shift», για την εναλλαγή μεταξύ της Ελληνικής και της Λατινικής διάταξης πληκτρολογίου.



Βήμα 18: Εξέλιξη εγκατάστασης βασικού συστήματος

Στο βήμα αυτό πραγματοποιείται ένα ακόμη μέρος της συνολικής εγκατάστασης του βασικού συστήματος.

Οδηγία: Εξέλιξη της εγκατάστασης του βασικού συστήματος.



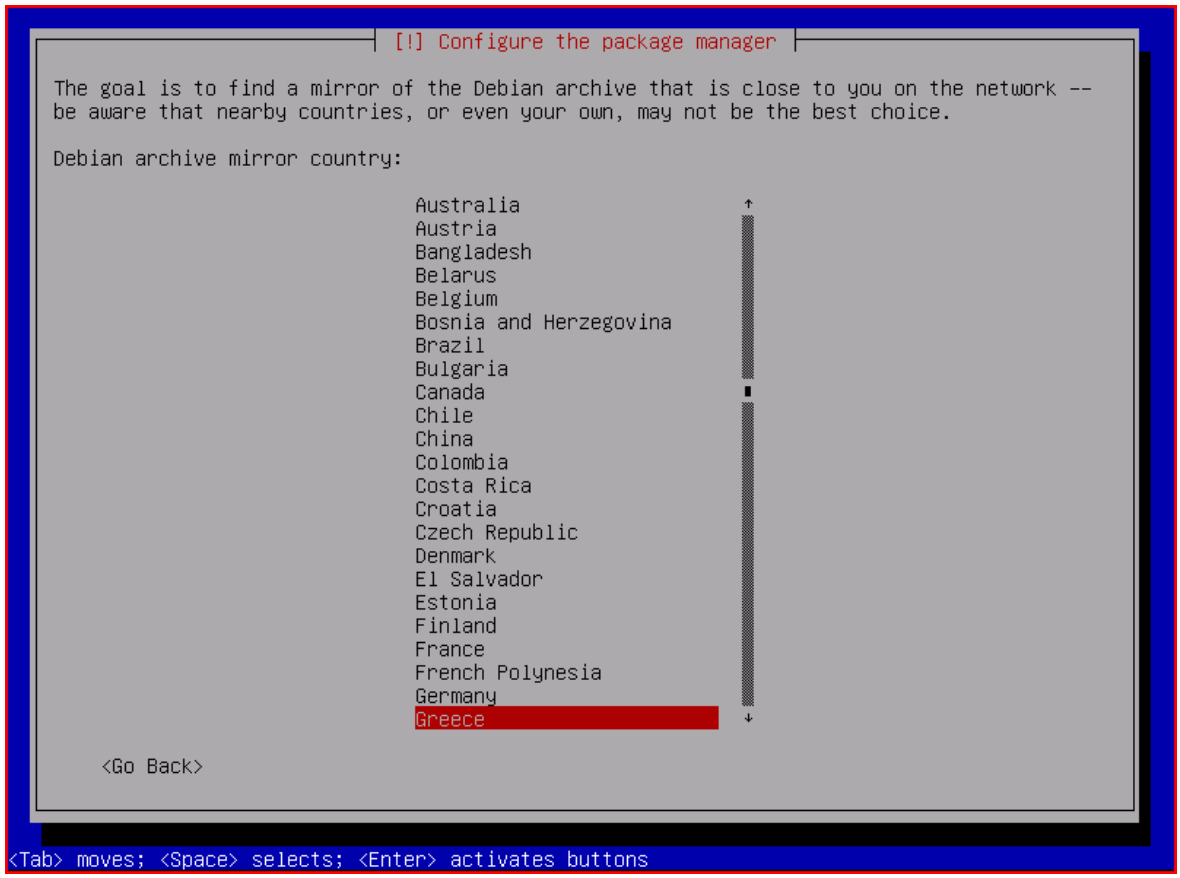
Βήμα 19: Ρύθμιση της εφαρμογής διαχείρισης πακέτων

Ένα από τα βοηθήματα με τα οποία γίνεται η εγκατάσταση εφαρμογών στο Debian GNU/Linux είναι η εφαρμογή διαχείρισης πακέτων (Advanced Package Tool). Η εφαρμογή apt έχει αναπτυχθεί με στόχο την αυτοματοποίηση της διαδικασίας εγκατάστασης των πακέτων και αναλαμβάνει όλα τα σχετικά στάδια:

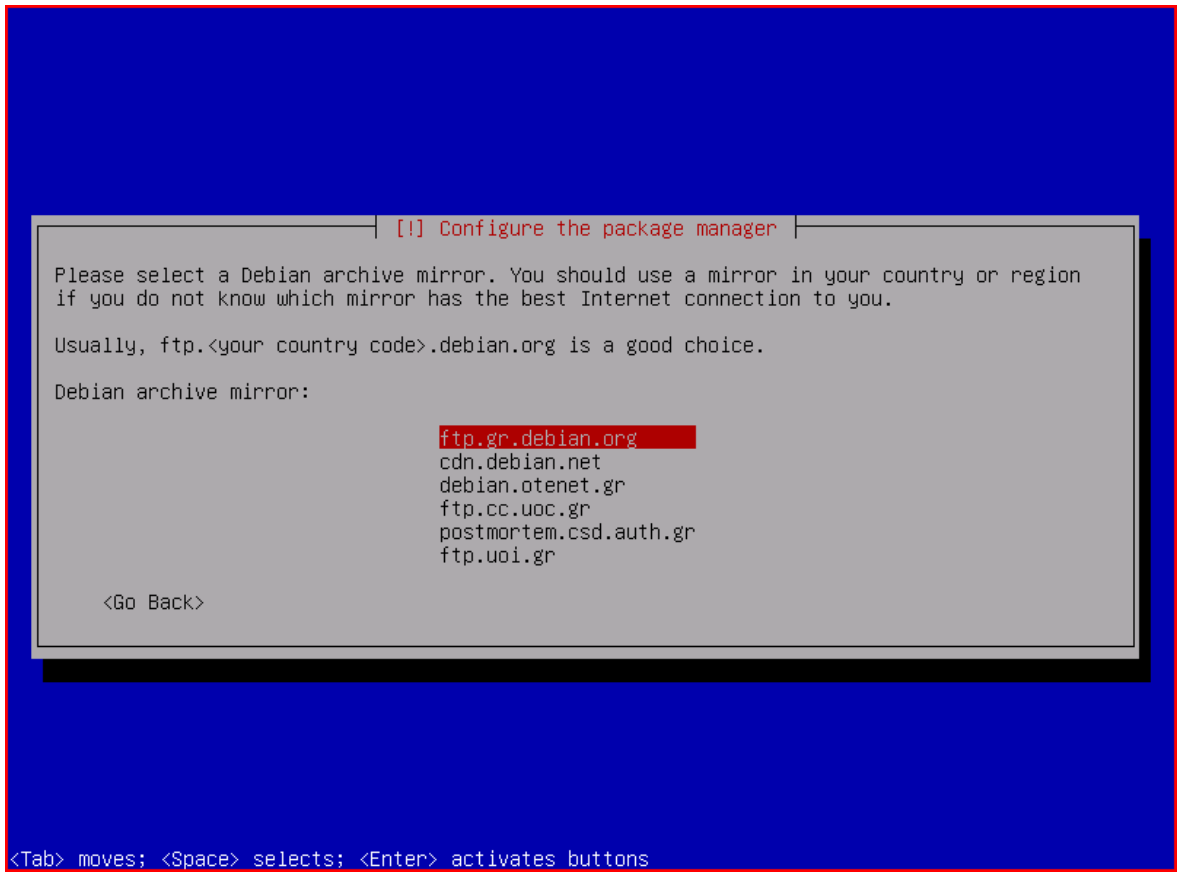
- μεταφόρτωση του προς εγκατάσταση πακέτου
- μεταφόρτωση των εξαρτήσεων του προς εγκατάσταση πακέτου
- εγκατάσταση όλων των πακέτων, με τη σωστή σειρά προτεραιότητας
- ρύθμιση όλου του εμπλεκόμενου λογισμικού

Όπως είναι φυσικό, η συγκεκριμένη εφαρμογή θα πρέπει ρυθμιστεί, ώστε να γνωρίζει από πού μπορεί να ανακτήσει τα προς εγκατάσταση πακέτα. Η ρύθμιση αυτή θα πραγματοποιηθεί στο τρέχων βήμα της διαδικασίας εγκατάστασης, με την επιλογή του βασικού καθρέφτη του αποθετηρίου αναβαθμίσεων. Μάλιστα, για να πραγματοποιούνται με τη μέγιστη δυνατή ταχύτητα οι μεταφορτώσεις που απαιτούνται στη συνέχεια, ο παραπάνω καθρέφτης θα οριστεί να βρίσκεται στη χώρα στην οποία είναι εγκατεστημένος ο εξυπηρετητής (μετά την ολοκλήρωση της εγκατάστασης θα χρειαστεί να ρυθμιστούν επιπλέον παράμετροι στο σχετικό αρχείο ρυθμίσεων της εν λόγω εφαρμογής).

Οδηγία: Επιλέγουμε τη γεωγραφική τοποθεσία, στην οποία είναι εγκατεστημένος ο εξυπηρετητής (με δεδομένο ότι αυτός βρίσκεται στην Ελλάδα, επιλέγουμε «Greece»).



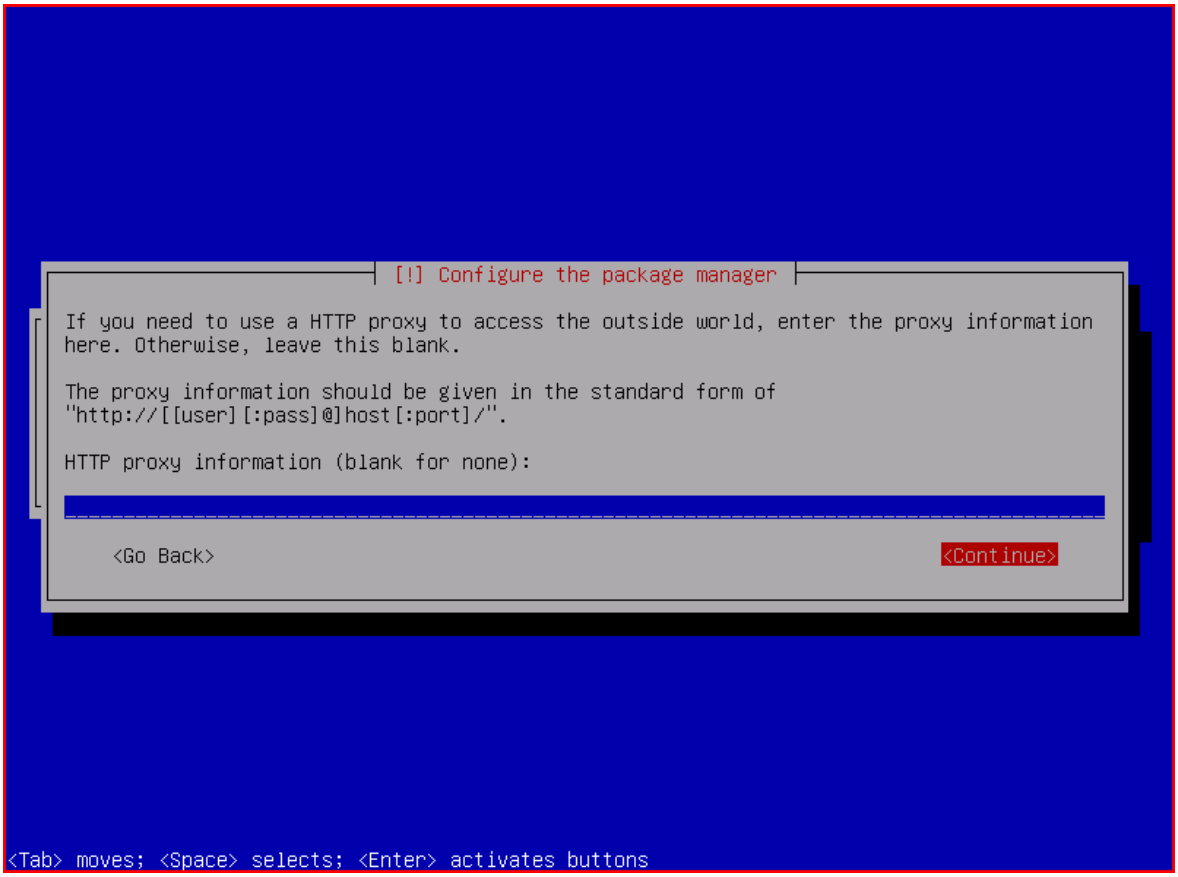
Οδηγία: Επιβεβαιώνουμε την επιλογή του προκαθορισμένου καθρέφτη αποθετηρίου αναβαθμίσεων της συγκεκριμένης γεωγραφικής τοποθεσίας.



Βήμα 20: Εισαγωγή στοιχείων διαμεσολαβητή HTTP

Εάν ο εξυπηρετητής είναι εγκατεστημένος σε δίκτυο, στο οποίο λειτουργεί τοπικός διαμεσολαβητής HTTP (HTTP proxy server), τότε θα πρέπει σε αυτό το βήμα να οριστούν οι σχετικές πληροφορίες.

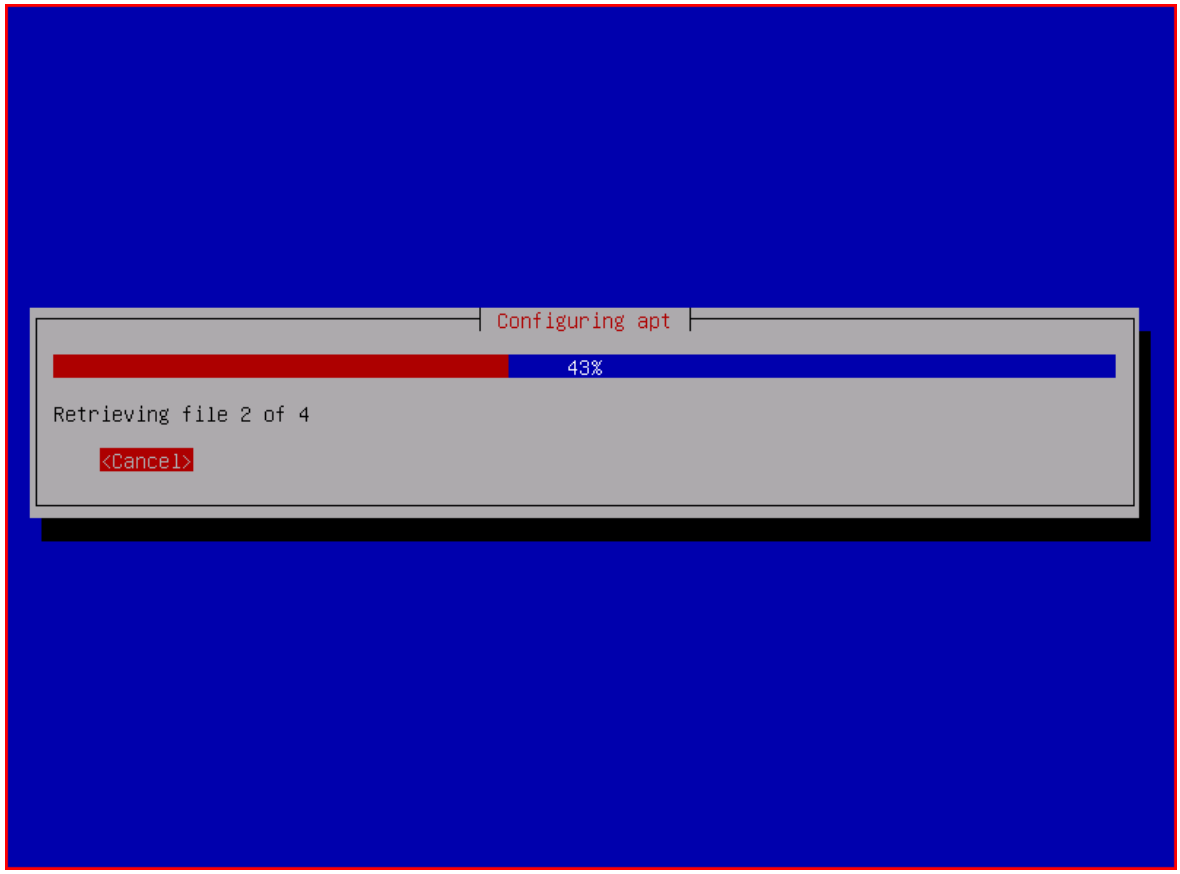
Οδηγία: Εάν αυτό απαιτείται, εισάγουμε τα στοιχεία πρόσβασης στον τοπικό διαμεσολαβητή HTTP.



Βήμα 20: Επικαιροποίηση της βάσης δεδομένων της εφαρμογής apt

Γίνεται ενημέρωση της τοπικής βάσης δεδομένων της εφαρμογής διαχείρισης πακέτων, σχετικά με τα πακέτα που είναι διαθέσιμα στον καθρέφτη αποθετηρίου αναβαθμίσεων που έχουμε επιλέξει.

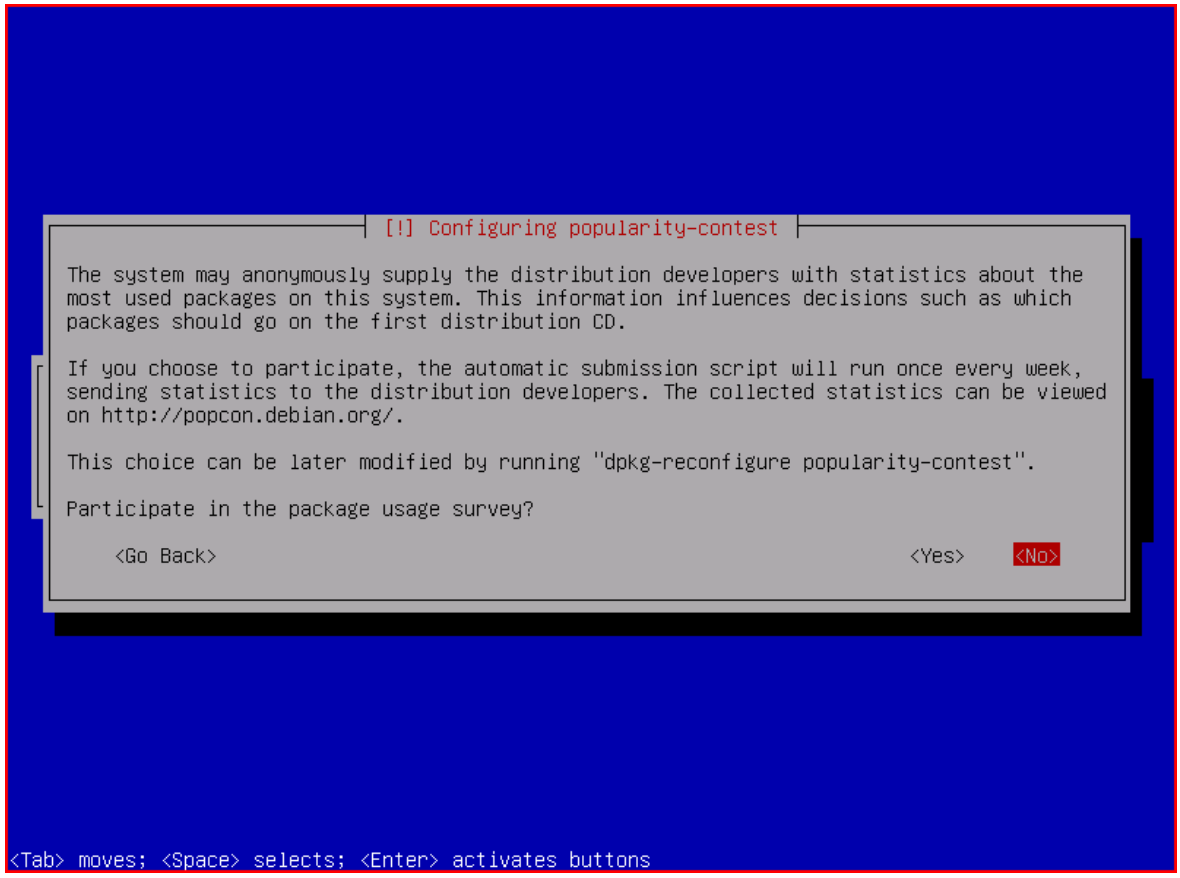
Οδηγία: Γίνεται επικαιροποίηση της βάσης δεδομένων της εφαρμογής apt.



Βήμα 21: Ρύθμιση επιλογής συμμετοχής στην έρευνα χρήσης πακέτων

Για την καλύτερη υποστήριξη της ανάπτυξης του εμπλεκόμενου λογισμικού, έχει αποφασιστεί από την ομάδα ανάπτυξης του Debian GNU/Linux να γίνεται εβδομαδιαίως μια ανώνυμη συλλογή πληροφοριών σχετικά με τα χρησιμοποιούμενα πακέτα. Στο παρών βήμα θα πρέπει να καθοριστεί αν ο συγκεκριμένος εξυπηρετητής θα συμμετάσχει ή όχι στην εν λόγω έρευνα.

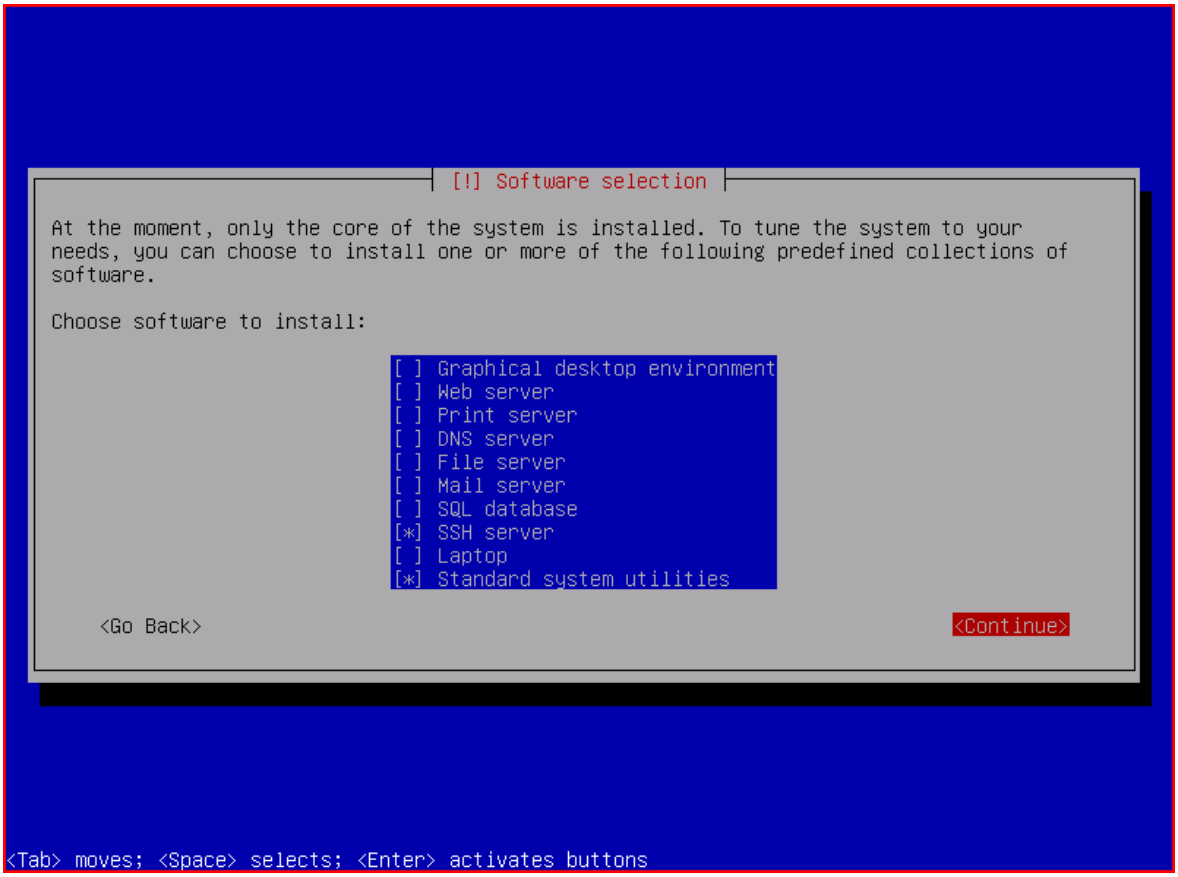
Οδηγία: Καθορίζουμε την επιλογή ή όχι συμμετοχής στην ανώνυμη έρευνα χρήσης πακέτων.



Βήμα 22: Επιλογή των προς εγκατάσταση μερών του συστήματος

Στο τρέχων βήμα προσφέρεται στο χρήστη η δυνατότητα για αυτοματοποιημένη εγκατάσταση πολλών από τις εφαρμογές παροχής των υπηρεσιών του εξυπηρετητή. Παρότι η εκμετάλλευση της δυνατότητας αυτής θα απλοποιούσε τη διαδικασία εγκατάστασης του τρέχοντος οδηγού, εντούτοις για να υπάρχει μεγαλύτερος έλεγχος πάνω στο τι εγκαθίσταται και τι όχι, καθώς και στο ποιες θα είναι οι ακριβείς ρυθμίσεις του εμπλεκόμενου λογισμικού, σε αυτή τη φάση θα εγκατασταθούν μόνο τα πακέτα του βασικού συστήματος. Σε μεταγενέστερο βήμα, όλο το υπόλοιπο απαιτούμενο λογισμικό θα εγκατασταθεί χειρωνακτικά, πάνω από μια ασφαλή σύνδεση, για την επίτευξη της οποίας θα επιλέξουμε να εγκατασταθεί και το λογισμικό της υπηρεσίας SSH.

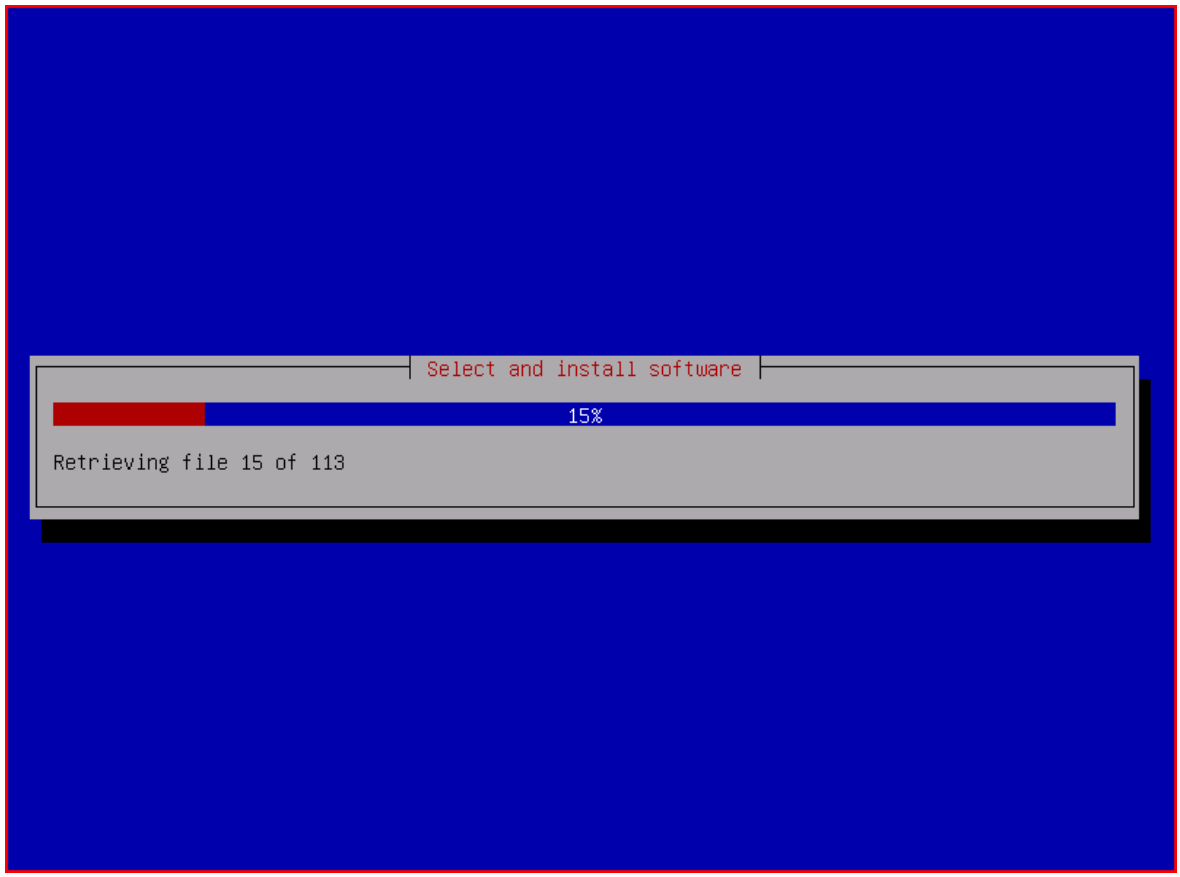
Οδηγία: Επιλέγουμε την εγκατάσταση του βασικού συστήματος, καθώς και του διακομιστή SSH.



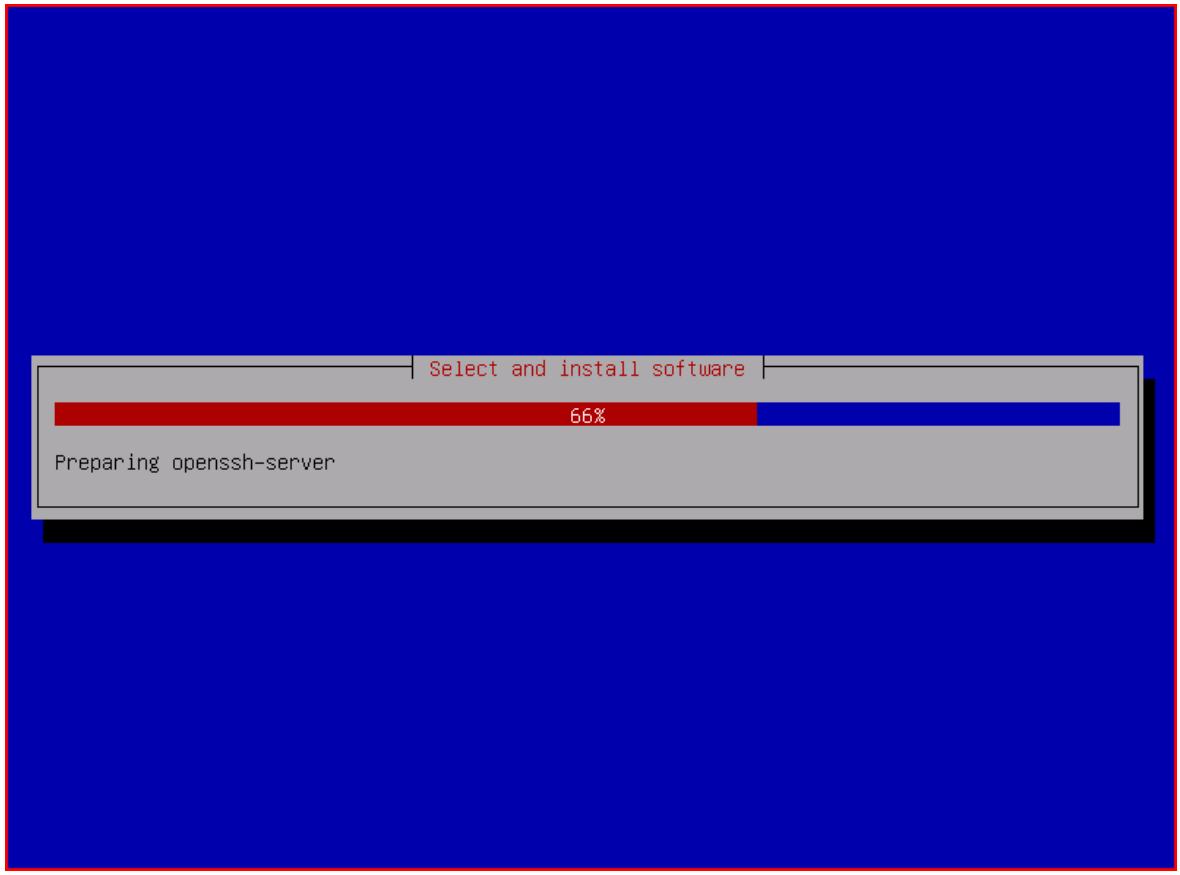
Βήμα 23: Εγκατάσταση του συστήματος

Στο τρέχων βήμα πραγματοποιείται η μεταφόρτωση και η εγκατάσταση όλου του επιλεγμένου λογισμικού.

Οδηγία: Γίνεται μεταφόρτωση των πακέτων από τον καθρέφτη αποθετηρίου αναβαθμίσεων στο σύστημά μας.



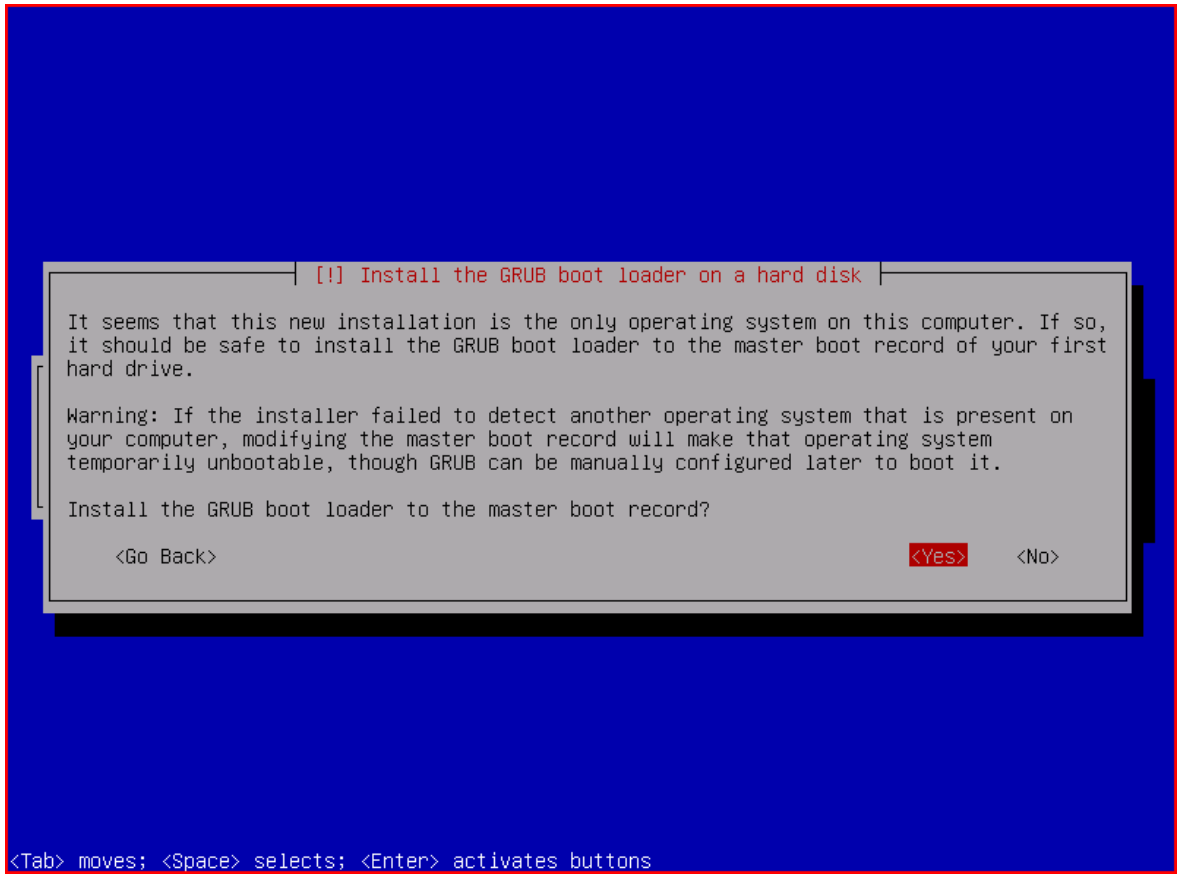
Οδηγία: Γίνεται εγκατάσταση όλου του επιλεγμένου λογισμικού.



Βήμα 24: Εγκατάσταση εκκινητή συστήματος GRUB

Η εγκατάσταση του βασικού μέρους του λειτουργικού συστήματος έχει μόλις ολοκληρωθεί και το μόνο που απομένει για να είναι δυνατή η εκκίνηση του συστήματος με αυτό, είναι η εγκατάσταση του σχετικού λογισμικού εκκίνησης. Το Debian GNU/Linux χρησιμοποιεί εξ' ορισμού τον εκκινητή συστήματος GRUB, ο οποίος και θα εγκατασταθεί στην κύρια εγγραφή εκκίνησης (Master Boot Record) του δίσκου.

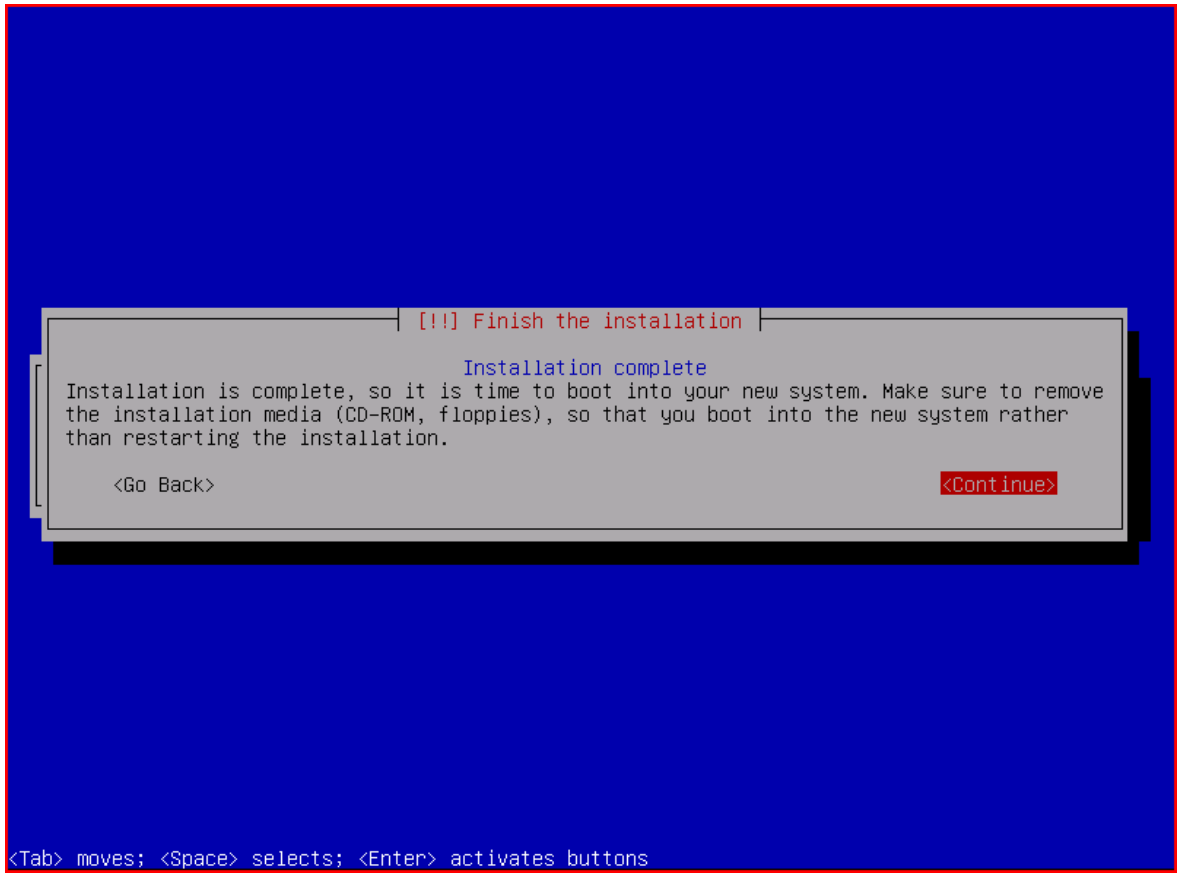
Οδηγία: Επιλέγουμε την εγκατάσταση του εκκινητή συστήματος GRUB στην κύρια εγγραφή εκκίνησης (Master Boot Record) του δίσκου.



Βήμα 25: Επανεκκίνηση συστήματος

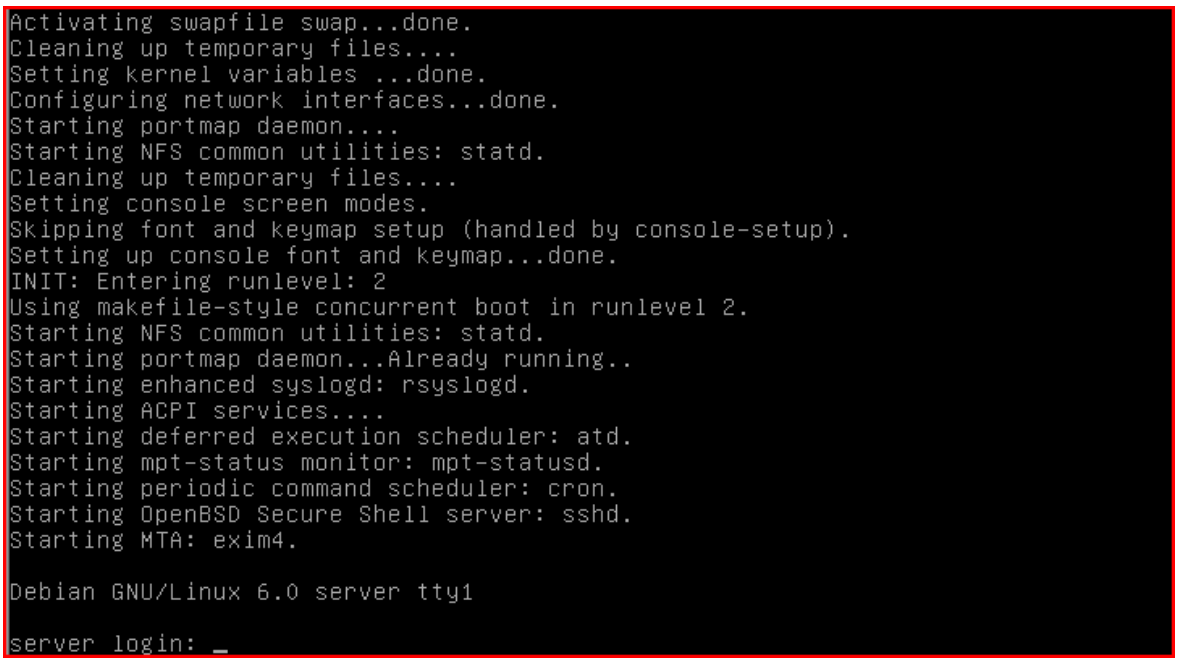
Με την εγκατάσταση του λογισμικού εκκίνησης, το πρώτο μέρος του οδηγού της παρούσας πτυχιακής εργασίας, που αφορά στην εγκατάσταση του βασικού μέρους του λειτουργικού συστήματος Debian GNU/Linux του εξυπηρετητή, έχει ολοκληρωθεί. Για να τεθεί ο εξυπηρετητής σε κανονική λειτουργία, θα πρέπει να αφαιρεθεί ο οπτικός δίσκος με τον οποίο έγινε η εγκατάσταση του Debian GNU/Linux και να επανεκκινηθεί το σύστημα. Βέβαια, στην περίπτωση που αυτό απαιτείται, θα πρέπει να επιλεγεί να εκκινήσει το σύστημα από το σκληρό δίσκο στον οποίο έγινε η εγκατάσταση και όχι από τον οδηγό του οπτικού δίσκου αυτής όπως πριν.

Οδηγία: Αφαιρούμε τον οπτικό δίσκο της εγκατάστασης και επιλέγουμε «Continue» για να ολοκληρωθεί η εγκατάσταση και να γίνει επανεκκίνηση του συστήματος.



Βήμα 26: Πέρας εγκατάστασης βασικού συστήματος

Μετά την ολοκλήρωση της επανεκκίνησης του συστήματος βρισκόμαστε αντιμέτωποι με την οθόνη υποδοχής χρήστη, στην οποία έχουμε τη δυνατότητα να χρησιμοποιήσουμε τα διαπιστευτήρια ενός εκ των δύο χρηστών που δημιουργήθηκαν στα προηγούμενα βήματα και να συνδεθούμε στον εξυπηρετητή.



Επειδή, όμως, η συγκεκριμένη σύνδεση με το απομακρυσμένο σύστημα δεν είναι ασφαλής, είναι απαραίτητο να χρησιμοποιηθεί η υπηρεσία SSH (βήμα 22), ώστε να γίνουν τα επόμενα βήματα εγκατάστασης με τη μέγιστη δυνατή ασφάλεια. Έτσι, στο αμέσως επόμενο κεφάλαιο, θα γίνει αρχικά αναφορά στον τρόπο χρήσης του συγκεκριμένου πρωτοκόλλου για την επίτευξη μιας ασφαλούς σύνδεσης με τον εξυπηρετητή και έπειτα θα συνεχιστεί η εγκατάσταση και παραμετροποίηση του υπόλοιπου λογισμικού που απαιτείται για τη λειτουργία, εποπτεία και διαχείριση του συστήματος.

ΚΕΦΑΛΑΙΟ 3

Στο αμέσως προηγούμενο κεφάλαιο πραγματοποιήθηκε η εγκατάσταση του βασικού λειτουργικού συστήματος Debian GNU/Linux, καθώς και της προαιρετικής υπηρεσίας SSH, ώστε ο εξυπηρετητής να είναι σε θέση να παράσχει στο χρήστη τη δυνατότητα ασφαλούς σύνδεσης μαζί του. Μια τέτοιου είδους σύνδεση, με χρήση της διαθέσιμης πλέον υπηρεσίας SSH, είναι απαραίτητο να εξασφαλιστεί, ώστε να διατηρηθεί σε υψηλά επίπεδα η ασφάλεια του συστήματος στα επόμενα βήματα του παρόντος οδηγού. Έτσι, στο παρών κεφάλαιο αρχικά θα παρουσιαστεί η διαδικασία που απαιτείται για να επιτευχθεί μια σύνδεση ασφαλούς κελύφους και ακολούθως θα συνεχιστεί η εγκατάσταση και παραμετροποίηση όλου του υπόλοιπου λογισμικού που απαιτείται, ώστε να παρέχονται με ασφάλεια οι υπηρεσίες του εξυπηρετητή διαδικτύου.

Σύνδεση ασφαλούς κελύφους (SSH)

Μέχρι το τρέχων βήμα ο ίδιος ο εξυπηρετητής δεν είχε τη δυνατότητα να παρέχει υπηρεσίες, συνεπώς κάποιο άλλο πληροφοριακό σύστημα μας παρείχε τη δυνατότητα πρόσβασης σε αυτόν. Αυτό όμως σημαίνει ότι, ανεξαρτήτως του τύπου της πρόσβασης στον εξυπηρετητή, οι διαμεταγωγές δεδομένων που έλαβαν χώρα ήταν εκτεθειμένες σε τρίτους, όπως για παράδειγμα το προσωπικό του κέντρου δεδομένων όπου βρίσκονται εγκατεστημένα τα δύο πληροφοριακά συστήματα (ο εξυπηρετητής και το σύστημα που παρέχει την πρόσβαση σε αυτόν). Σε υλοποιήσεις όπου χρησιμοποιούνται πρωτόκολλα σύνδεσης που δεν υποστηρίζουν την κρυπτοποίηση των μεταφερομένων δεδομένων, το επίπεδο της παρεχόμενης ασφάλειας είναι σαφώς χαμηλότερο και οι διαμεταγωγές είναι εκτεθειμένες ακόμα και σε χρήστες πληροφοριακών συστημάτων που μπορεί να βρίσκονται οπουδήποτε στην υφήλιο! Βέβαια, σε οποιαδήποτε μη ασφαλή σύνδεση είναι εκτεθειμένα σε τρίτους ακόμη και τα διαπιστευτήρια των χρηστών, που τους παρέχουν την πρόσβαση στο πληροφοριακό σύστημα. Έτσι, γίνεται απόλυτα ξεκάθαρη η επιτακτική ανάγκη υιοθέτησης μιας ασφαλέστερης λύσης.

Με στόχο την ικανοποίηση αυτής της ανάγκης έχει σχεδιαστεί το πρωτόκολλο SSH (Secure SHell) [84], το οποίο υποστηρίζει απομακρυσμένες συνδέσεις με ασφάλεια. Έχει δημιουργηθεί ώστε να είναι σε θέση να παρέχει τη δυνατότητα ασφαλούς μεταφοράς

δεδομένων, απομακρυσμένων υπηρεσιών κελύφους ή εκτέλεσης εντολών, καθώς και άλλων ασφαλών υπηρεσιών δικτύου μεταξύ δύο υπολογιστών τους οποίους συνδέει με μια ασφαλή σύνδεση τύπου εξυπηρετητή - πελάτη. Αναπτύχθηκε ως αντικαταστάτης του Telnet [85], καθώς και άλλων μη ασφαλών πρωτοκόλλων, όπως τα rsh και rexec, και πλέον χρησιμοποιείται ευρέως σε όλες σχεδόν τις πλατφόρμες πληροφοριακών συστημάτων.

SSH σε περιβάλλον Linux

Στην περίπτωση του Debian GNU/Linux, καθώς και των περισσοτέρων Unix-οειδών λειτουργικών συστημάτων, η χρήση της υπηρεσίας SSH είναι ιδιαίτερα απλή, μιας και αρκεί η εκτέλεση της σχετικής εντολής ssh [86] στην κονσόλα/τερματικό (terminal), για να συνδεθούμε με ασφάλεια στο απομακρυσμένο σύστημα. Η εν λόγω εντολή είναι φυσικά πλήρως παραμετροποιήσιμη, όμως για την επίτευξη της σύνδεσης στον παρών οδηγό αρκούν η παράμετρος για την πόρτα σύνδεσης, το όνομα χρήστη, καθώς και το όνομα του τομέα ή η διεύθυνση δικτύου του απομακρυσμένου συστήματος. Έτσι, η τελική μορφή της συγκεκριμένης εντολής στο παράδειγμα του οδηγού είναι η παρακάτω:

```
ssh -p 22 root@192.168.204.134
```

Σημείωση: Με δεδομένο ότι η εξ' ορισμού πόρτα σύνδεσης της υπηρεσίας SSH είναι η 22, η συγκεκριμένη παράμετρος μπορεί και να παραληφθεί. Αναφέρεται όμως εσκεμμένα, μιας και σε επόμενο βήμα του οδηγού η πόρτα σύνδεσης θα τροποποιηθεί, συνεπώς η αναφορά της παραμέτρου αυτής θα είναι απαραίτητη για την ολοκλήρωση της σύνδεσης.

Το γραφικό περιβάλλον σύνδεσης σε μια κονσόλα απομακρυσμένου πληροφοριακού συστήματος είναι φυσικά εντελώς περιττό, αν όμως κάποιος το επιθυμεί, μπορεί να χρησιμοποιήσει κάποιες από τις εφαρμογές που έχουν αναπτυχθεί για το σκοπό αυτό. Τέτοια παραδείγματα αποτελούν η εφαρμογή SSH-GUI (γραφικό περιβάλλον διεπαφής της ssh), η εφαρμογή lCRT (http://code.google.com/p/lcrt/), ή ακόμα και πιο «παράδοξες» λύσεις, όπως η χρήση της εντολής fish (fish://user@host/path/to/dir) για σύνδεση στο απομακρυσμένο σύστημα μέσα από έναν απλό περιηγητή διαδικτύου που υποστηρίζει τη συγκεκριμένη δυνατότητα (πχ Konqueror).

SSH σε περιβάλλον Windows

Σε περιβάλλον Windows, υπάρχουν και εμπορικές αλλά και ανοιχτού κώδικα εφαρμογές, οι οποίες, αδιαφορώντας για τη διαφορετικότητα των δύο λειτουργικών συστημάτων, είναι σε θέση να παράσχουν απομακρυσμένη πρόσβαση στο τερματικό του Debian GNU/Linux του εξυπηρετητή. Εντελώς επιγραμματικά αναφέρονται οι αρκετά γνωστές Absolute Telnet/SSH, CopSSH, OpenSSH, Private Shell, οι οποίες βέβαια αποτελούν ένα μικρό δείγμα από το σύνολο των εφαρμογών που είναι διαθέσιμες στον τελικό χρήστη του συγκεκριμένου λειτουργικού συστήματος [87].

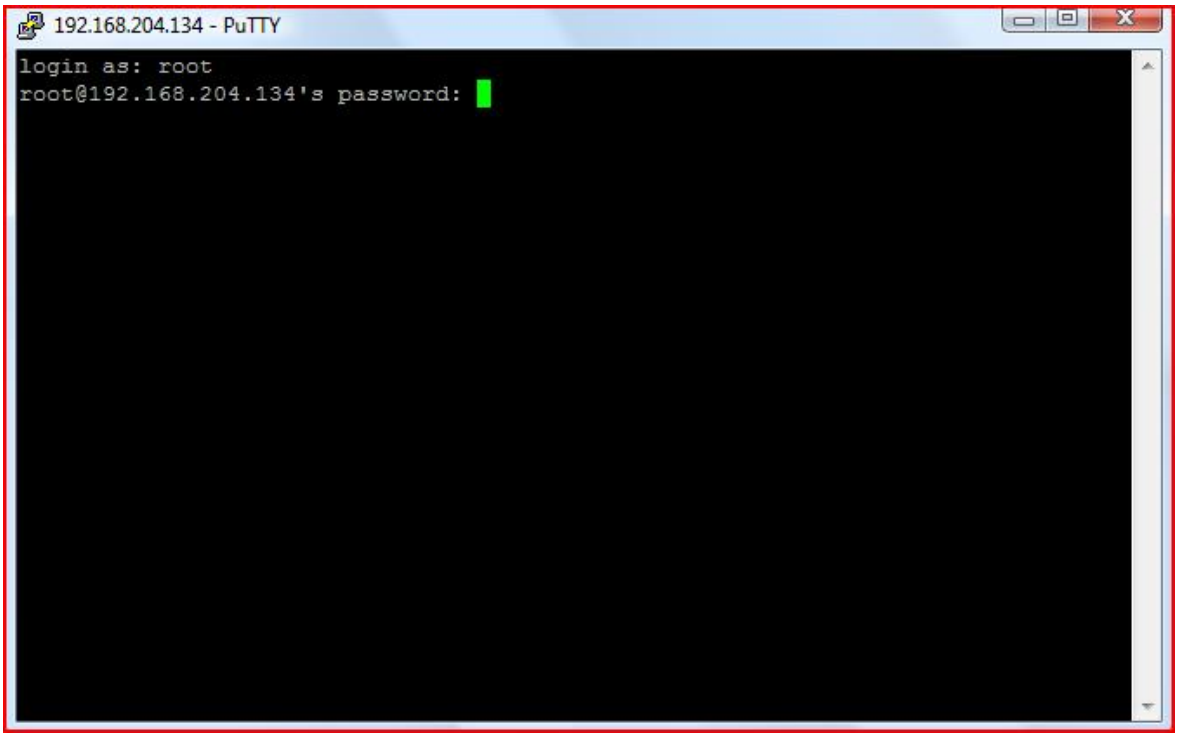
Ανάμεσα στις σχετικές εφαρμογές της κατηγορίας του ελεύθερου λογισμικού / λογισμικού ανοιχτού κώδικα συμπεριλαμβάνεται και η ευρέως διαδεδομένη PuTTY. Η συγκεκριμένη εφαρμογή υποστηρίζει συνδέσεις με το παλαιότερο και χωρίς δυνατότητα κρυπτογράφησης δεδομένων πρωτόκολλο Telnet, αλλά και με τον αντικαταστάτη αυτού, το σύγχρονο SSH στις υλοποιήσεις SSH1 και SSH2 [88]. Δίνοντας έμφαση στη δυνατότητα που παρέχεται για σύνδεση δύο πληροφοριακών συστημάτων με εντελώς διαφορετικής πλατφόρμας λογισμικό (Linux και Windows), η συγκεκριμένη εφαρμογή έχει επιλεγεί να χρησιμοποιηθεί για την επίτευξη της ασφαλούς SSH σύνδεσης με τον εξυπηρετητή στον οδηγό της παρούσας πτυχιακής εργασίας.

Η εφαρμογή είναι ιδιαίτερα απλή στη χρήση της. Με την εκτέλεσή της εμφανίζεται στο χρήστη ένα παράθυρο διαλόγου στο οποίο εισάγονται οι βασικές παράμετροι που αφορούν στη σύνδεση. Στο πεδίο «Host Name» εισάγεται το όνομα τομέα ή η διεύθυνση δικτύου του απομακρυσμένου συστήματος, στο «Connection type» επιλέγεται το πρωτόκολλο SSH, στο πεδίο «Port» εισάγεται η πόρτα στην οποία θα πραγματοποιηθεί η σύνδεση και στη συνέχεια, με χρήση της επιλογής «Open», πραγματοποιείται η επιθυμητή σύνδεση.

Πριν από την ολοκλήρωση της σύνδεσης, ο χρήστης θα βρεθεί κατά πάσα πιθανότητα αντιμέτωπος με το παρακάτω παράθυρο διαλόγου:

Το συγκεκριμένο μήνυμα προειδοποίησης ασφαλείας προκύπτει από μια λειτουργία του πρωτοκόλλου SSH, με την οποία ο χρήστης προστατεύεται από δικτυακές επιθέσεις τύπου spoofing (μη εξουσιοδοτημένη ανακατεύθυνση της σύνδεσης σε τρίτο πληροφοριακό σύστημα). Κάθε φορά που πραγματοποιείται σύνδεση με κάποιο νέο εξυπηρετητή, ο χρήστης ειδοποιείται σχετικά και του παρέχεται η δυνατότητα να ολοκληρώσει τη σύνδεση, ή να τερματίσει τη διαδικασία. Την πρώτη λοιπόν και μόνο φορά που θα συνδεθούμε στον εξυπηρετητή είναι ασφαλές το να εμπιστευθούμε το αποτύπωμα του κλειδιού rsa2 αυτού επιλέγοντας «Yes». Εάν χωρίς να έχει προηγηθεί σχετική τροποποίηση ρυθμίσεων, το συγκεκριμένο μήνυμα εμφανιστεί εκ νέου σε μελλοντική σύνδεση, τότε θα πρέπει να θορυβηθούμε και να εξετάσουμε περισσότερο τις λεπτομέρειες πριν συνεχίσουμε.

Μετά τη θετική απόκριση στην προειδοποίηση ασφαλείας γίνεται αυτόματη αποθήκευση του νέου host key του εξυπηρετητή και εμφανίζεται στο χρήστη το παρακάτω παράθυρο τερματικού, μέσα από το οποίο του ζητούνται τα διαπιστευτήρια πρόσβασης στο απομακρυσμένο πληροφοριακό σύστημα. Εισάγονται σε δύο ξεχωριστά βήματα το όνομα χρήστη, καθώς και ο κωδικός πρόσβασης αυτού και στη συνέχεια ολοκληρώνεται η σύνδεση και παρέχεται στο χρήστη η πρόσβαση στην κονσόλα του απομακρυσμένου συστήματος.



Σημείωση: Επειδή μετά την εισαγωγή του ονόματος χρήστη δεν παρέχεται η δυνατότητα τροποποίησής του, θα πρέπει να δοθεί ιδιαίτερη προσοχή ώστε να μη συμβούν λάθη κατά την πληκτρολόγηση.

Δεύτερο στάδιο εγκατάστασης

Χρησιμοποιώντας τα διαπιστευτήρια του διαχειριστή, όπως αυτά καθορίστηκαν στο πρώτο στάδιο της εγκατάστασης, ολοκληρώνουμε με κάποιον από τους προαναφερθέντες τρόπους την ασφαλή, SSH σύνδεση με το απομακρυσμένο σύστημα. Έτσι, αποκτάμε πρόσβαση στο τερματικό του εξυπηρετητή και είμαστε έτοιμοι να εκτελέσουμε τα ακόλουθα βήματα της διαδικασίας εγκατάστασης και παραμετροποίησης όλου του λογισμικού που απαιτείται για την παροχή των υπηρεσιών, αλλά και για την εποπτεία και διαχείριση του συστήματος.

Εγκατάσταση Vi IMproved

Ως επεξεργαστής κειμένου στα επόμενα στάδια του οδηγού θα χρησιμοποιηθεί ο επεξεργαστής κειμένου vi που εγκαθίσταται με το βασικό σύστημα σε μια τυπική εγκατάσταση Debian GNU/Linux. Επειδή όμως η προκαθορισμένη έκδοσή του

παρουσιάζει μια περίεργη συμπεριφορά (πχ τύπωση χαρακτήρων στην οθόνη, όταν επιχειρείται μετακίνηση του κέρσορα στην κατάσταση επεξεργασίας κειμένου κτλ), θα πραγματοποιηθεί εγκατάσταση της πιο βελτιωμένης έκδοσης, vim.

Οδηγία: Εκτελούμε την παρακάτω εντολή και στη σχετική ερώτηση, επιβεβαιώνουμε με enter την πρόθεση για εγκατάσταση του πακέτου vim-nox:

```
apt-get install vim-nox
```

Τροποποίηση ρυθμίσεων SSH

Η εξ' ορισμού σύνδεση μέσω της υπηρεσίας SSH γίνεται στην πόρτα 22 και έτσι, ο συγκεκριμένος αριθμός πόρτας χρησιμοποιείται από διάφορα κακόβουλα script, που έχουν δημιουργηθεί με σκοπό να αποκτήσουν και να προσφέρουν στο χρήστη τους τη δυνατότητα πρόσβασης σε συστήματα με χαμηλό επίπεδο ασφάλειας. Με στόχο την επίτευξη του υψηλότερου δυνατού επιπέδου ασφάλειας, στην παρούσα εργασία αφενός θα τροποποιηθεί η συγκεκριμένη πόρτα σύνδεσης, αφετέρου, όπως ήδη αναφέρθηκε στο βήμα 11 του προηγούμενου κεφαλαίου, θα απαγορευτεί στο διαχειριστή του συστήματος να συνδέεται απομακρυσμένα με αυτό. Για τη διαχείριση του συστήματος, θα πρέπει ο υπεύθυνος αρχικά να πραγματοποιεί σύνδεση μέσω της υπηρεσίας SSH στη νέα πόρτα, χρησιμοποιώντας τα διαπιστευτήρια του απλού χρήστη που έχει ήδη δημιουργηθεί σε προηγούμενο βήμα του οδηγού. Στη συνέχεια, θα πρέπει να αιτείται εκχώρηση «ανεβασμένων δικαιωμάτων» (elevated rights), ώστε να είναι εφικτή η διαχείριση του συστήματος.

Έτσι, μετά την ολοκλήρωση των σχετικών τροποποιήσεων, για να μπορέσει κάποιος να βλάψει τον εξυπηρετητή θα πρέπει να ψάξει χειρονακτικά την πόρτα απομακρυσμένης σύνδεσης, να «μαντέψει» το όνομα και τον κωδικό πρόσβασης του απλού χρήστη και αφού αποκτήσει την απομακρυσμένη πρόσβαση, να «μαντέψει» και τον κωδικό του διαχειριστή, ώστε να αποκτήσει τα δικαιώματά του και να είναι σε θέση να πραγματοποιήσει σημαντικές τροποποιήσεις του συστήματος.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων SSH (sshd_config):

```
vi /etc/ssh/sshd_config
```

Οδηγία: Στη γραμμή 5 του αρχείου, αλλάζουμε τον αριθμό της πόρτας από την προκαθορισμένη 22, σε κάποια άλλη, η οποία δε χρησιμοποιείται (πχ 22222):

```
[...]
# What ports, IPs and protocols we listen for
Port 22222
[...]
```

Οδηγία: Στη γραμμή 26 του ίδιου αρχείου, αφαιρούμε το δικαίωμα του διαχειριστή να συνδέεται απομακρυσμένα, αλλάζοντας τη μεταβλητή «PermitRootLogin» από το προκαθορισμένο «yes», σε «no»:

```
[...]
PermitRootLogin no
[...]
```

Οδηγία: Επανεκκινούμε την υπηρεσία SSH ώστε να ισχύσουν άμεσα οι αλλαγές:

```
/etc/init.d/ssh restart
```

Σε αυτό το σημείο θα πρέπει να αποσυνδεθούμε από τον εξυπηρετητή και να συνδεθούμε εκ νέου χρησιμοποιώντας τη νέα πόρτα, καθώς και το όνομα και τον κωδικό πρόσβασης του απλού χρήστη (όχι του διαχειριστή). Έπειτα, θα πρέπει να αιτηθούμε τα ανεβασμένα δικαιώματα με την εντολή «su» προσθέτοντας την παράμετρο «-», ώστε να αποκτήσουμε και το περιβάλλον εργασίας του διαχειριστή (το αποτέλεσμα της «su -» θα είναι αυτό που θα είχαμε εάν είχαμε συνδεθεί αρχικά ως ο υπερ-χρήστης του συστήματος).

Τροποποίηση αρχείου πηγών εφαρμογής διαχείρισης πακέτων

Στο προηγούμενο κεφάλαιο έγινε καθορισμός του προεπιλεγμένου καθρέφτη αποθετηρίου αναβαθμίσεων βάσει της γεωγραφικής τοποθέτησης του συστήματος. Το επιθυμητό αποτέλεσμα πίσω από αυτή την ενέργεια είναι το να πραγματοποιείται η πρόσβαση στον καθρέφτη με μεγάλη ταχύτητα διαμεταγωγής δεδομένων και οι απαιτούμενες μεταφορτώσεις να ολοκληρώνονται χωρίς καθυστερήσεις. Η συγκεκριμένη μέθοδος είναι αρκετά ικανοποιητική, λαμβάνοντας υπόψη ότι είναι και η μόνη διαθέσιμη στο πρώτο τμήμα της εγκατάστασης του βασικού συστήματος. Στην τρέχουσα φάση

όμως, μπορεί να χρησιμοποιηθεί ένας πιο αντικειμενικός τρόπος καθορισμού του ταχύτερου καθρέφτη αποθετηρίου αναβαθμίσεων, ο οποίος περιλαμβάνει αξιολόγηση όλων των διαθέσιμων καθρεφτών με τη διενέργεια συγκριτικού ελέγχου της ταχύτητας απόκρισης αυτών. Η εν λόγω διαδικασία είναι εντελώς αυτοματοποιημένη και γίνεται με χρήση της εντολής netselect-apt, που έχει αναπτυχθεί για αυτόν ακριβώς το σκοπό [31].

Με την εκτέλεσή της, η netselect-apt θα μεταφορτώσει στον εξυπηρετητή μια λίστα όλων των διαθέσιμων καθρεφτών παγκοσμίως [32] και στη συνέχεια θα καταγράψει τους χρόνους απόκρισης (latency) για τον κάθε ένα από αυτούς. Ο χρόνος απόκρισης του εκάστοτε καθρέφτη καθορίζει την εγγύτητά του, η οποία όμως επηρεάζει καθοριστικά και την ταχύτητα διαμεταγωγής δεδομένων. Έτσι, η εφαρμογή netselect-apt θα είναι σε θέση να επιλέξει αντικειμενικά τον ταχύτερο από τους διαθέσιμους καθρέφτες, τον οποίο και θα ορίσει ως προεπιλεγμένο στο νέο αρχείο πηγών της εφαρμογής διαχείρισης πακέτων, που θα δημιουργήσει στον τρέχων κατάλογο χρήσης.

Οδηγία: Αντιγράφουμε το υπάρχων αρχείο πηγών της εφαρμογής διαχείρισης πακέτων στο φάκελο αντιγράφων ασφαλείας των τροποποιημένων αρχείων:

```
cp /etc/apt/sources.list /root/backups/sources.list
```

Οδηγία: Εγκαθιστούμε την εφαρμογή netselect-apt, η οποία δεν αποτελεί μέρος του βασικού συστήματος και δεν έχει εγκατασταθεί στο προηγούμενο κεφάλαιο. Επιβεβαιώνουμε την πρόθεσή μας με «enter» στη σχετική ερώτηση:

```
apt-get install netselect-apt
```

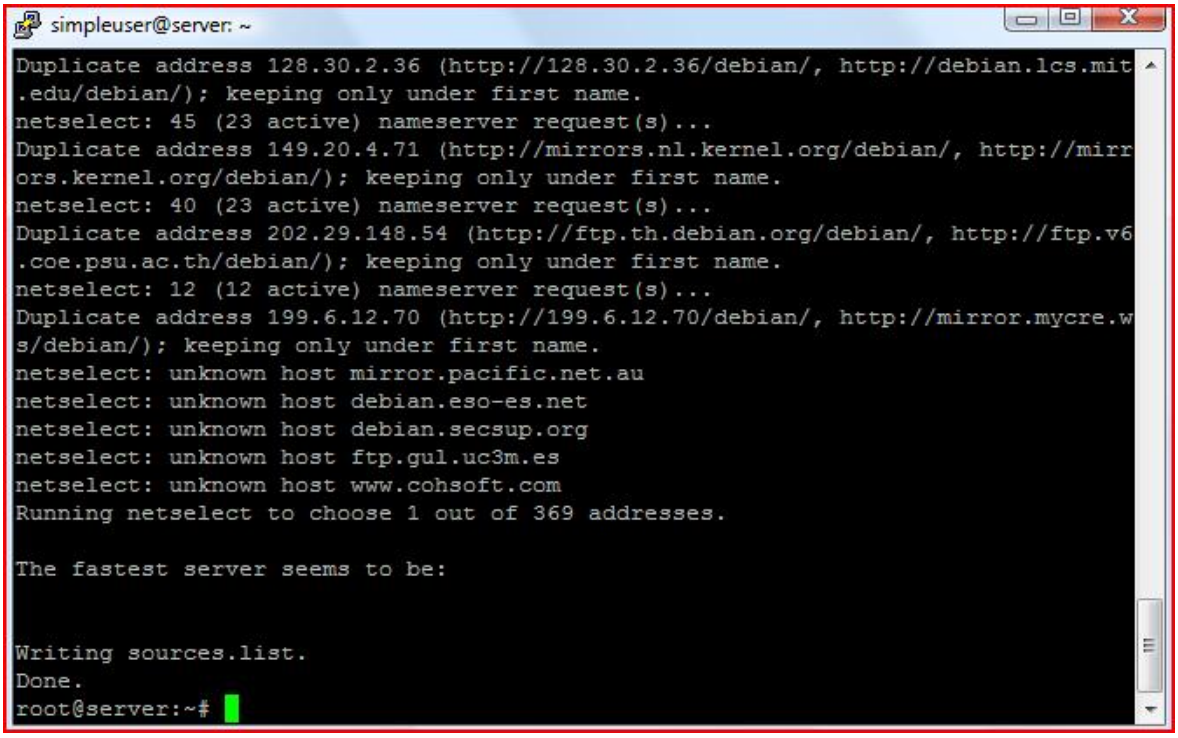
Οδηγία: Εκτελούμε την εντολή διενέργειας του συγκριτικού ελέγχου των καθρεφτών και δημιουργίας του νέου αρχείου πηγών της εφαρμογής διαχείρισης πακέτων:

```
netselect-apt
```

Εάν δεν υπάρξει πρόβλημα, μετά από ένα μικρό χρονικό διάστημα η εντολή θα μας ενημερώσει για τον ταχύτερο καθρέφτη και παράλληλα, θα δημιουργήσει το νέο αρχείο πηγών:

```
The fastest server seems to be:
        http://212.219.56.135/sites/ftp.debian.org/debian/
Writing sources.list.
Done.
```

Σε ορισμένες περιπτώσεις, όπως στο παρακάτω στιγμιότυπο οθόνης, δεν επιλέγεται κάποιος εξυπηρετητής και δημιουργείται ένα κενό αρχείο πηγών. Αυτό συνήθως οφείλεται στην περιορισμένη πρόσβαση στο διαδίκτυο, πιθανώς λόγω της ύπαρξης τείχους προστασίας (firewall), το οποίο και δεν επιτρέπει την ορθή εκτέλεση της netselect-apt. Σε τέτοια περίπτωση θα πρέπει να επικοινωνήσουμε με το διαχειριστή του δικτύου, ώστε να προβεί στις απαραίτητες ενέργειες για την εξάλειψη του προβλήματος.



Οδηγία: Για την αντικατάσταση του παλαιού αρχείου πηγών με το νέο, μετακινούμε το τελευταίο από τον τρέχοντα φάκελο στο φάκελο /etc/apt:

```
mv ./sources.list /etc/apt/sources.list
```

Σε μεταγενέστερο βήμα του οδηγού θα πραγματοποιηθεί εγκατάσταση της αντιικής εφαρμογής ClamAv, η οποία θα χρησιμοποιείται για τον έλεγχο των συνημμένων των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Η συγκεκριμένη εφαρμογή θα πρέπει να ενημερώνεται καθημερινά μεταφορτώνοντας ένα ενημερωμένο αντίγραφο της βάσης

δεδομένων ιών της από το αποθετήριο «squeeze-updates», όπου διατηρείται η πλέον ενημερωμένη έκδοση του εν λόγω αντιγράφου. Συνεπώς, στην περίπτωση που δεν έχει καταχωρηθεί από τη netselect-apt το συγκεκριμένο αποθετήριο στο αρχείων πηγών, αυτό θα πρέπει να γίνει χειρονακτικά.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο πηγών της εφαρμογής διαχείρισης πακέτων:

```
vi /etc/apt/sources.list
```

Οδηγία: Προσθέτουμε τις παρακάτω γραμμές, χρησιμοποιώντας τον εξυπηρετητή που έχει επιλεγεί από τη netselect-apt (στο παράδειγμα χρησιμοποιείται ο http://ftp.gr.debian.org/debian/):

```
[...]
deb http://ftp.gr.debian.org/debian/ squeeze-updates main
deb-src http://ftp.gr.debian.org/debian/ squeeze-updates main
[...]
```

Οδηγία: Εκτελούμε επικαιροποίηση της βάσης δεδομένων της apt-get:

```
apt-get update
```

Οδηγία: Εκτελούμε επικαιροποίηση του συστήματος, επιβεβαιώνοντας εάν απαιτηθεί την πρόθεσή μας απαντώντας με «enter» στη σχετική ερώτηση:

```
apt-get upgrade
```

Τροποποίηση αρχείου ρυθμίσεων δικτύου

Στο βήμα 6 της εγκατάστασης του βασικού συστήματος πραγματοποιήθηκαν οι ρυθμίσεις δικτύου του εξυπηρετητή. Αυτό έγινε είτε μέσω του διακομιστή διευθυνσιοδότησης (DHCP), είτε χειρονακτικά μέσα από σχετικές ερωτ-απαντήσεις. Σε κάθε περίπτωση όμως, ο εξυπηρετητής θα πρέπει να έχει στατική διεύθυνση δικτύου (IP) και να μην εξαρτάται από τη διαθεσιμότητα του εξυπηρετητή DHCP. Για το λόγο αυτό, θα πρέπει να τροποποιηθεί κατάλληλα το αρχείο ρυθμίσεων δικτύου, με τη διεύθυνση, τη μάσκα, καθώς και την πύλη του δικτύου, που θα παρασχεθούν από τον υπεύθυνο του

κέντρου δεδομένων, ή από τον πάροχο του συστήματος (στην περίπτωση που ο εξυπηρετητής είναι εγκαταστημένος σε κέντρο δεδομένων εκτός της επιχείρησης).

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων δικτύου:

```
vi /etc/network/interfaces
```

Οδηγία: Εισάγουμε τα στοιχεία που αφορούν στον εξυπηρετητή και το δίκτυο όπως παρακάτω:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.204.134
        netmask 255.255.255.0
        gateway 192.168.204.1
        network 192.168.204.0
        broadcast 192.168.204.255
```

Οδηγία: Στη συνέχεια επανεκκινούμε την υπηρεσία δικτύου:

```
/etc/init.d/networking restart
```

Στην διανομή Squeeze του Debian GNU/Linux υπάρχει περίπτωση να μην ολοκληρωθεί η επανεκκίνηση της υπηρεσίας δικτύου, αλλά να παρουσιαστεί το μήνυμα σφάλματος: «Running /etc/init.d/networking restart is deprecated because it may not enable again some interfaces.», με προτεινόμενη λύση τη χρήση των εντολών «ifdown» για τον τερματισμό της υπηρεσίας δικτύου και «ifup» για την επανενεργοποίησή του. Εάν προσπαθήσουμε να πετύχουμε την επανεκκίνηση της υπηρεσίας δικτύου χρησιμοποιώντας τις δύο αυτές εντολές μεμονωμένα, θα διαπιστώσουμε ότι μετά από την εκτέλεση της πρώτης δε θα έχουμε πλέον πρόσβαση στον εξυπηρετητή. Έτσι, μπορούμε είτε να συνδυάσουμε τις δύο εντολές σε μία:

```
ifdown eth0 && ifup eth0
```

είτε να επανεκκινήσουμε ολόκληρο το σύστημα:

```
reboot
```

Σημείωση: Εάν απαιτούνται, υπάρχουν διαθέσιμες διαδικτυακά περισσότερες πληροφορίες και για την επανεκκίνηση της υπηρεσίας δικτύου [33], αλλά και για τις ρυθμίσεις δικτύου γενικότερα [34].

Τροποποίηση αρχείου hosts

Το αρχείο hosts χρησιμοποιείται από τον εξυπηρετητή για την επίλυση ονομάτων συστημάτων (αντιστοίχιση αυτών με διευθύνσεις δικτύου), μεταξύ των οποίων συγκαταλέγεται και ο ίδιος ο εξυπηρετητής. Κατά την εγκατάσταση του βασικού συστήματος έχουν γίνει αυτόματα οι απαιτούμενες καταχωρίσεις στο εν λόγω αρχείο, οι οποίες όμως είναι απαραίτητο να τροποποιηθούν όπως παρακάτω.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο hosts:

```
vi /etc/hosts
```

Οδηγία: Στην πρώτη γραμμή του αρχείου, προσθέτουμε πριν από το προκαθορισμένο όνομα του συστήματος (localhost), το κανονικοποιημένο, πλήρες όνομα αυτού (locahost.localdomain):

```
127.0.0.1       localhost.localdomain   localhost
[...]
```

Οδηγία: Στη δεύτερη γραμμή του ίδιου αρχείου, αντικαθιστούμε τη διεύθυνση localhost (127.0.0.1), με την πραγματική διεύθυνση του συστήματος:

```
[...]
192.168.204.134       server.mydomain.gr      server
[...]
```

Τροποποίηση αρχείου hostname

Το όνομα του συστήματος έχει επίσης καταχωρηθεί αυτόματα στο αρχείο /etc/hostname. Και η συγκεκριμένη αυτόματη καταχώριση θα πρέπει να τροποποιηθεί ώστε να περιλαμβάνει το πλήρες κανονικοποιημένο όνομα του συστήματος (συμπεριλαμβανομένου και του ονόματος τομέα), ώστε οι εντολές «hostname –f» και «hostname» να επιστρέφουν το ίδιο αποτέλεσμα.

Σημείωση: Σε αυτό το σημείο τα αποτελέσματα των εντολών «hostname –f» και «hostname» είναι:

```
hostname -f
server.mydomain.gr
hostname
server
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο hostname:

```
vi /etc/hostname
```

Οδηγία: Προσθέτουμε το όνομα τομέα στο υπάρχον όνομα συστήματος:

```
server.mydomain.gr
```

Οδηγία: Ενεργοποιούμε τις αλλαγές με:

```
/etc/init.d/hostname.sh start
```

Σημείωση: Σε αυτό το σημείο τα αποτελέσματα των εντολών «hostname –f» και «hostname» θα πρέπει πλέον να είναι:

```
hostname -f
server.mydomain.gr
hostname
server.mydomain.gr
```

Αλλαγή προκαθορισμένου κελύφους

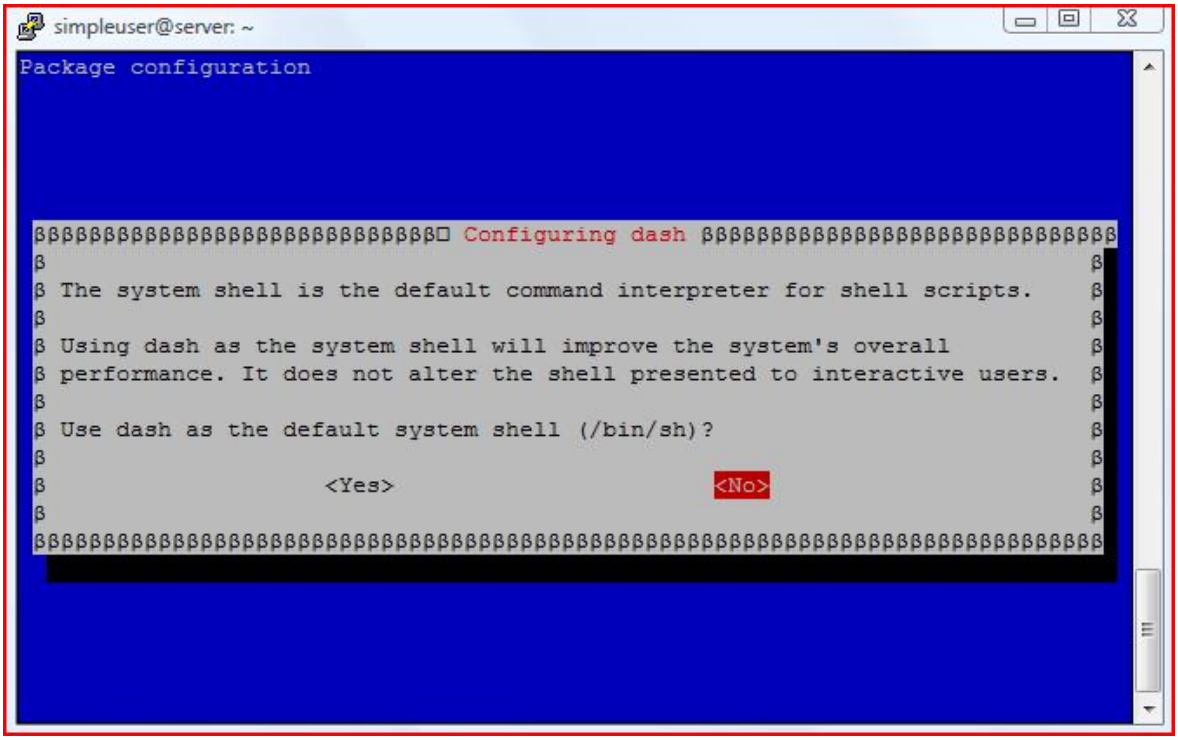
Το προκαθορισμένο κέλυφος για τη διανομή Squeeze είναι το dash, το οποίο διαφέρει αρκετά σε σχέση με το μέχρι πρόσφατα προκαθορισμένο κέλυφος του Debian GNU/Linux, το bash [35]. Επειδή όμως το bash είναι απαραίτητο για την εγκατάσταση του ISPConfig, θα πρέπει να οριστεί αυτό ως προκαθορισμένο κέλυφος, διαφορετικά η εγκατάσταση του ISPConfig θα αποτύχει.

Σημείωση: Η εμφάνιση του προκαθορισμένου κελύφους μπορεί να πραγματοποιηθεί με την εντολή «echo $SHELL», ενώ όλων των διαθέσιμων κελυφών με την εντολή «cat /etc/shells».

Οδηγία: Εκτελούμε την εντολή για τροποποίηση των ρυθμίσεων του κελύφους dash:

```
dpkg-reconfigure dash
```

Οδηγία: Επιλέγουμε να μην είναι το dash το προκαθορισμένο κέλυφος:



Ενημέρωση - συγχρονισμός ρολογιού

Σχεδόν στο σύνολο των πληροφοριακών συστημάτων λειτουργούν δύο μηχανισμοί παρακολούθησης του χρόνου, το ρολόι του υλικού (το οποίο είναι εφοδιασμένο με μπαταρία ώστε να μπορεί να διατηρεί τη σωστή ημερομηνία και ώρα ακόμα και όταν το σύστημα είναι εκτός λειτουργίας) και το ρολόι του λογισμικού (το οποίο είναι υπεύθυνο για την παροχή των ρυθμίσεων χρόνου στο σύστημα και το οποίο είναι ενεργό μόνο για το διάστημα που το τελευταίο είναι σε λειτουργία). Το πρώτο από τα δύο ρολόγια είναι αρκετά αξιόπιστο, όμως το δεύτερο συνήθως παρουσιάζει μικρές ή μεγάλες αποκλίσεις.

Οι τυχόν αποκλίσεις από την πραγματική ώρα δεν είναι ούτε επιθυμητές, ούτε αποδεκτές στην περίπτωση ενός εξυπηρετητή διαδικτύου, μιας και πάνω σε αυτόν στηρίζεται η καλή λειτουργία άλλων συστημάτων ή διεργασιών. Για παράδειγμα, δεν είναι αξιοποιήσιμη μια καταγραφή συμβάντος, όταν δεν είναι αξιόπιστος ο χρόνος τέλεσης αυτού. Έτσι, με στόχο τη διατήρηση μιας αξιόπιστης ώρας στο λογισμικό ρολόι του συστήματος, θα πρέπει να γίνονται συνεχείς διορθώσεις αυτού.

Για το συγκεκριμένο σκοπό έχουν αναπτυχθεί διάφορες εφαρμογές, δύο από τις οποίες είναι διαθέσιμες και στο Debian GNU/Linux: η ntpdate και η ntpd [36, 37, 38]. Η φιλοσοφία πίσω από τη διαδικασία είναι απλή, με χρήση του πρωτοκόλλου NTP (Network Time Protocol), ζητείται η ημερομηνία/ώρα από κάποιον διακομιστή NTP και η απάντηση χρησιμοποιείται για τη ρύθμιση του ρολογιού του συστήματος. Η διαφορά μεταξύ των δύο εφαρμογών είναι ότι η πρώτη εκτελείται είτε κατά την εκκίνηση του συστήματος, είτε κατ' απαίτηση και πραγματοποιεί διορθώσεις που μπορεί να είναι μεγάλες, ενώ η δεύτερη τρέχει ως δαίμονας (daemon) και χρησιμοποιώντας λίγη από την επεξεργαστική ισχύ του συστήματος πραγματοποιεί συνεχείς μικροδιορθώσεις. Η παράλληλη εγκατάσταση και των δύο εφαρμογών στο ίδιο σύστημα δεν παρουσιάζει προβλήματα, έτσι, στο επόμενο βήμα θα εγκατασταθούν στον εξυπηρετητή και οι δύο εφαρμογές.

Οδηγία: Εγκαθιστούμε τις εφαρμογές ntpdate και ntpd, με τα αντίστοιχα πακέτα ntpdate και ntp, επιβεβαιώνοντας την πρόθεσή μας με «enter» στη σχετική ερώτηση:

```
apt-get install ntpdate ntp
```

Η εφαρμογή ntpd εκτελείται αυτόματα αμέσως μετά την εγκατάστασή της. Εάν για κάποιο λόγο απαιτηθεί να εκκινηθεί χειρονακτικά, αυτό μπορεί να γίνει με την εντολή:

```
/etc/init.d/ntp start
```

Οδηγία: Ελέγχουμε την ορθότητα της τρέχουσας ημερομηνίας/ώρας του συστήματος εκτελώντας την εντολή date:

```
date
```

Εγκατάσταση Postfix, Courier, Getmail, Saslauthd, MySQL, rkhunter, binutils, sudo

Όπως έχει ήδη αναφερθεί, ο πίνακας ελέγχου και διαχείρισης ISPConfig του εξυπηρετητή βασίζεται σε άλλες εφαρμογές, επίσης ανοιχτού κώδικα, οι οποίες μάλιστα θα πρέπει να εγκατασταθούν και παραμετροποιηθούν πριν από την εγκατάσταση του ίδιου του πίνακα ελέγχου. Στο τρέχων βήμα θα πραγματοποιηθεί η εγκατάσταση των παρακάτω από τις εν λόγω εφαρμογές:

- **Postfix** [39]: Εξυπηρετητής ηλεκτρονικού ταχυδρομείου που ξεκίνησε στο τμήμα έρευνας της IBM, από τον Wietse Zweitze Venema, ως εναλλακτική λύση στη ευρέως χρησιμοποιούμενη εφαρμογή sendmail. Βασικές επιδιώξεις των προγραμματιστών του θέλουν το postfix να είναι γρήγορο, ασφαλές και εύκολο στη διαχείριση.

- **Courier** [40]: Αρθρωτής σύνθεσης εξυπηρετητής ηλεκτρονικού ταχυδρομείου που σχεδιάστηκε και αναπτύχθηκε ώστε να μπορεί να λειτουργήσει παράλληλα με άλλες εφαρμογές εξυπηρέτησης ηλεκτρονικού ταχυδρομείου, μιας και τα αρθρώματα έχουν υλοποιηθεί με τρόπο ώστε να είναι δυνατό να ενεργοποιηθούν ή απενεργοποιηθούν μεμονωμένα.

- **Getmail** [41]: Προτείνεται ως εναλλακτική λύση στην πολύ γνωστή εφαρμογή fetchmail. Υποστηρίζει πρωτόκολλα POP3, IMAP4 και SDPS και χρησιμοποιείται από το ISPConfig για την ανάκτηση μηνυμάτων ηλεκτρονικού ταχυδρομείου από άλλους διακομιστές.

- **Saslauthd** [42]: Το Simple Authentication and Security Layer είναι μια μέθοδος προσθήκης υποστήριξης αυθεντικοποίησης σε πρωτόκολλα που βασίζονται σε σύνδεση (connection based protocols). Χρησιμοποιώντας το SASL, θα προστίθεται αυτόματα εντολή για ταυτοποίηση και αυθεντικοποίηση του χρήστη και, προαιρετικά, θα εισάγεται ένα επίπεδο ασφαλείας μεταξύ του πρωτοκόλλου και της σύνδεσης, τηρώντας όσα περιγράφονται στις προδιαγραφές RFC22222.

- **MySQL** [43, 44]: Πρόκειται για το πασίγνωστο λογισμικό διαχείρισης σχεσιακών βάσεων δεδομένων, το οποίο παρέχει έναν ταχύτατο, πραγματικά πολυχρηστικό, καθώς και πολυνηματικό εξυπηρετητή αυτών. Θα εγκατασταθούν τα πακέτα που σχετίζονται με τον εξυπηρετητή αλλά και το λογισμικό πελάτη.

- **Rkhunter** [45]: Διαχειριστικό εργαλείο για τον έλεγχο ύπαρξης κακόβουλου λογισμικού σε συστήματα Unix ή κλώνους αυτού. Το κακόβουλο λογισμικό που χρησιμοποιείται σε τέτοια συστήματα (rootkit, κερκόπορτες, σκουλήκια, κτλ), έχει στόχο να προσφέρει στο χρήστη του απομακρυσμένη πρόσβαση σε αυτά, με απώτερο σκοπό την τέλεση κακόβουλων πράξεων. Για την αντιμετώπισή του έχουν αναπτυχθεί διάφορες εφαρμογές όπως το Zeppoo, το chkrootkit, καθώς και το OSSEC, όμως στην περίπτωση του πίνακα ελέγχου ISPConfig, έχει επιλεγεί από την ομάδα ανάπτυξης το rkhunter. Αυτό, αφού εγκατασταθεί στο σύστημα, θα ελέγχει για πιθανή ύπαρξη κακόβουλου κώδικα και θα ενημερώνει το διαχειριστή αυτού, μέσω αναφορών που θα αποστέλλονται σε αυτόν με μήνυμα ηλεκτρονικού ταχυδρομείου.

- **Binutils** [46, 47]: Πρόκειται για το πακέτο Δυαδικών εργαλείων GNU, το οποίο είναι μια συλλογή από εργαλεία προγραμματισμού, που έχουν αναπτυχθεί για το χειρισμό αντικειμενικού κώδικα σε διάφορες μορφές αντικειμενικών αρχείων.

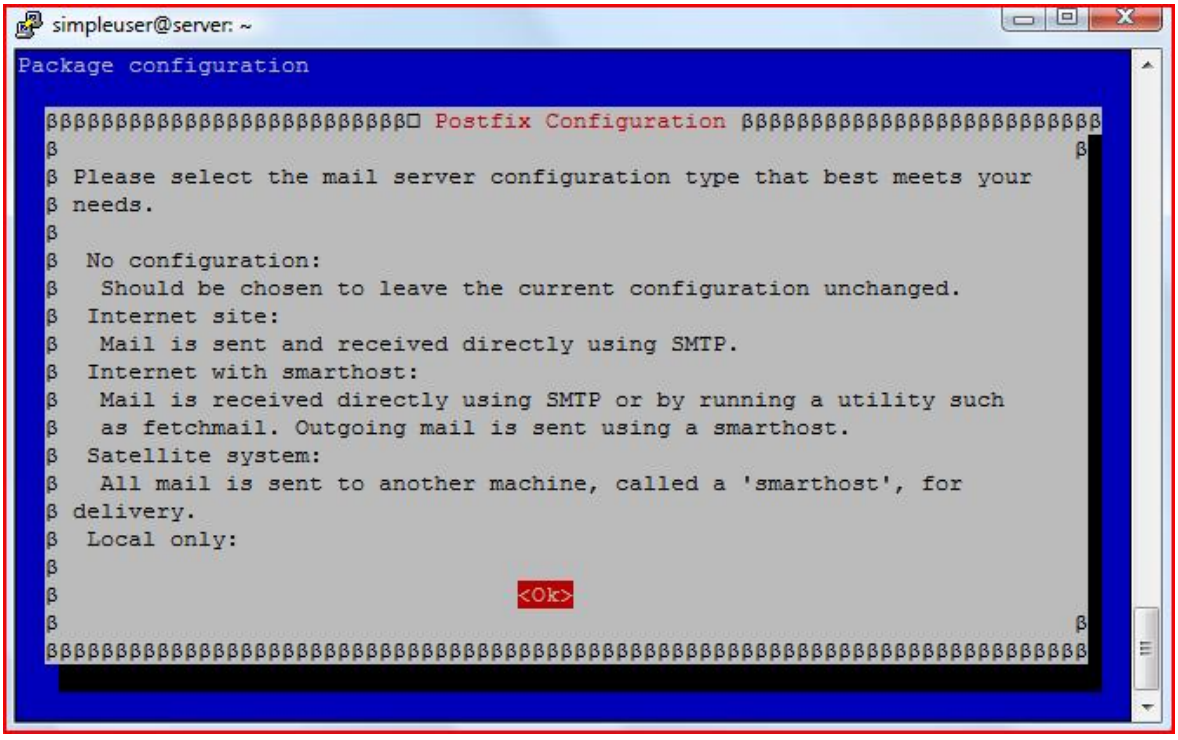
- **Sudo**: Εφαρμογή η οποία παρέχει περιορισμένα δικαιώματα υπερ-χρήστη σε επιλεγμένους, απλούς χρήστες του συστήματος. Η εφαρμογή προτείνεται ως ασφαλέστερη εναλλακτική λύση, συγκρινόμενη με τις τυπικές συνεδρίες

υπερ-χρήστη. Έτσι, ο κωδικός του υπερχρήστη δε χρειάζεται να συνοδεύει την προσωρινή εκχώρηση επιπλέον δικαιωμάτων στους απλούς χρήστες, οι εντολές που δεν απαιτούν επιπλέον δικαιώματα υπερχρήστη μπορούν και εκτελούνται με δικαιώματα απλού χρήστη και τέλος, κάθε αίτηση εκχώρησης δικαιωμάτων υπερχρήστη προκαλεί εγγραφή του ονόματος απλού χρήστη που έκανε την αίτηση, καθώς και της εντολής που τη συνόδευε στο αρχείο καταγραφής.

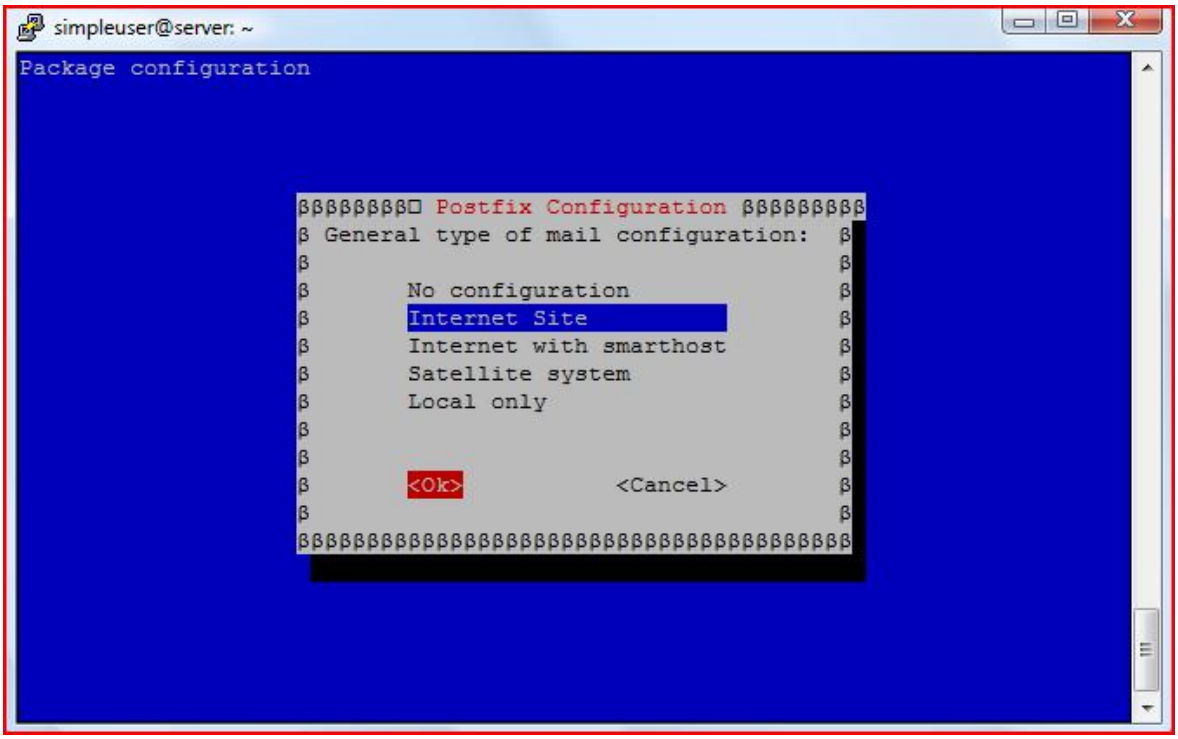
Οδηγία: Εκτελούμε την παρακάτω εντολή και επιβεβαιώνουμε την πρόθεσή μας για εγκατάσταση των επιλεγμένων πακέτων με «enter»:

```
  apt-get install postfix postfix-mysql postfix-doc mysql-
client mysql-server courier-authdaemon courier-authlib-mysql
courier-pop courier-pop-ssl courier-imap courier-imap-ssl
libsasl2-2 libsasl2-modules libsasl2-modules-sql sasl2-bin
libpam-mysql openssl courier-maildrop getmail4 rkhunter
binutils sudo
```

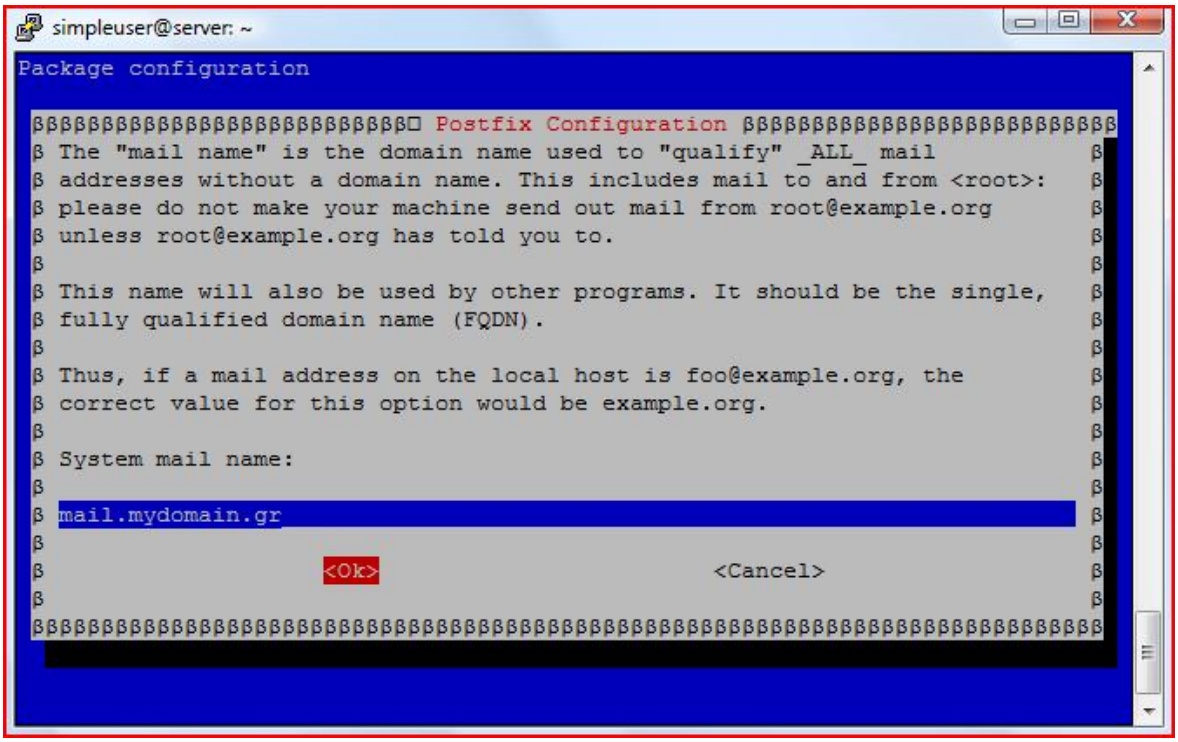
Οδηγία: Ενημερωνόμαστε για τις διαθέσιμες επιλογές σχετικά με το είδος του εξυπηρετητή ηλεκτρονικού ταχυδρομείου και επιλέγουμε OK για να προχωρήσουμε στο επόμενο βήμα:



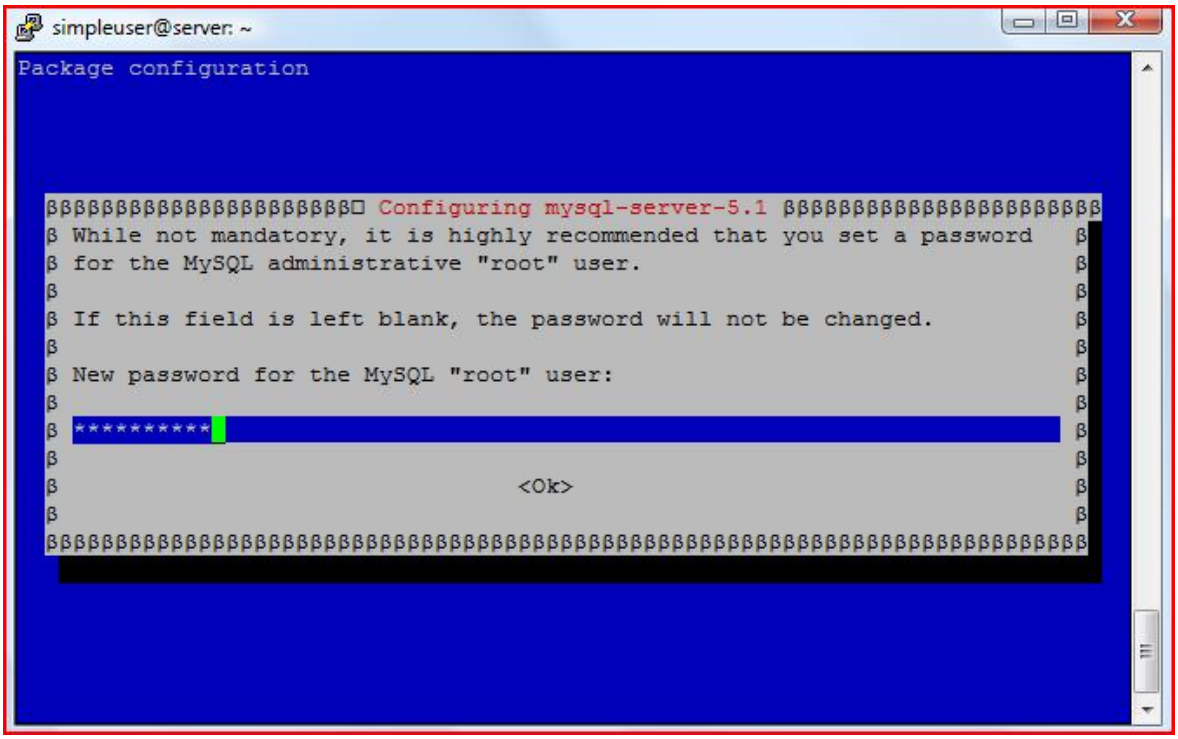
Οδηγία: Επιλέγουμε το πακέτο ρυθμίσεων «Internet Site»:



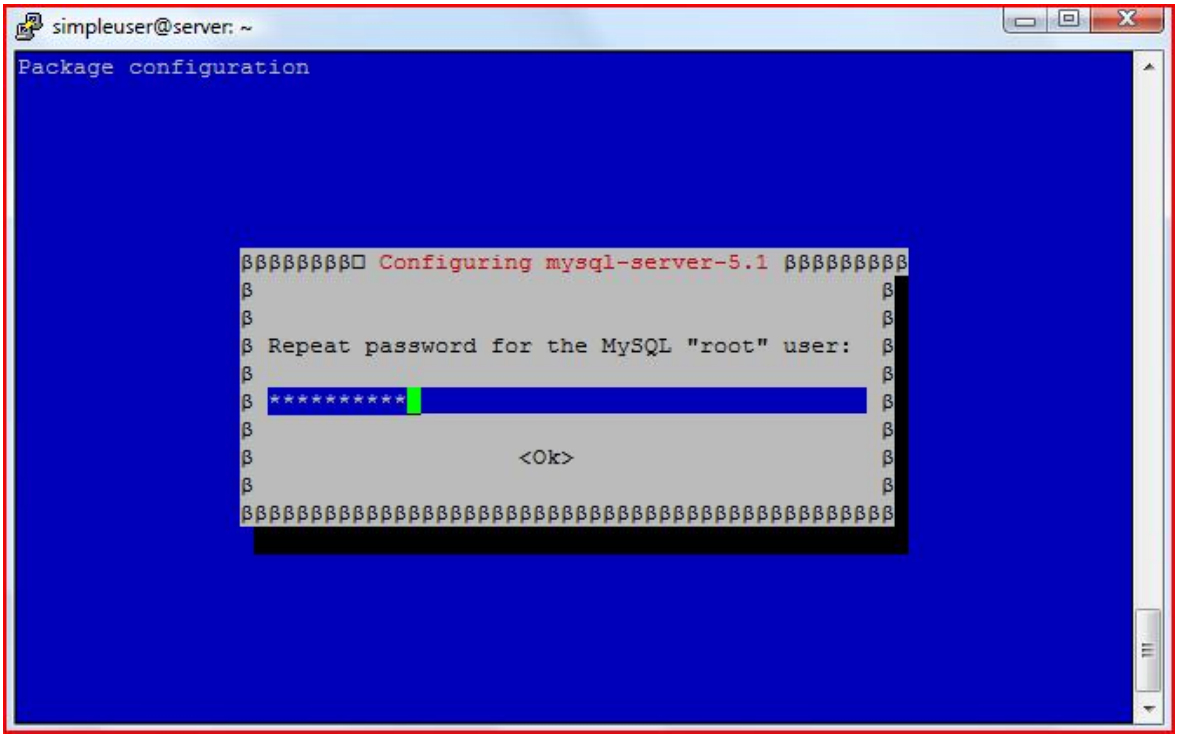
Οδηγία: Εισάγουμε το πλήρες κανονικοποιημένο όνομα για τον εξυπηρετητή ηλεκτρονικού ταχυδρομείου. Αυτό μπορεί να συμπίπτει με το όνομα του εξυπηρετητή ή να είναι το σύνηθες mail.όνομα-τομέα, όπως στο παράδειγμα:



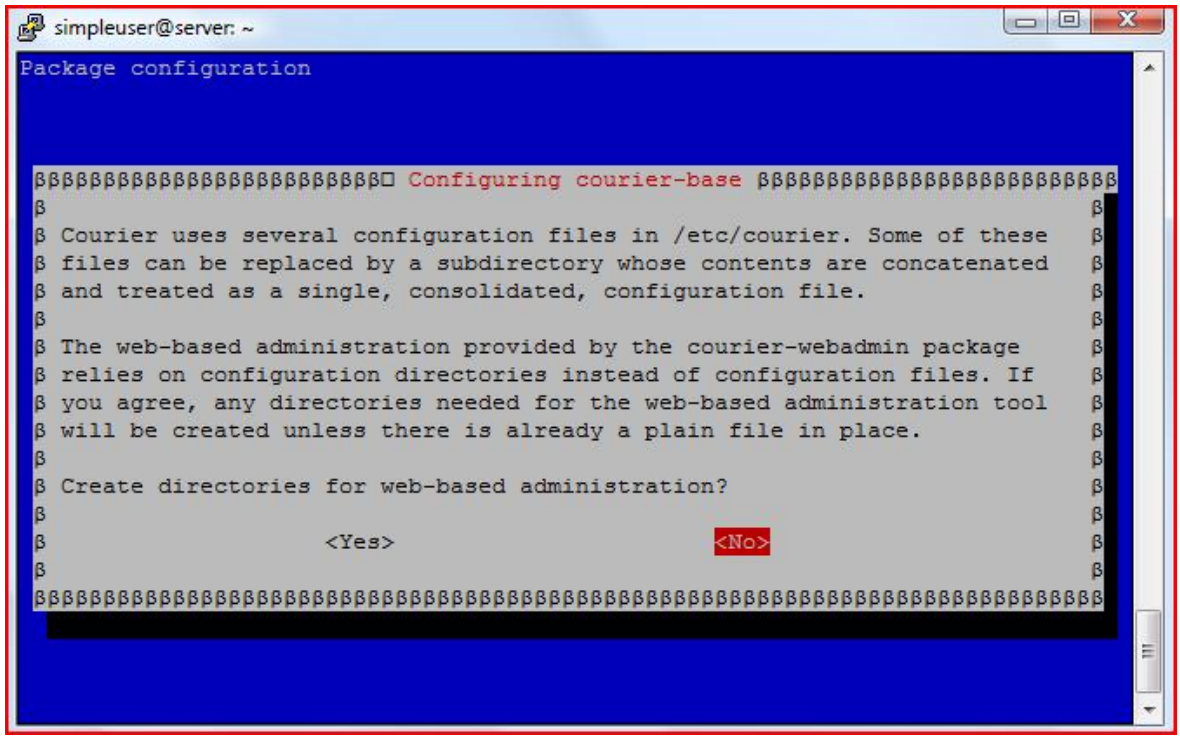
Οδηγία: Εισάγουμε τον επιθυμητό κωδικό χρήστη για το διαχειριστή της MySQL (root). Ισχύουν και εδώ όλα όσα έχουν αναφερθεί στο βήμα 9 της εγκατάστασης του βασικού συστήματος, σχετικά με τον κωδικό χρήστη του διαχειριστή:



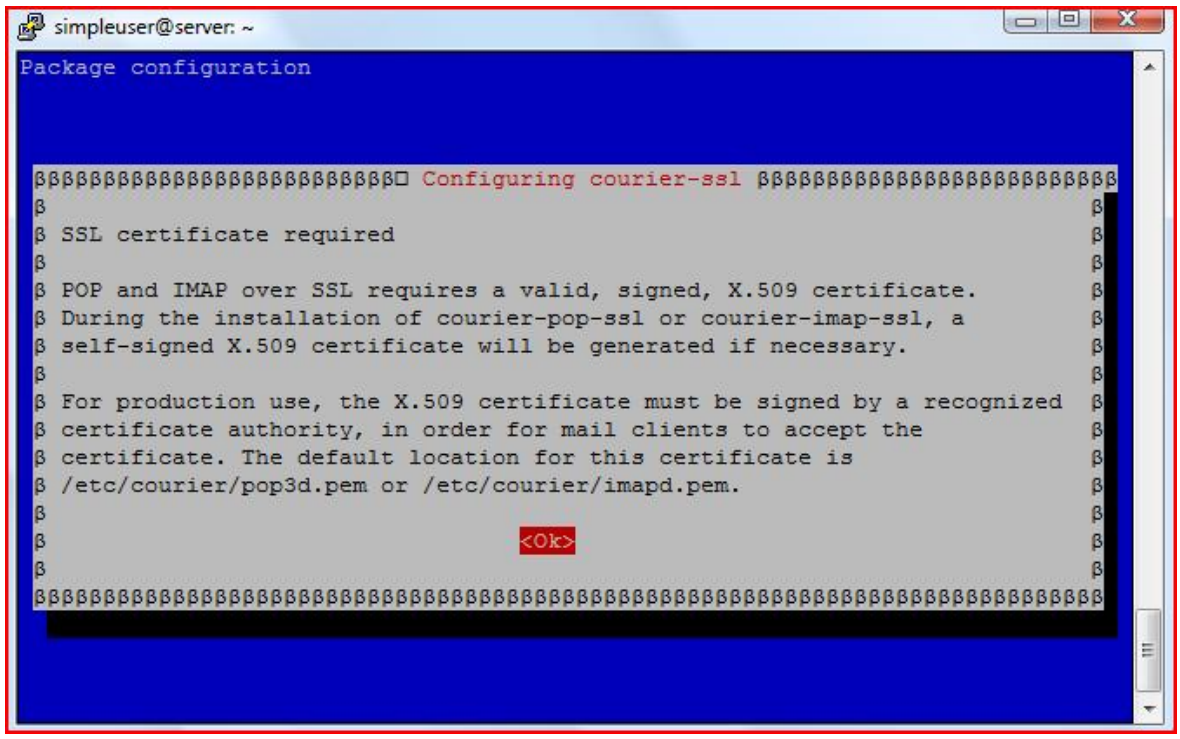
Οδηγία: Για αποφυγή λαθών πληκτρολόγησης, ζητείται εκ νέου η εισαγωγή του κωδικού χρήστη του διαχειριστή της MySQL:



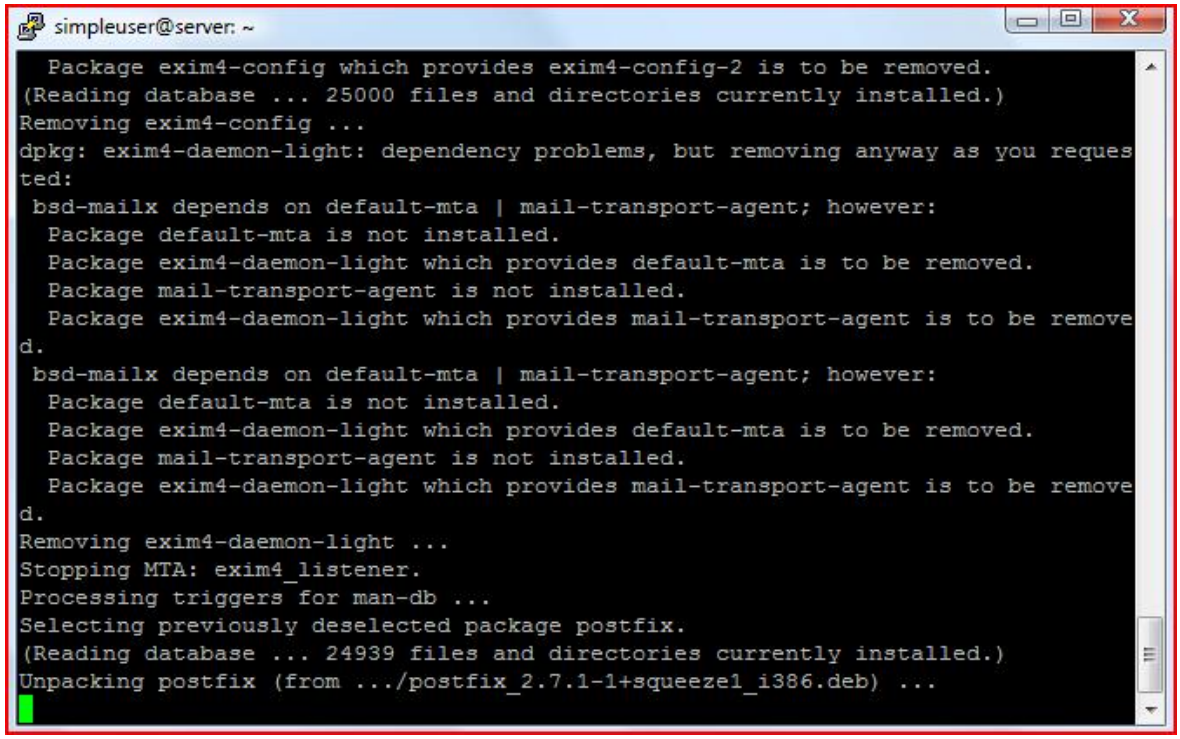
Οδηγία: Επιλέγουμε να μη δημιουργηθούν οι φάκελοι για τη web-based διαχείριση της εφαρμογής εξυπηρέτησης ηλεκτρονικού ταχυδρομείου courier (αυτή θα γίνεται διά μέσου του ISPConfig):



Οδηγία: Για τη χρήση των υπηρεσιών POP και IMAP με ασφαλή σύνδεση SSL, απαιτείται η δημιουργία των κατάλληλων X.509 πιστοποιητικών. Αυτή θα γίνει αυτόματα με προεπιλεγμένες ρυθμίσεις και τα πιστοποιητικά που θα παραχθούν, θα τοποθετηθούν στο φάκελο /etc/courier/:



Οδηγία: Η εγκατάσταση πραγματοποιείται:



Postfix με SSL

Για να ενεργοποιηθεί η δυνατότητα ασφαλούς σύνδεσης με την υπηρεσία αποστολής μηνυμάτων ηλεκτρονικής αλληλογραφίας (smtps), θα πρέπει να πραγματοποιηθούν οι απαραίτητες τροποποιήσεις στο αρχείο ρυθμίσεων master.cf της εφαρμογής Postfix.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο master.cf:

```
vi /etc/postfix/master.cf
```

Οδηγία: Αποσχολιάζουμε, διαγράφοντας τον πρώτο χαρακτήρα (#), τις γραμμές 17, 18, 19 και 20:

```
[...]
smtps     inet  n       -       -       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
[...]
```

Οδηγία: Επανεκκινούμε την εφαρμογή Postfix για να ισχύσουν άμεσα οι αλλαγές:

```
/etc/init.d/postfix restart
```

Επαναδημιουργία πιστοποιητικών SSL για IMAP και POP3

Κατά την εγκατάσταση των πακέτων της εφαρμογής courier δημιουργήθηκαν αυτόματα τα πιστοποιητικά που απαιτούνται, ώστε να υπάρχει η δυνατότητα παροχής ασφαλούς SSL πρόσβασης μέσω των πρωτοκόλλων IMAP και POP3. Για τη δημιουργία των πιστοποιητικών, χρησιμοποιήθηκαν οι προκαθορισμένες ρυθμίσεις και όχι τα πραγματικά στοιχεία που αφορούν στον εξυπηρετητή. Θα πρέπει λοιπόν να τροποποιηθούν κατάλληλα τα σχετικά αρχεία ρυθμίσεων, να διαγραφούν τα υπάρχοντα πιστοποιητικά και να δημιουργηθούν νέα.

Οδηγία: Διαγράφουμε τα υπάρχοντα πιστοποιητικά:

```
cd /etc/courier
rm -f /etc/courier/imapd.pem
rm -f /etc/courier/pop3d.pem
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο imapd.cnf:

```
vi /etc/courier/imapd.cnf
```

Οδηγία: Τροποποιούμε τις πληροφορίες σχετικά με τον ιδιοκτήτη του πιστοποιητικού στις γραμμές 12, 13, 14, 17 και 18 (C=χώρα, ST=περιοχή/νομός, L=τοποθεσία, CN=όνομα συστήματος, emailAddress=διεύθυνση ηλεκτρονικού ταχυδρομείου):

```
[...]
[ req_dn ]
C=GR
ST=Attiki
L=Sintagma
O=Courier Mail Server
OU=Automatically-generated IMAP SSL key
CN=server.mydomain.gr
emailAddress=webmaster@mydomain.gr
[...]
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο pop3d.cnf:

```
vi /etc/courier/pop3d.cnf
```

Οδηγία: Όπως και στην περίπτωση του imapd.cnf, τροποποιούμε τις πληροφορίες σχετικά με τον ιδιοκτήτη του τρέχοντος πιστοποιητικού στις γραμμές 12, 13, 14, 17 και 18 (C=χώρα, ST=περιοχή/νομός, L=τοποθεσία, CN=όνομα συστήματος, emailAddress=διεύθυνση ηλεκτρονικού ταχυδρομείου):

```
[...]
[ req_dn ]
C=GR
ST=Attiki
L=Sintagma
O=Courier Mail Server
OU=Automatically-generated POP3 SSL key
CN=server.mydomain.gr
emailAddress=webmaster@domain.gr
[...]
```

Οδηγία: Δημιουργούμε εκ νέου τα δύο πιστοποιητικά:

```
mkimapdcert
mkpop3dcert
```

Οδηγία: Επανεκκινούμε τις υπηρεσίες courier-imap-ssl και courier-pop-ssl, ώστε να ισχύσουν άμεσα οι αλλαγές:

```
/etc/init.d/courier-imap-ssl restart
/etc/init.d/courier-pop-ssl restart
```

Τροποποίηση παραμέτρου σύνδεσης MySQL

Η MySQL είναι προκαθορισμένη να επιτρέπει συνδέσεις μόνο τοπικά, στο σύστημα που έχει εγκατασταθεί (localhost). Έτσι, στην περίπτωση που για την παροχή των σχετικών υπηρεσιών χρησιμοποιηθούν περισσότεροι από έναν εξυπηρετητές, απαιτείται τροποποίηση του σχετικού αρχείου ρυθμίσεων, ώστε να υπάρχει η δυνατότητα σύνδεσης όλων αυτών των απομακρυσμένων συστημάτων στις εκάστοτε τοπικές βάσεις δεδομένων. Είναι βέβαια προφανές, ότι η συγκεκριμένη ενέργεια δεν είναι απαραίτητο να πραγματοποιηθεί στην περίπτωση που θα χρησιμοποιηθεί ένας και μόνο εξυπηρετητής διαδικτύου.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο my.cnf:

```
vi /etc/mysql/my.cnf
```

Οδηγία: Μετατρέπουμε σε σημείωση τη γραμμή 47 (bind-address =127.0.0.1) προσθέτοντας στη αρχή της γραμμής το χαρακτήρα σημείωσης (#):

```
[...]
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address           = 127.0.0.1
[...]
```

Οδηγία: Επανεκκινούμε τη MySQL:

```
/etc/init.d/mysql restart
```

Οδηγία: Ελέγχουμε ότι οι αλλαγές είναι σε ισχύ, συγκρίνοντας το αποτέλεσμα της εντολής:

```
netstat -tap | grep mysql
```

με το παρακάτω (θα πρέπει να υπάρχει το σύμβολο του άστρου πριν το «:mysql» και όχι το κανονικοποιημένο όνομα του εξυπηρετητή «localhost.localdomain»):

```
tcp   0   0   *:mysql   *:*   LISTEN   6782/mysqld
```

Εγκατάσταση Amavisd-new, SpamAssassin, Clamav, εφαρμογών συμπίεσης αρχείων

Στο τρέχων βήμα θα συνεχιστεί η εγκατάσταση εφαρμογών που απαιτούνται για τη λειτουργία του ISPConfig. Συγκεκριμένα, θα εγκατασταθούν εφαρμογές που σχετίζονται με τον έλεγχο των μηνυμάτων, καθώς και των συνημμένων αυτών, κατά τη διακίνηση της ηλεκτρονικής αλληλογραφίας.

- **Amavisd-new** [48]: Πρόκειται για μια υψηλών επιδόσεων, αξιόπιστη εφαρμογή «γεφύρωσης» των εφαρμογών διακίνησης ηλεκτρονικής αλληλογραφίας και των εφαρμογών ελέγχου περιεχομένων αυτής (εφαρμογές ανίχνευσης ιών ή ανεπιθύμητης αλληλογραφίας).

- **SpamAssassin** [49, 50]: Είναι μια ικανότατη εφαρμογή καταπολέμησης της ανεπιθύμητης αλληλογραφίας. Το spamassassin χρησιμοποιώντας μια ποικιλία τεχνικών εντοπισμού, καθιστά αδύνατη την παράκαμψή του από

τους επίδοξους spammers. Μάλιστα, το 2006 βραβεύτηκε με το Linux New Media Award, ως η καλύτερη λύση καταπολέμησης ανεπιθύμητης αλληλογραφίας σε συστήματα GNU/Linux.

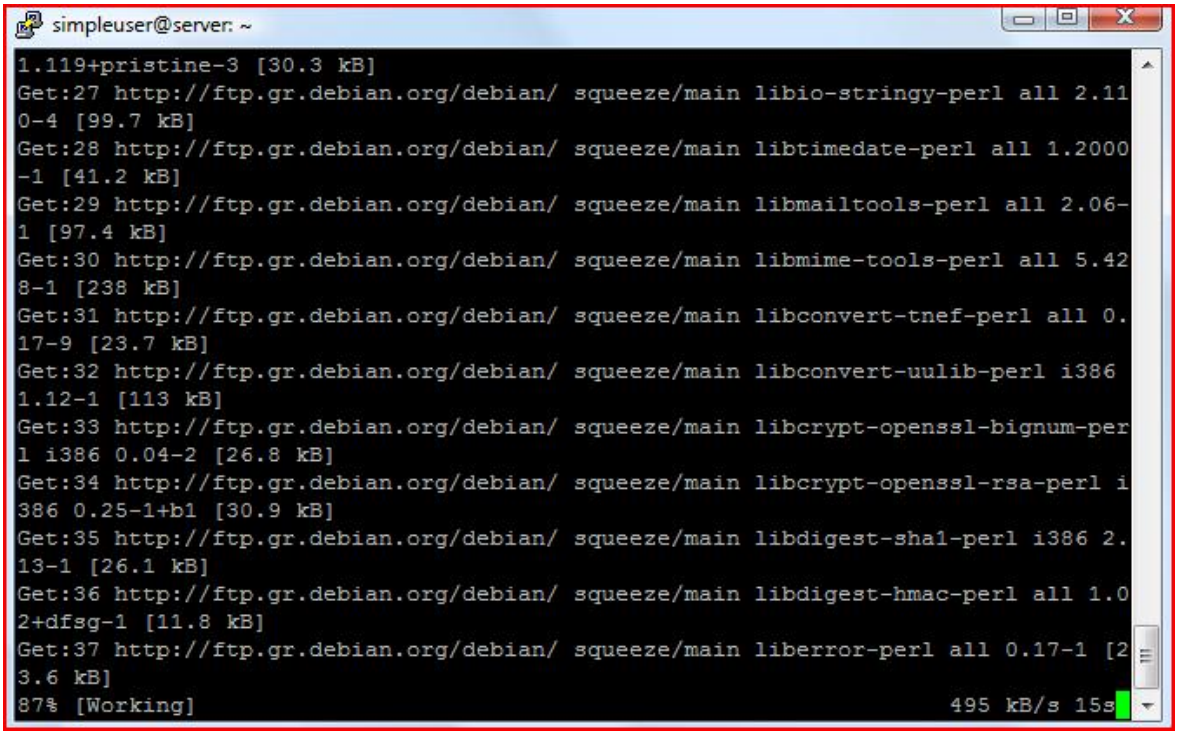
- **Clamav** [51, 52]: Δωρεάν, ανεξάρτητη πλατφόρμας εφαρμογή ανίχνευσης κακόβουλου λογισμικού. Το Clam AntiVirus σχεδιάστηκε ειδικά για τη συγκεκριμένη χρήση και πλέον αποτελεί το «de facto» στάνταρντ του λογισμικού ανίχνευσης κακόβουλου λογισμικού σε εξυπηρετητές ηλεκτρονικού ταχυδρομείου, όπου πραγματοποιεί έλεγχο των συνημμένων της ηλεκτρονικής αλληλογραφίας.

- **Εφαρμογές συμπίεσης - αποσυμπίεσης αρχείων**: Παράλληλα με τις ανωτέρω εφαρμογές, για τον πλήρη έλεγχο της ηλεκτρονικής αλληλογραφίας απαιτείται και θα πραγματοποιηθεί η εγκατάσταση εφαρμογών συμπίεσης - αποσυμπίεσης αρχείων, ώστε να είναι δυνατός ο έλεγχος των περιεχομένων σε ένα συμπιεσμένο, συνημμένο αρχείο, σε μήνυμα ηλεκτρονικού ταχυδρομείου. Οι εφαρμογές αυτού του τύπου, που θα εγκατασταθούν είναι οι zoo, unzip, bzip2, arj, nomarch, lzop, cabextract και zip.

Οδηγία: Εκτελούμε την παρακάτω εντολή και επιβεβαιώνουμε την πρόθεσή μας για εγκατάσταση των επιλεγμένων πακέτων με «enter»:

```
  apt-get install amavisd-new spamassassin clamav clamav-
daemon zoo unzip bzip2 arj nomarch lzop cabextract apt-
listchanges libnet-ldap-perl libauthen-sasl-perl clamav-docs
daemon libio-string-perl libio-socket-ssl-perl libnet-ident-
perl zip libnet-dns-perl
```

Οδηγία: Πραγματοποιείται η εγκατάσταση των πακέτων που ζητήσαμε:



Οδηγία: Η εφαρμογή Amavisd φορτώνει εσωτερικά τη βιβλιοθήκη φίλτρων του SpamAssassin, έτσι δεν είναι απαραίτητο να εκτελείται το τελευταίο για να επιτυγχάνεται ο έλεγχος της ηλεκτρονικής αλληλογραφίας. Συνεπώς, σταματάμε τη λειτουργία του και απενεργοποιούμε την εκτέλεσή του κατά την εκκίνηση του συστήματος:

```
/etc/init.d/spamassassin stop
update-rc.d -f spamassassin remove
```

Εγκατάσταση Apache2, PHP5, phpMyAdmin, FCGI, suExec, Pear, mcrypt

Συνεχίζεται και στο παρών βήμα η εγκατάσταση του απαιτούμενου για τη λειτουργία του ISPConfig λογισμικού, με εστίαση στην ομάδα των παρακάτω εφαρμογών.

- **Apache2** [53]: Δημοφιλής, ανοιχτού κώδικα, εξυπηρετητής Παγκόσμιου Ιστού (web server), για σύγχρονα λειτουργικά συστήματα, μεταξύ των οποίων τα unix-οειδή και τα windows. Στόχος του εγχειρήματος σχεδιασμού και ανάπτυξης του Apache HTTP server ήταν και εξακολουθεί να είναι η παροχή ενός ασφαλούς, επαρκούς και επεκτάσιμου εξυπηρετητή, ο οποίος θα είναι σε θέση να παράσχει υπηρεσίες ιστού, εναρμονισμένες με τα τρέχοντα

πρότυπα http. Ο συγκεκριμένος στόχος φαίνεται να έχει επιτευχθεί και με το παραπάνω, εάν αναλογιστεί κανείς την αποδοχή που ο Apache απολαμβάνει από τους υπευθύνους συστημάτων παροχής υπηρεσιών Παγκοσμίου Ιστού (ο Apache σήμερα εξυπηρετεί σχεδόν τα ¾ των εν λόγω συστημάτων).

- **PHP5** [54, 55]: Η PHP είναι γλώσσα προγραμματισμού που χρησιμοποιείται για τη δημιουργία σελίδων του παγκοσμίου ιστού, οι οποίες έχουν δυναμικό περιεχόμενο. Μια σελίδα δυναμικού περιεχομένου PHP θα πρέπει να υποστεί επεξεργασία από ένα συμβατό εξυπηρετητή ιστού (π.χ. Apache), ώστε να παραχθεί σε πραγματικό χρόνο το τελικό περιεχόμενο, το οποίο και θα σταλεί στο πρόγραμμα περιήγησης των επισκεπτών σε μορφή κώδικα HTML.

- **phpMyAdmin** [56, 57]: Πρόκειται για μια ανοιχτού κώδικα εφαρμογή, η οποία έχει γραφεί σε γλώσσα PHP, ειδικά για τη διαχείριση των εξυπηρετητών MySQL. Η πρόσβαση στην εφαρμογή επιτυγχάνεται με ένα απλό περιηγητή ιστοσελίδων, μέσω του οποίου προσφέρεται στο χρήστη ένα γραφικό περιβάλλον διεπαφής, από όπου μπορούν να πραγματοποιηθούν εργασίες διαχείρισης βάσεων δεδομένων.

- **FastCGI** [58, 59]: Το FastCGI ή FCGI είναι ένα πρωτόκολλο διασύνδεσης διαδραστικών προγραμμάτων και εξυπηρετητών Παγκοσμίου Ιστού. Αποτελεί μια παραλλαγή του παλαιότερου Common Gateway Interface (CGI) και έχει κύριο λόγο ύπαρξης την προσπάθεια περιορισμού του συνολικού «κόστους» της διασύνδεσης, επιτρέποντας έτσι στον εξυπηρετητή να διαχειρίζεται ταυτόχρονα περισσότερες αιτήσεις.

- **suExec** [60, 61]: Το suEXEC είναι ένα πρόσθετο χαρακτηριστικό του εξυπηρετητή ιστού Apache, το οποίο επιτρέπει στους χρήστες του να εκτελούν εφαρμογές CGI και SSI ως διαφορετικοί χρήστες (κανονικά όλες οι διεργασίες του εξυπηρετητή ιστού εκτελούνται με τον προκαθορισμένο λογαριασμό χρήστη). Με σωστή χρήση, το suEXEC περιορίζει σημαντικά την επικινδυνότητα ασφαλείας που εμπεριέχεται στη δυνατότητα των χρηστών να αναπτύσσουν και να εκτελούν ιδιωτικές εφαρμογές CGI και SSI.

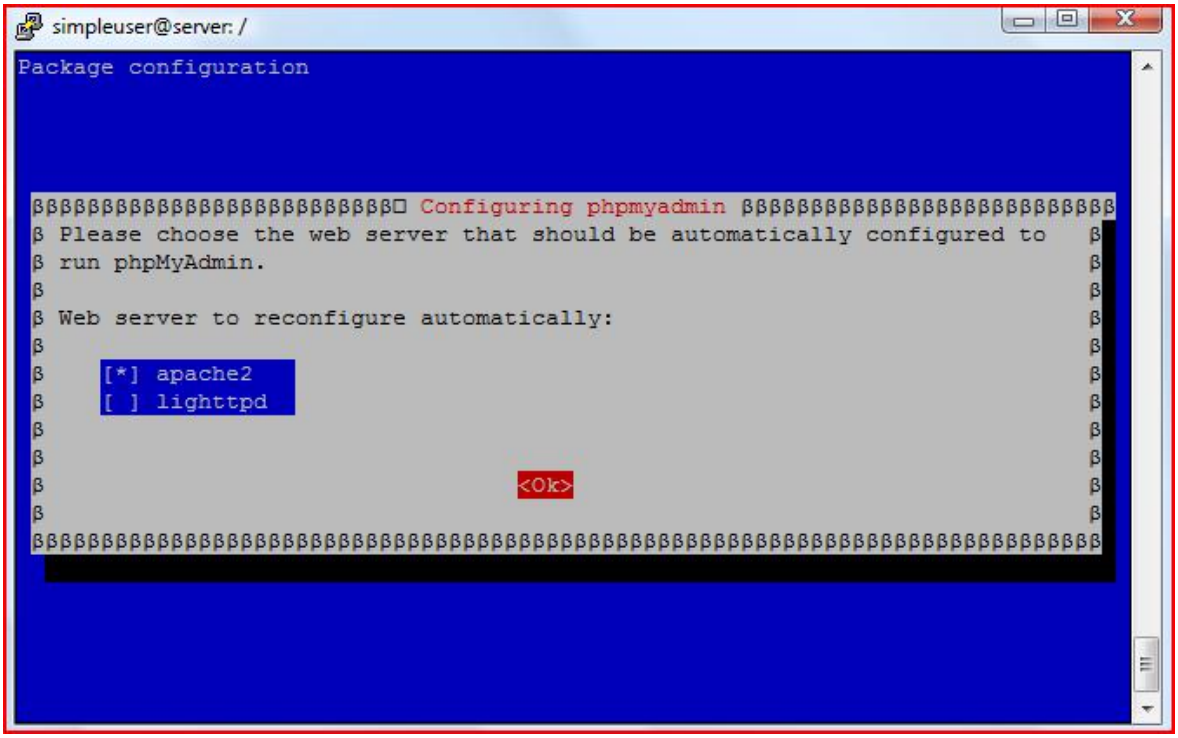
- **Pear** [62]: Το ακρωνύμιο PEAR προκύπτει από το πλήρες "PHP Extension and Application Repository" και αφορά σε ένα πλαίσιο εργασίας (framework), το οποίο έχει δημιουργηθεί για να παρέχει:
  - Μια δομημένη βιβλιοθήκη ανοιχτού κώδικα για τους χρήστες της PHP
  - Ένα σύστημα διανομής κώδικα και διαχείρισης πακέτων
  - Ένα πρότυπο για κώδικα γραμμένο σε PHP
  - Έναν ιστοχώρο, μια λίστα ηλεκτρονικού ταχυδρομείου καθώς και καθρέφτες μεταφορτώσεων για την υποστήριξη της κοινότητας PHP/PEAR.

- **mcrypt** [63, 64]: Εργαλείο κρυπτοποίησης που δημιουργήθηκε με σκοπό να αντικαταστήσει τη δημοφιλή εντολή crypt των συστημάτων Unix. Επιτρέπει στους προγραμματιστές να χρησιμοποιούν μια ευρεία γκάμα συναρτήσεων κρυπτοποίησης, χωρίς να χρειάζεται να τροποποιήσουν σημαντικά τον κώδικά τους. Χρησιμοποιεί σύγχρονους αλγόριθμους, μεταξύ των οποίων περιλαμβάνονται οι des, blowfish, arcfour, enigma, ghost, LOKI97, RC2, serpent, threeway, twofish, wake, XTEA.

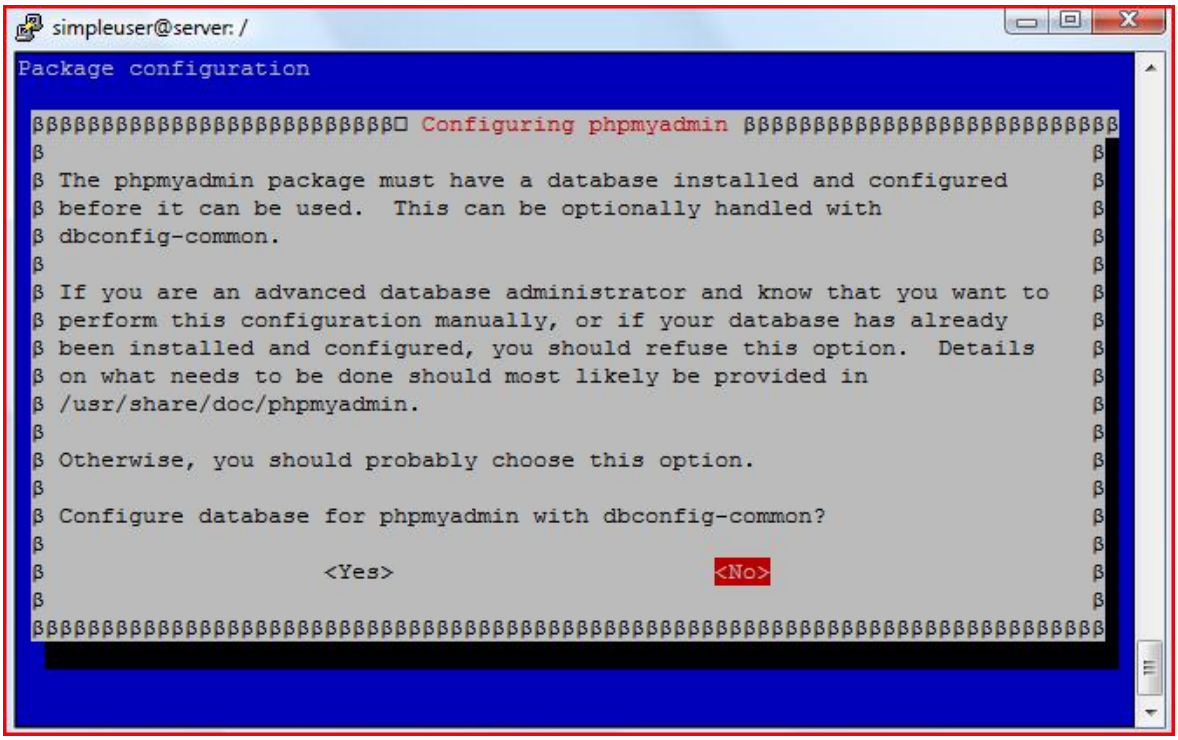
Οδηγία: Εκτελούμε την παρακάτω εντολή και επιβεβαιώνουμε την πρόθεσή μας για εγκατάσταση των επιλεγμένων πακέτων με «enter»:

```
  apt-get install apache2 apache2.2-common apache2-doc
apache2-mpm-prefork apache2-utils libexpat1 ssl-cert
libapache2-mod-php5 php5 php5-common php5-gd php5-mysql php5-
imap phpmyadmin php5-cli php5-cgi libapache2-mod-fcgid
apache2-suexec php-pear php-auth php5-mcrypt mcrypt php5-
imagick imagemagick libapache2-mod-suphp libruby libapache2-
mod-ruby
```

Οδηγία: Επιλέγουμε αυτόματη παραμετροποίηση του εξυπηρετητή ιστού apache2:



Οδηγία: Επιλέγουμε να μην γίνει διαχείριση της βάσης δεδομένων για την εφαρμογή phpMyAdmin με το dbconfig-common:



Οδηγία: Εκτελούμε την παρακάτω εντολή για να ενεργοποιηθούν τα αρθρώματα suexec, rewrite, ssl, actions, και include του Apache:

```
a2enmod suexec rewrite ssl actions include
```

Οδηγία: Επανεκκινούμε τον Apache για να ισχύσουν άμεσα οι αλλαγές:

```
/etc/init.d/apache2 restart
```

Εγκατάσταση των PureFTPd και Quota.

Πραγματοποιείται ένα ακόμη βήμα εγκατάστασης εφαρμογών, απαιτούμενων για τη λειτουργία του ISPConfig. Στο τρέχων βήμα θα εγκατασταθούν οι εφαρμογές:

- **PureFTPd** [65, 66]: Ο PureFTPd είναι ένας υψηλής ποιότητας, ασφαλής εξυπηρετητής FTP, ο οποίος εναρμονίζεται με τις προδιαγραφές του πρωτοκόλλου File Transfer Protocol και διατίθεται δωρεάν. Η ομάδα ανάπτυξής του εστιάζει στην ασφάλεια και επιδιώκει απλότητα και αποτελεσματικότητα, παρέχοντας απλές λύσεις στις συνήθεις απαιτήσεις και ταυτόχρονα, επιπλέον χαρακτηριστικά για πιο εξειδικευμένες χρήσεις.

- **Quota** [67]: Πρόκειται για ένα προαιρετικό χαρακτηριστικό του λειτουργικού συστήματος, το οποίο επιτρέπει τον περιορισμό των χρηστών σχετικά με τη χρήση του συστήματος αρχείων. Χρησιμοποιώντας αυτού του είδους την ποσόστωση σε ένα πολυχρηστικό περιβάλλον, όπως αυτό ενός διαδικτυακού εξυπηρετητή, ο διαχειριστής είναι σε θέση να καθορίσει αφενός το μέρος της χωρητικότητας του δίσκου που θα μπορεί να χρησιμοποιήσει ο κάθε χρήστης, αφετέρου τον αριθμό των αρχείων που θα μπορούν να δημιουργηθούν στον καθορισμένο χώρο. Ένα δεύτερο, χρησιμότατο εργαλείο που θα εγκατασταθεί με την εφαρμογή quota, είναι το quotatool, το οποίο επιτρέπει τον καθορισμό των παραμέτρων ποσόστωσης από τη γραμμή εντολών, χωρίς να απαιτείται αλληλεπίδραση με το χρήστη.

Οδηγία: Εκτελούμε την παρακάτω εντολή και επιβεβαιώνουμε την πρόθεσή μας για εγκατάσταση των επιλεγμένων πακέτων με «enter»:

```
  apt-get install pure-ftpd-common pure-ftpd-mysql quota
quotatool
```

Για τη σωστή λειτουργία του ISPConfig θα πρέπει ο εξυπηρετητής PureFTPd να εκκινεί ως αυτόνομος δαίμονας και όχι να είναι ελεγχόμενος από το inetd. Επιπλέον, θα πρέπει να γίνει η κατάλληλη ρύθμιση, ώστε να μπορούν οι απομονωμένοι (chrooted) χρήστες να ακολουθούν τους συμβολικούς δεσμούς (symlinks), ακόμη και στην περίπτωση που οι τελευταίοι δείχνουν έξω από τον χώρο, στον οποίο οι χρήστες έχουν περιοριστεί.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων του PureFTPd, pure-ftpd-common:

```
  vi /etc/default/pure-ftpd-common
```

Οδηγία: Στη γραμμή 7 βεβαιωνόμαστε ότι η τιμή της μεταβλητής STANDALONE_OR_INETD είναι standalone (διαφορετικά την τροποποιούμε κατάλληλα) και στη γραμμή 13 αλλάζουμε την τιμή της VIRTUALCHROOT από false σε true:

```
  [...]
  STANDALONE_OR_INETD=standalone
  [...]
  VIRTUALCHROOT=true
  [...]
```

Οδηγία: Έλεγχος των ρυθμίσεων του inetd σχετικά με την εκκίνηση της υπηρεσίας PureFTPd. Ανοίγουμε το αρχείο inetd.conf:

```
  vi /etc/inetd.conf
```

Οδηγία: Βεβαιωνόμαστε ότι αν υπάρχει γραμμή που περιλαμβάνει την εντολή εκκίνησης του PureFTPd (όπως στο παράδειγμα), αυτή είναι μαρκαρισμένη ως σημείωση:

```
  [...]
  #:STANDARD: These are standard services.
  #ftp    stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/pure-
ftpd-wrapper
  [...]
```

Οδηγία: Εάν χρειάστηκε να τροποποιήσουμε το αρχείο inetd.conf, θα πρέπει να επανεκκινήσουμε την υπηρεσία inetd:

```
  /etc/init.d/openbsd-inetd restart
```

Το πρωτόκολλο FTP είναι σχεδιασμένο ώστε να πραγματοποιεί όλες τις μεταφορές δεδομένων, ακόμα και αυτές των κωδικών πρόσβασης, με τη μορφή απλού κειμένου και έτσι, δεν είναι καθόλου ασφαλές! Εάν αυτό δεν είναι επιθυμητό, υπάρχει η δυνατότητα χρήσης του συγκεκριμένου πρωτοκόλλου πάνω από συνεδρία TLS, η οποία θα κρυπτοποιήσει τα δεδομένα πριν τη μεταφορά τους. Η σχετική ρύθμιση βρίσκεται στο αρχείο /etc/pure-ftpd/conf/TLS και μπορεί να έχει τις παρακάτω τιμές:

- μη ύπαρξη του αρχείου TLS ή τιμή «0»: επιτρέπονται μόνο απλές FTP συνεδρίες
- τιμή «1»: επιτρέπονται απλές FTP, αλλά και FTP πάνω από TLS (ασφαλείς) συνεδρίες
- τιμή «2»: επιτρέπονται μόνο FTP πάνω από TLS (ασφαλείς) συνεδρίες

Οδηγία: Δημιουργούμε και ρυθμίζουμε ανάλογα το αρχείο TLS. Για παράδειγμα, εάν η πολιτική ασφαλείας του εξυπηρετητή μας δεν επιτρέπει τις μη ασφαλείς FTP συνεδρίες, τότε θα πρέπει να δημιουργήσουμε το αρχείο TLS με περιεχόμενο την τιμή «2», εκτελώντας την παρακάτω εντολή:

```
  echo 2 > /etc/pure-ftpd/conf/TLS
```

Για να χρησιμοποιήσουμε τις ασφαλείς συνεδρίες FTP πάνω από TLS, θα πρέπει με τα ακόλουθα βήματα να δημιουργήσουμε ένα SSL πιστοποιητικό.

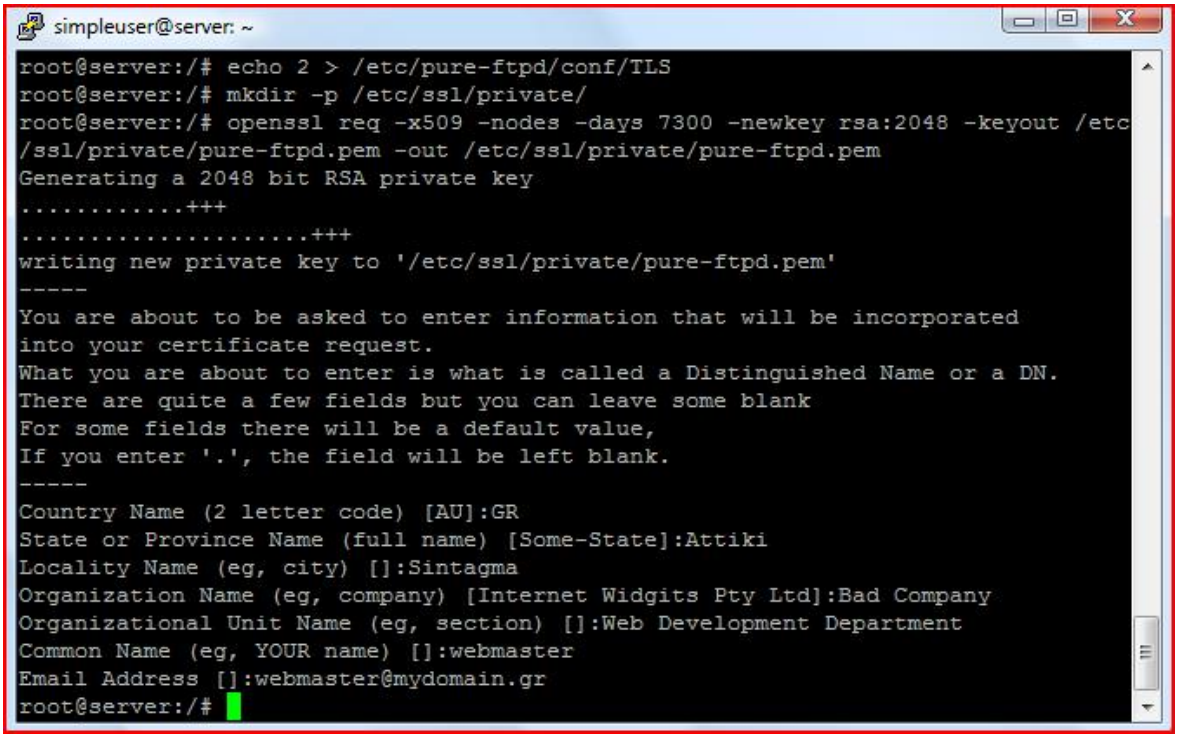
Οδηγία: Αρχικά δημιουργούμε το φάκελο που θα φιλοξενήσει το πιστοποιητικό (/etc/ssl/private/):

```
  mkdir -p /etc/ssl/private/
```

Οδηγία: Στη συνέχεια, δημιουργούμε το πιστοποιητικό με την εντολή:

```
  openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -
keyout /etc/ssl/private/pure-ftpd.pem -out
/etc/ssl/private/pure-ftpd.pem
```

Οδηγία: Εισάγουμε τις πληροφορίες σχετικά με τον ιδιοκτήτη του πιστοποιητικού, όπως στις τελευταίες οκτώ (8) γραμμές του παρακάτω παραδείγματος:



Οδηγία: Τροποποιούμε τα δικαιώματα (permissions) του πιστοποιητικό που μόλις δημιουργήσαμε, απαγορεύοντας στους υπόλοιπους χρήστες την πρόσβαση σε αυτό:

```
  chmod 600 /etc/ssl/private/pure-ftpd.pem
```

Οδηγία: Επανεκκινούμε την υπηρεσία PureFTPd για να ισχύσουν άμεσα οι αλλαγές:

```
  /etc/init.d/pure-ftpd-mysql restart
```

Το αρχείο fstab (File Systems TABle) είναι ένα αρχείο ρυθμίσεων στα λειτουργικά συστήματα GNU/Linux, στο οποίο διατηρείται μια λίστα με όλους τους διαθέσιμους δίσκους αποθήκευσης δεδομένων, τις κατατμήσεις αυτών, καθώς και το πως θα γίνει η ενσωμάτωσή τους στο σύστημα αρχείων. Στον εν λόγω αρχείο θα πρέπει να ενσωματωθούν οι επιλογές userquota και grpguota (μαζί με τις παραμέτρους τους), στην κατάλληλη κατάτμηση, ώστε στη συνέχεια να ενεργοποιηθεί με επιτυχία η ποσόστωση (quota).

Οδηγία: Ανοίγουμε το αρχείο fstab για επεξεργασία:

```
vi /etc/fstab
```

Οδηγία: Στην κατάτμηση με σημείο προσάρτησης «/home», μετά το είδος του συστήματος αρχείων (ext4), αντικαθιστούμε την επιλογή «defaults» με «errors=remount-ro,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0»:

```
[...]
# /home was on /dev/sda2 during installation
UUID=b149ca0a-b9e0-42de-a184-146d45d85c1b /home ext4 errors=remount-ro,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0 0 2
# swap was on /dev/sda3 during installation
[...]
```

Το ISPConfig χρησιμοποιεί το φάκελο «/var/www» για τη δημιουργία των φακέλων των νέων χρηστών. Στη μέχρι τώρα εγκατάσταση όμως γίνεται προετοιμασία για χρήστη του σημείου προσάρτησης «/home» για τους φακέλους χρηστών. Θα πρέπει λοιπόν, αφενός να μετακινηθεί ο υπάρχον φάκελος «/var/www» στο φάκελο «/home», αφετέρου, να δημιουργηθεί ένας συμβολικός δεσμός (symlink) που θα δείχνει στη νέα θέση από την παλαιά, ώστε να λειτουργεί απροβλημάτιστα το ISPConfig.

Οδηγία: Εκτελούμε τις παρακάτω εντολές για να μετακινήσουμε το φάκελο /var/www στο /home και για να δημιουργήσουμε το συμβολικό δεσμό που θα δείχνει από το /var/www στο /home/www:

```
mv /var/www /home
ln -s /home/www /var/www
```

Οδηγία: Εκτελούμε τις παρακάτω εντολές για να ενεργοποιήσουμε την ποσόστωση:

```
mount -o remount /home
quotacheck -avugm
quotaon -avug
```

Οδηγία: Μετά την εκτέλεση της τελευταίας εντολής θα πρέπει να ενημερωθούμε για την επιτυχία ενεργοποίησης της ποσόστωσης με το μήνυμα:

```
/dev/sda2 [/home]: group quotas turned on
/dev/sda2 [/home]: user quotas turned on
```

Οδηγία: Περαιτέρω πληροφορίες σχετικά με την ποσόστωση μπορούμε να αντλούμε με την εντολή «repquota -u /home», η οποία θα πρέπει σε αυτό το σημείο να επιστρέψει τα ακόλουθα:

```
*** Report for user quotas on device /dev/sda2
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used soft hard grace    used soft hard grace
----------------------------------------------------------------------
root       --      28       0       0              4       0       0
simpleuser --      20       0       0              5       0       0
```

Εγκατάσταση BIND

Ο BIND [68, 69] ή αλλιώς named, είναι ο πιο χρησιμοποιημένος εξυπηρετητής ονομάτων τομέα (DNS) στο διαδίκτυο, υποστηρίζεται από το Internet Software Consortium (www.isc.org) και αποτελεί το «de facto» πρότυπο στα συστήματα GNU/Linux. Μαζί με τον BIND, θα γίνει εγκατάσταση και του προαιρετικού πακέτου dnsutils [70], το οποίο περιέχει εργαλεία προγραμμάτων - πελάτη που έχουν προκύψει από τον BIND.

Οδηγία: Εγκαθιστούμε τα πακέτα bind9 και dnsutils με την εντολή:

```
apt-get install bind9 dnsutils
```

Εγκατάσταση Vlogger, Webalizer, AWstats, geoip-database

Ένα ακόμη βήμα εγκατάστασης εφαρμογών, απαιτούμενων για τη λειτουργία του ISPConfig:

- **Vlogger** [71]: Είναι μια εφαρμογή που σχεδιάστηκε και αναπτύχθηκε για να αντιμετωπίσει το πρόβλημα διαχείρισης των αρχείων καταγραφής στους εξυπηρετητές διαδικτύου. Είναι σε θέση να διαχωρίσει τα αρχεία καταγραφής, ανά χρήστη ή/και ανά επιθυμητό χρονικό διάστημα (πχ ημέρας).

- **Webalizer** [72, 73]: Πρόκειται για μια πολυγλωσσική εφαρμογή ανάλυσης και οπτικοποίησης των αρχείων καταγραφής. Παρά την ευκολία ρύθμισής της, είναι σε θέση να παράγει υψηλής λεπτομέρειας αναφορές χρήσης (σε μορφή HTML, ώστε να είναι εύκολα προσβάσιμες μέσα από κάποιον απλό περιηγητή διαδικτύου).

- **AWstats** [74, 75]: Εφαρμογή παρόμοια με τη webalizer, διαβάζει τα αρχεία καταγραφής και παράγει σελίδες ιστού με όλες τις διαθέσιμες σε αυτά πληροφορίες σε μορφή γραφικών.

- **geoip-database** [76]: Εργαλείο, που περιλαμβάνει τη δωρεάν βάση δεδομένων GeoLiteCountry, στην οποία μπορεί να αναζητηθεί η χώρα που αντιστοιχεί σε μια δοθείσα διεύθυνση IP ή ένα δοθέν όνομα συστήματος.

Οδηγία: Εγκαθιστούμε τα προαναφερθέντα πακέτα με την εντολή:

```
apt-get install vlogger webalizer awstats geoip-database
```

Η εφαρμογή awstats, κατά την εγκατάστασή της, δημιουργεί δύο νέες προγραμματισμένες εργασίες (cron jobs), τις οποίες θα πρέπει να απενεργοποιήσουμε,

χαρακτηρίζοντάς τες ως σημείωση (comment out), μιας και το IPSConfig θα δημιουργεί αυτόματα τις απαραίτητες καταχωρίσεις.

Οδηγία: Ανοίγουμε το αρχείο awstats για επεξεργασία:

```
vi /etc/cron.d/awstats
```

Οδηγία: Μετατρέπουμε σε σημείωση τις δύο προγραμματισμένες εργασίες, εισάγοντας το χαρακτήρα σημείωσης (#) στην αρχή των γραμμών 1 και 4:

```
#*/10 * * * * www-data [ -x /usr/share/awstats/tools/update.sh ] &&
/usr/share/awstats/tools/update.sh

# Generate static reports:
#10 03 * * * www-data [ -x /usr/share/awstats/tools/buildstatic.sh ]
&& /usr/share/awstats/tools/buildstatic.sh
```

Εγκατάσταση fail2ban

Η εφαρμογή fail2ban [77, 78] δεν ανήκει στο σύνολο των εφαρμογών που απαιτούνται για τη λειτουργία του ISPConfig και έτσι χαρακτηρίζεται από την ομάδα ανάπτυξής του ως προαιρετική (παρόλο που ακόμη και σε περίπτωση μη εγκατάστασής της θα εξακολουθεί να γίνεται η προσπάθεια προβολής των σχετικών αρχείων καταγραφής). Ωστόσο, η φύση της συγκεκριμένης εφαρμογής την εντάσσει σε αυτές που στοχεύουν στην ασφαλή λειτουργία του συστήματος στο οποίο εγκαθίστανται. Για το λόγο αυτό, στον οδηγό της παρούσας εργασίας η εφαρμογή fail2ban έχει αποφασιστεί να χαρακτηριστεί ως απαραίτητη για την επίτευξη και διατήρηση ενός υψηλού επιπέδου ασφάλειας του εξυπηρετητή και θα εγκατασταθεί. Μετά την εγκατάστασή της, η εν λόγω εφαρμογή θα «παρακολουθεί» τον εξυπηρετητή, «διαβάζοντας» σε συνεχή βάση τα αρχεία καταγραφής συμβάντων αυτού. Έτσι, στην περίπτωση που αυτό απαιτηθεί, θα απαγορεύει την πρόσβαση σε αυτόν συγκεκριμένων διευθύνσεων IP, οι οποίες θα έχουν δείξει σημάδια κακόβουλης χρήσης, όπως πολλαπλές εισαγωγές λανθασμένου κωδικού χρήστη, προσπάθεια εντοπισμού αδυναμιών του συστήματος κτλ.

Η τυπική αντίδραση της fail2ban μετά από εντοπισμό κακόβουλης χρήσης περιλαμβάνει την κατάλληλη ενημέρωση των κανόνων του τείχους προστασίας (firewall

rules), ή εναλλακτικά του πίνακα του TCP Wrapper, ούτως ώστε να αποκλείεται για συγκεκριμένο χρονικό διάστημα η διεύθυνση IP από την οποία πραγματοποιήθηκε η κακόβουλη χρήση. Επιπλέον, η εφαρμογή μπορεί να ρυθμιστεί ώστε να εκτελεί και άλλες ενέργειες που μπορούν να εκτελεστούν με Python scripts, από την αποστολή ενημερωτικού μηνύματος ηλεκτρονικού ταχυδρομείου στο διαχειριστή του συστήματος, μέχρι και, όπως χαρακτηριστικά αναφέρεται στην επίσημη ιστοσελίδα της, την εξαγωγή του δίσκου του αναγνώστη οπτικών δίσκων (CD-ROM).

Η λειτουργία της εφαρμογής βασίζεται σε φίλτρα, τα οποία θα πρέπει να δημιουργηθούν για καθεμία από τις υπό έλεγχο υπηρεσίες. Τα φίλτρα αυτά σχηματίζονται με χρήση κανονικών εκφράσεων (regexes ή regular expressions), οι οποίες και τα καθιστούν πολύ εύκολα παραμετροποιήσιμα. Ο συνδυασμός ενός φίλτρου και της ενέργειας που αντιστοιχεί σε αυτό είναι γνωστός ως «φυλακή» (jail). Τέτοια «φυλακή» είναι δυνατό να καθοριστεί για να αποτραπεί η κακόβουλη χρήση οποιασδήποτε υπηρεσίας δικτύου του συστήματος, αρκεί η συγκεκριμένη υπηρεσία να διατηρεί αρχείο καταγραφής συμβάντων.

Δύο μειονεκτήματα που προς το παρόν παρουσιάζει η εφαρμογή fail2ban είναι η έλλειψη υποστήριξης της νέας γενιάς διευθύνσεων IPv6, καθώς και η έλλειψη δυνατότητας προστασίας του συστήματος απέναντι σε «κατανεμημένες βίαιες επιθέσεις» (distributed brute force attacks), στις οποίες η διεύθυνση IP του κακόβουλου χρήστη δεν παραμένει σταθερή.

Οδηγία: Εγκαθιστούμε την εφαρμογή fail2ban με την εντολή:

```
apt-get install fail2ban
```

Όπως αναφέρθηκε και παραπάνω, η κάθε «φυλακή» είναι συνδυασμός ενός φίλτρου, με βάση το οποίο θα πραγματοποιηθεί έρευνα για κακόβουλη χρήση, καθώς και της αντίστοιχης ενέργειας αντιμετώπισης αυτής (συνήθως αποκλεισμός του κακόβουλου χρήστη). Σε κάθε «φυλακή» επιτρέπεται η χρήση ενός και μόνο φίλτρου, υπάρχει όμως η δυνατότητα εισαγωγής περισσότερων της μιας ενέργειας (όπως για παράδειγμα αποκλεισμός του κακόβουλου χρήστη, εύρεση επιπλέον πληροφοριών που αφορούν σε

αυτόν και τέλος, αποστολή ενημερωτικού μηνύματος ηλεκτρονικού ταχυδρομείου στο διαχειριστή του συστήματος).

Η τυπική δομή μιας «φυλακής» περιλαμβάνει την επικεφαλίδα της (πχ [ssh-dos]), τη μεταβλητή που καθορίζει εάν η συγκεκριμένη «φυλακή» είναι ενεργοποιημένη ή όχι (πχ enabled = true), την πόρτα δικτύου που χρησιμοποιεί η ελεγχόμενη υπηρεσία (πχ port=ssh, sftp), το φίλτρο που έχει δημιουργηθεί και θα χρησιμοποιηθεί για τον εντοπισμό του κακόβουλου χρήστη (πχ filter=sshd-ddos), το αρχείο καταγραφής της υπηρεσίας, στο οποίο θα γίνει ο έλεγχος για κακόβουλη χρήση (πχ logpath=/var/log/messages) και τέλος, το μέγιστο πλήθος ανεκτών αποτυχημένων προσπαθειών για πρόσβαση στη συγκεκριμένη υπηρεσία (πχ maxretry=5).

Στη διαδικασία εγκατάστασης της εφαρμογής fail2ban δημιουργούνται αυτόματα «φυλακές» για ορισμένες βασικές υπηρεσίες του συστήματος (apache, courier, ssh), οι οποίες και καταχωρούνται στο προκαθορισμένο αρχείο «φυλακών» jail.conf. Θεωρητικά εκκρεμεί μόνο η δημιουργία των «φυλακών» για τις υπόλοιπες υπηρεσίες του συστήματος, οι οποίες και θα τελούν υπό την προστασία της fail2ban. Επειδή όμως υπάρχει η περίπτωση σε μελλοντική επικαιροποίηση να αλλοιωθούν οι καταχωρίσεις στο αρχείο jail.conf, όλες οι επιθυμητές εγγραφές θα πραγματοποιηθούν συγκεντρωτικά σε νέο αρχείο jail.local, το οποίο και θα δημιουργηθεί για το λόγο αυτό. Μεταξύ των απαιτούμενων «φυλακών» που θα καταχωρηθούν χειρονακτικά στο εν λόγω αρχείο, θα συμπεριληφθεί και η «φυλακή» που απαιτείται για τον έλεγχο κακόβουλης χρήσης της εφαρμογής roundcube, η οποία θα εγκατασταθεί στο αμέσως επόμενο βήμα του οδηγού.

Οδηγία: Δημιουργούμε το αρχείο «φυλακών» jail.local:

```
touch /etc/fail2ban/jail.local
```

Οδηγία: Ανοίγουμε το αρχείο jail.local για επεξεργασία:

```
vi /etc/fail2ban/jail.local
```

Οδηγία: Προσθέτουμε στο αρχείο jail.local τις παρακάτω «φυλακές» μεριμνώντας οι πόρτες της υπηρεσίας SSH, καθώς και της roundcube (που όπως αναφέρθηκε θα εγκατασταθεί στο αμέσως επόμενο βήμα του οδηγού) να είναι σωστές. Για την υπηρεσία

SSH η πόρτα έχει επιλεγεί σε προηγούμενο βήμα (στον οδηγό χρησιμοποιήθηκε η πόρτα 22222), ενώ για την εφαρμογή roundcube θα πρέπει να επιλεχθεί κάποια ελεύθερη πόρτα, η οποία και θα χρησιμοποιηθεί κατά τη διαδικασία εγκατάστασής της (στο παράδειγμα του οδηγού θα χρησιμοποιηθεί η πόρτα 33333).

```
[ssh]
enabled = true
port    = 22222
filter  = sshd
logpath  = /var/log/auth.log
maxretry = 3

[pureftpd]
enabled  = true
port     = ftp
filter   = pureftpd
logpath  = /var/log/syslog
maxretry = 3

[sasl]
enabled  = true
port     = smtp
filter   = sasl
logpath  = /var/log/mail.log
maxretry = 3

[courierpop3]
enabled  = true
port     = pop3
filter   = courierpop3
logpath  = /var/log/mail.log
maxretry = 3

[courierpop3s]
enabled  = true
port     = pop3s
filter   = courierpop3s
logpath  = /var/log/mail.log
maxretry = 3
```

```
[courierimap]
enabled  = true
port     = imap2
filter   = courierimap
logpath  = /var/log/mail.log
maxretry = 3

[courierimaps]
enabled  = true
port     = imaps
filter   = courierimaps
logpath  = /var/log/mail.log
maxretry = 3

[roundcube]
enabled  = true
port     = http,33333
filter   = roundcube
logpath  = /var/log/roundcube/userlogins
maxretry = 3
```

Η fail2ban θα αναζητήσει τα φίλτρα που χρησιμοποιήθηκαν στις παραπάνω «φυλακές» στο φάκελο φίλτρων της, στη διαδρομή: /etc/fail2ban/filter.d/. Με εξαίρεση τα φίλτρα sshd, καθώς και sasl, τα οποία έχουν δημιουργηθεί αυτόματα με την εγκατάσταση της εφαρμογής, όλα τα υπόλοιπα πρέπει και θα δημιουργηθούν χειρονακτικά ακολούθως.

Η τυπική δομή ενός φίλτρου περιλαμβάνει δύο μεταβλητές που καθορίζουν το κείμενο εκείνο που θα αναζητείται στο αρχείο καταγραφής της υπηρεσίας, για την οποία γίνεται έρευνα κακόβουλης χρήσης. Η πρώτη μεταβλητή είναι η failregex, η οποία αφορά σε μορφή κειμένου καταχώρισης του αρχείου καταγραφής που προκύπτει μετά από κακόβουλη χρήση της εκάστοτε υπηρεσίας του συστήματος. Έτσι, κάθε καταχώριση του αρχείου καταγραφής της ελεγχόμενης υπηρεσίας θα συγκρίνεται με τη μεταβλητή failregex και στην περίπτωση που υπάρχει ομοιομορφία, τότε η εγγραφή θα λαμβάνεται υπόψη για τον εντοπισμό της κακόβουλης χρήσης. Παρομοίως, η εγγραφή θα αγνοείται εάν το κείμενό της εμπίπτει στα προκαθορισμένα της δεύτερης μεταβλητής, ignoreregex.

Ο προσδιορισμός του κειμένου προς αναζήτηση γίνεται με χρήση κανονικών εκφράσεων, οι οποίες καλούνται regexes ή regular expressions [79, 80]. Οι κανονικές εκφράσεις που έχουν επιλεγεί να καταχωρηθούν στα παρακάτω φίλτρα έχουν σχεδιαστεί από χρήστες της εφαρμογής fail2ban, έχουν πλέον αποσφαλματωθεί πλήρως, οπότε και χρησιμοποιούνται ευρέως.

Οδηγία: Δημιουργούμε το αρχείο φίλτρου pureftpd.conf:

```
touch /etc/fail2ban/filter.d/pureftpd.conf
```

Οδηγία: Ανοίγουμε το αρχείο pureftpd.conf για επεξεργασία:

```
vi /etc/fail2ban/filter.d/pureftpd.conf
```

Οδηγία: Προσθέτουμε στο αρχείο pureftpd.conf τις παρακάτω γραμμές:

```
[Definition]
failregex = .*pure-ftpd: \(.*@<HOST>\) \[WARNING\] Authentication
failed for user.*
ignoreregex =
```

Οδηγία: Δημιουργούμε το αρχείο φίλτρου courierpop3.conf:

```
touch /etc/fail2ban/filter.d/courierpop3.conf
```

Οδηγία: Ανοίγουμε το αρχείο courierpop3.conf για επεξεργασία:

```
vi /etc/fail2ban/filter.d/courierpop3.conf
```

Οδηγία: Προσθέτουμε στο αρχείο courierpop3.conf τις παρακάτω γραμμές:

```
[Definition]
failregex = pop3d: LOGIN FAILED.*ip=\[.*:<HOST>\]
ignoreregex =
```

Οδηγία: Δημιουργούμε το αρχείο φίλτρου courierpop3s.conf:

```
touch /etc/fail2ban/filter.d/courierpop3s.conf
```

Οδηγία: Ανοίγουμε το αρχείο courierpop3s.conf για επεξεργασία:

```
vi /etc/fail2ban/filter.d/courierpop3s.conf
```

Οδηγία: Προσθέτουμε στο αρχείο courierpop3s.conf τις παρακάτω γραμμές:

```
[Definition]
failregex = pop3d-ssl: LOGIN FAILED.*ip=\[.*:<HOST>\]
ignoreregex =
```

Οδηγία: Δημιουργούμε το αρχείο φίλτρου courierimap.conf:

```
touch /etc/fail2ban/filter.d/courierimap.conf
```

Οδηγία: Ανοίγουμε το αρχείο courierimap.conf για επεξεργασία:

```
vi /etc/fail2ban/filter.d/courierimap.conf
```

Οδηγία: Προσθέτουμε στο αρχείο courierimap.conf τις παρακάτω γραμμές:

```
[Definition]
failregex = imapd: LOGIN FAILED.*ip=\[.*:<HOST>\]
ignoreregex =
```

Οδηγία: Δημιουργούμε το αρχείο φίλτρου courierimaps.conf:

```
touch /etc/fail2ban/filter.d/courierimaps.conf
```

Οδηγία: Ανοίγουμε το αρχείο courierimaps.conf για επεξεργασία:

```
vi /etc/fail2ban/filter.d/courierimaps.conf
```

Οδηγία: Προσθέτουμε στο αρχείο courierimaps.conf τις παρακάτω γραμμές:

```
[Definition]
failregex = imapd-ssl: LOGIN FAILED.*ip=\[.*:<HOST>\]
ignoreregex =
```

Οδηγία: Δημιουργούμε το αρχείο φίλτρου roundcube.conf:

```
touch /etc/fail2ban/filter.d/roundcube.conf
```

Οδηγία: Ανοίγουμε το αρχείο roundcube.conf για επεξεργασία:

```
vi /etc/fail2ban/filter.d/roundcube.conf
```

Οδηγία: Προσθέτουμε στο αρχείο roundcube.conf τις παρακάτω γραμμές:

```
[Definition]
failregex = FAILED login for .*. from <host>
ignoreregex =
```

Από χρήστες της εφαρμογής έχει παρατηρηθεί το φαινόμενο της μη απαγόρευσης πρόσβασης κακόβουλων χρηστών κάτω από ορισμένες συνθήκες. Η προσωρινή λύση που έχει δοθεί στο συγκεκριμένο πρόβλημα, μέχρι αυτό να λυθεί μόνιμα από την ομάδα ανάπτυξης της fail2ban, είναι η προσθήκη μιας εντολής μικρής χρονικής καθυστέρησης στο αρχείο εντολών του προγράμματος - πελάτη της εφαρμογής.

Οδηγία: Ανοίγουμε το αρχείο fail2ban-client για επεξεργασία:

```
vi /usr/bin/fail2ban-client
```

Οδηγία: Στη γραμμή 145 του συγκεκριμένου αρχείου προσθέτουμε την εντολή time.sleep(0.05), ώστε να έχουμε το παρακάτω αποτέλεσμα:

```
[...]
 def __processCmd(self, cmd, showRet = True):
                beautifier = Beautifier()
                for c in cmd:
                        time.sleep(0.05)
                        beautifier.setInputCmd(c)
                        try:
[...]
```

Οδηγία: Για να ισχύσουν άμεσα οι αλλαγές που πραγματοποιήθηκαν, επανεκκινούμε την εφαρμογή fail2ban:

```
/etc/init.d/fail2ban restart
```

Σημείωση: Μπορούμε να ελέγξουμε εάν είναι ενεργοποιημένες όλες οι «φυλακές» που έχουν δημιουργηθεί, με την παρακάτω εντολή:

```
iptables -L -n
```

Εγκατάσταση roundcube

Η roundcube [81, 82] είναι μια web-based, πολυγλωσσική εφαρμογή πελάτη IMAP, με φιλικότατο περιβάλλον διεπαφής, τεχνολογίας Ajax και πλήρη υποστήριξη παροχής υπηρεσιών που θα περίμενε κανείς από μια αντίστοιχη desktop εφαρμογή ηλεκτρονικού ταχυδρομείου (υποστήριξη MIME, βιβλίο διευθύνσεων, φάκελοι αλληλογραφίας, αναζήτηση μηνύματος, ορθογράφος κτλ). Παρότι η συγκεκριμένη εφαρμογή είναι εντελώς προαιρετική για τη λειτουργία του ISPConfig, εντούτοις, η εγκατάστασή της είναι απαραίτητη, ώστε να παρέχεται στους χρήστες του συστήματος, η δυνατότητα πρόσβασης στην ηλεκτρονική τους αλληλογραφία, μέσα από ένα απλό περιηγητή διαδικτύου.

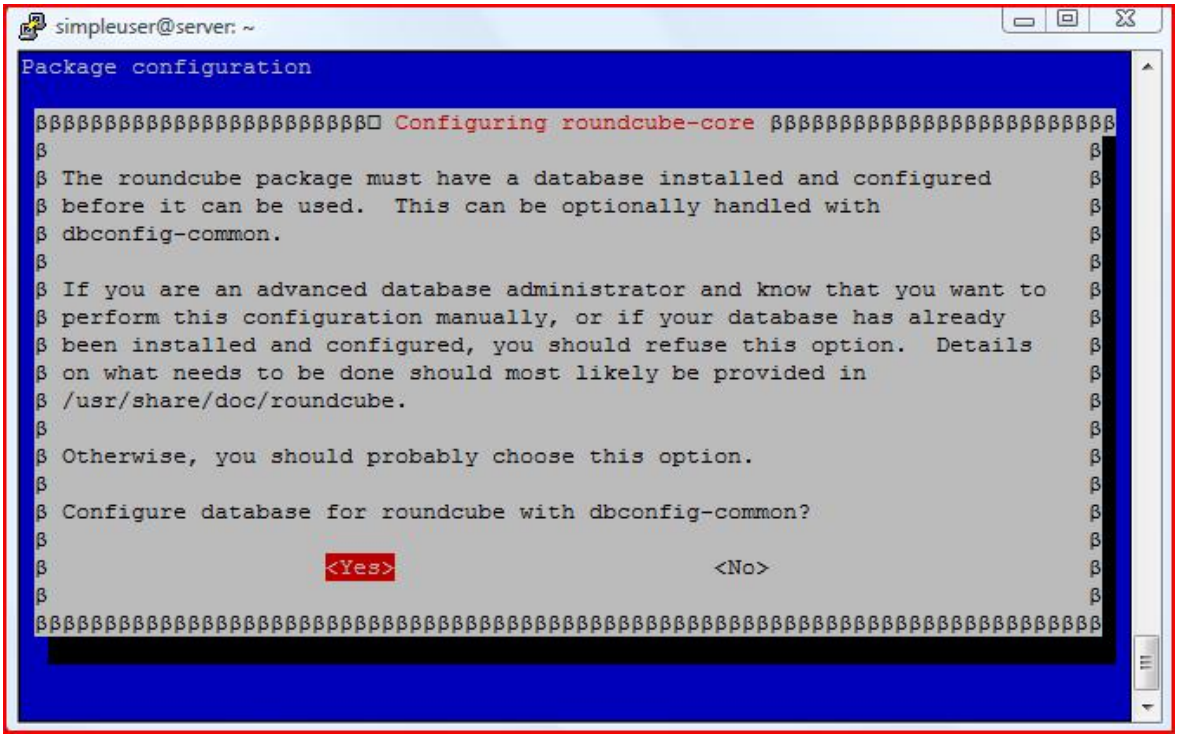
Η εν λόγω εφαρμογή είναι τόσο διαδεδομένη, ώστε πλέον χρησιμοποιείται παγκοσμίως, από πολλά Ιδρύματα Τριτοβάθμιας Εκπαίδευσης, για την παροχή υπηρεσιών ηλεκτρονικού ταχυδρομείου στους φοιτητές, καθώς και το προσωπικό τους (πχ Harvard University, UC Berkeley, Stevens Institute of Technology, Tilburg University, University of Sussex, University of Michigan). Η roundcube μπορεί να επικοινωνήσει με βάσεις δεδομένων μορφής MySQL, PostgreSQL ή SQLite, ενώ παράλληλα συνεργάζεται με την εφαρμογή fail2ban, που εγκαταστάθηκε στο αμέσως προηγούμενο βήμα, φροντίζοντας για τη διατήρηση της ασφάλειας του συστήματος σε υψηλά επίπεδα. Στο παράδειγμα του οδηγού έχει επιλεχθεί να χρησιμοποιηθεί η βάση δεδομένων μορφής MySQL και για το λόγο αυτό, μαζί με το πακέτο της εφαρμογής roundcube θα εγκατασταθεί και το πακέτο roundcube-mysql.

Οδηγία: Εκτελούμε την παρακάτω εντολή και επιβεβαιώνουμε την πρόθεσή μας για εγκατάσταση των επιλεγμένων πακέτων με «enter»:

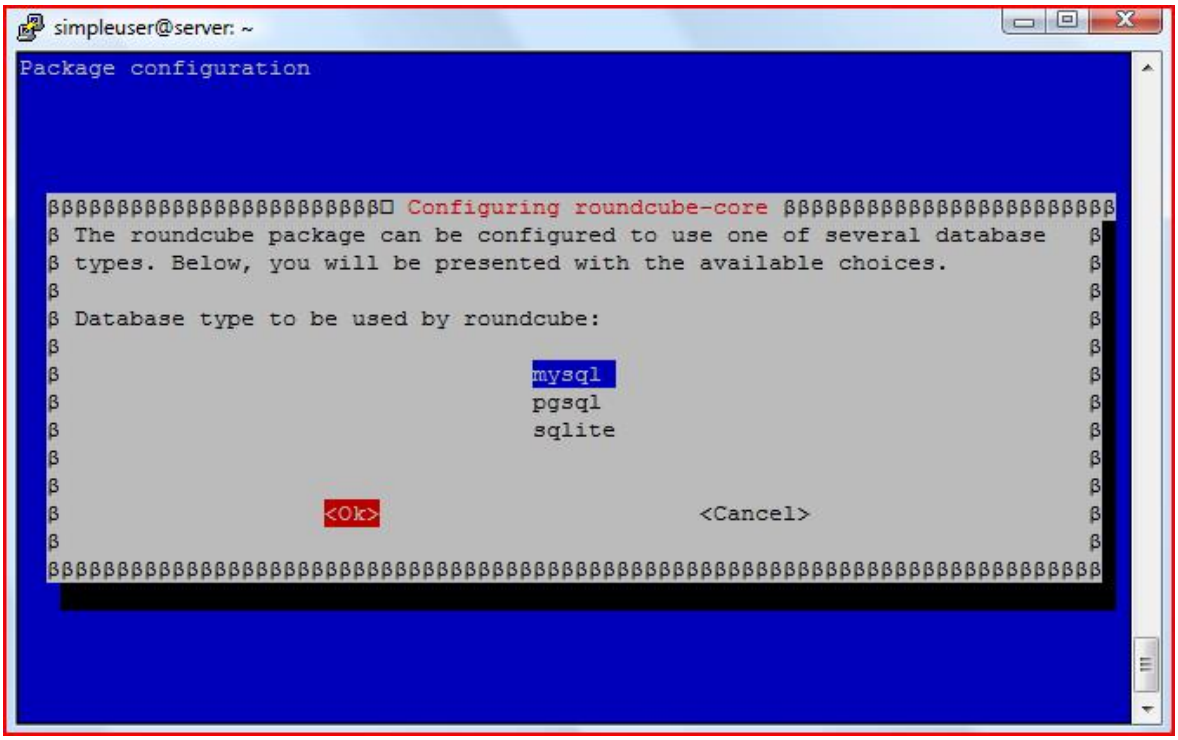
```
apt-get install roundcube roundcube-mysql
```

Η ρύθμιση της βάσης δεδομένων μπορεί είτε να γίνει αυτόματα με την εφαρμογή - πλαίσιο αυτοματοποίησης εργασιών διαχείρισης βάσεων δεδομένων dbconfig-common [83], είτε χειρονακτικά.

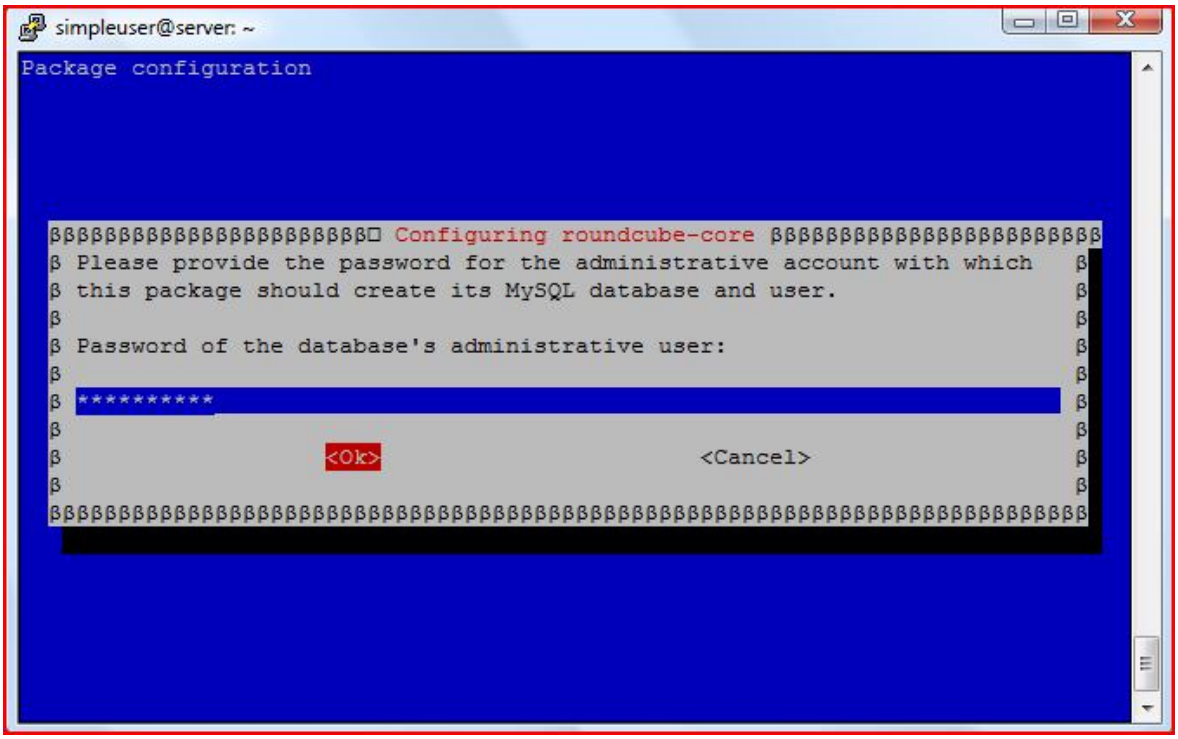
Οδηγία: Επιλέγουμε αυτόματη ρύθμιση της βάσης δεδομένων με το dbconfig-common, απαντώντας θετικά στο σχετικό παράθυρο διαλόγου:



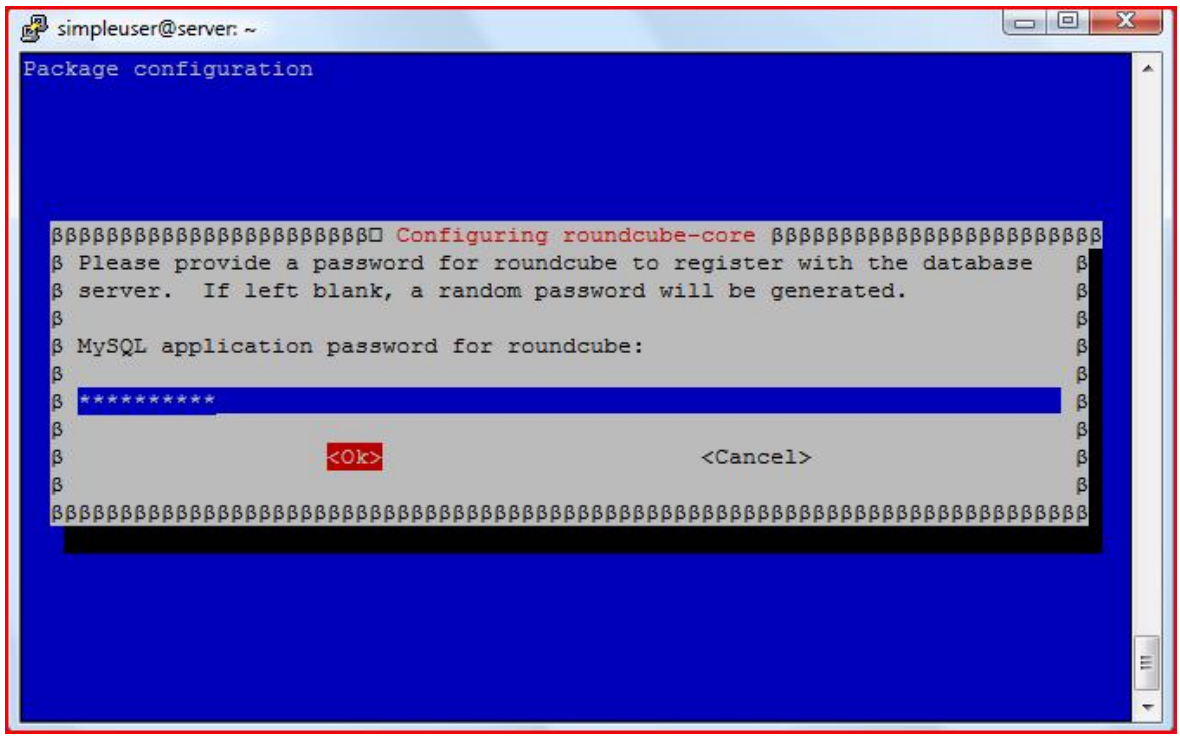
Οδηγία: Επιλέγουμε την εγκατάσταση της εφαρμογής roundcube με χρήση βάσης δεδομένων τύπου MySQL:



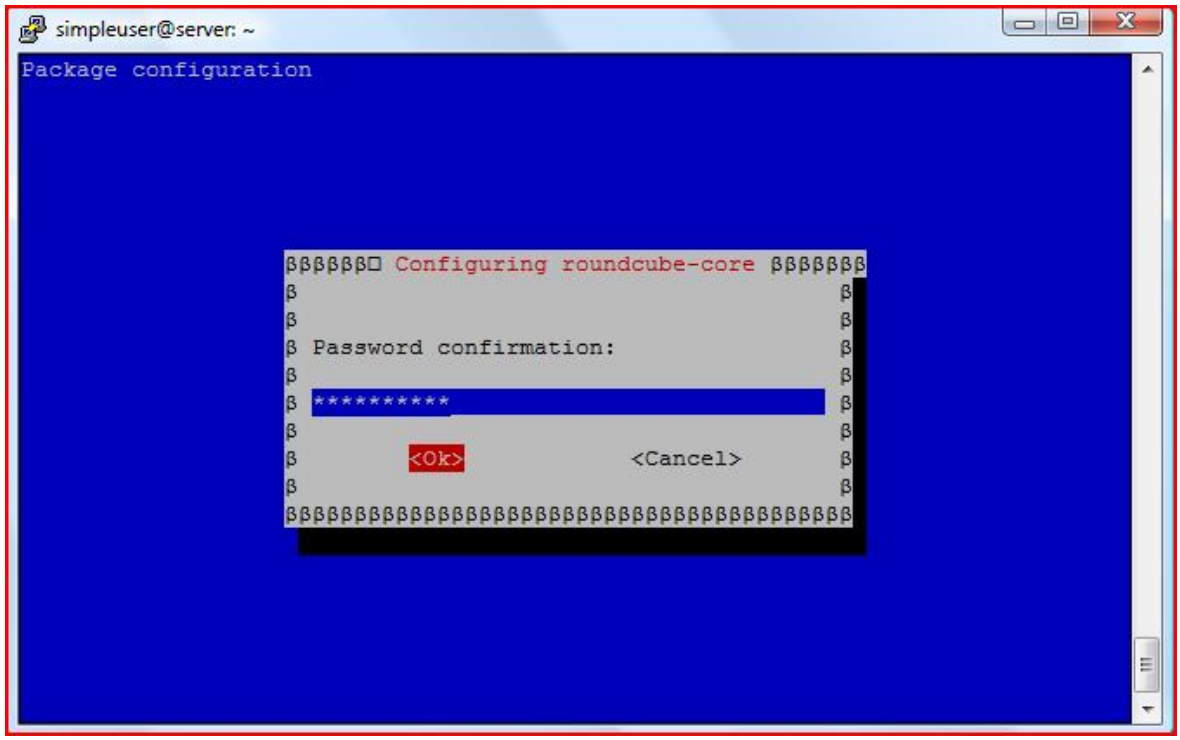
Οδηγία: Εισάγουμε τον κωδικό χρήστη για το διαχειριστή της MySQL (root), όπως αυτός έχει καθοριστεί στο βήμα εγκατάστασης της MySQL:



Οδηγία: Εισάγουμε τον κωδικό χρήστη για έναν απλό, χωρίς ειδικά δικαιώματα χρήστη, τον οποίο θα δημιουργήσει και θα χρησιμοποιεί η εφαρμογή roundcube για να επικοινωνεί με τη MySQL (ισχύουν και εδώ όσα έχουν προαναφερθεί για τους κωδικούς χρηστών):



Οδηγία: Για αποφυγή λαθών πληκτρολόγησης, εισάγουμε εκ νέου τον κωδικό χρήστη του απλού χρήστη:



Για να είναι προσβάσιμο το περιβάλλον διεπαφής της roundcube από μια φιλικότερη στο χρήστη URL διεύθυνση, όπως η http://www.mydomain.gr/webmail, θα πρέπει να δημιουργηθεί η αντίστοιχη καταχώριση στο αρχείο ρυθμίσεων roundcube.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων roundcube:

```
vi /etc/apache2/conf.d/roundcube
```

Οδηγία: Στην πέμπτη γραμμή του αρχείου εισάγουμε το παρακάτω κείμενο:

```
[...]
#    Alias /roundcube /var/lib/roundcube
Alias /webmail /var/lib/roundcube

# Access to tinymce files
[...]
```

Οδηγία: Πριν αποθηκεύσουμε τις αλλαγές και κλείσουμε το αρχείο ρυθμίσεων roundcube, θα πρέπει να προσθέσουμε στο τέλος του τις παρακάτω γραμμές, ώστε, όταν ζητάμε να συνδεθούμε στη υπηρεσία ηλεκτρονικού ταχυδρομείου μέσω της εφαρμογής roundcube, τότε να γίνεται αυτόματη ανακατεύθυνσή μας σε ασφαλή σύνδεση, μέσω του πρωτοκόλλου https, στην πόρτα που έχουμε επιλέξει και ορίσει στην αντίστοιχη «φυλακή» της εφαρμογής fail2ban για τη roundcube (στο παράδειγμα η 33333):

```
[...]
<IfModule mod_rewrite.c>
  <IfModule mod_ssl.c>
    <Location /webmail>
      RewriteEngine on
      RewriteCond %{HTTPS} !^on$ [NC]
      RewriteRule . https://%{HTTP_HOST}:33333%{REQUEST_URI}  [L]
    </Location>
  </IfModule>
</IfModule>
```

Οδηγία: Για την επικοινωνία της εφαρμογής roundcube με τη fail2ban, απαιτείται η μεταφόρτωση και εγκατάσταση του αντίστοιχου πρόσθετου με τις παρακάτω εντολές:

```
  cd /usr/share/roundcube/plugins/
  wget --no-check-certificate
http://github.com/downloads/mattrude/rc-plugin-
fail2ban/roundcube-fail2ban-plugin.1.0.tgz
  tar -xvzf roundcube-fail2ban-plugin.1.0.tgz
  touch /var/log/roundcube/userlogins
  chown www-data:www-data /var/log/roundcube/userlogins
```

Οδηγία: Τέλος, θα πρέπει να γίνει ενημέρωση του σχετικού αρχείου ρυθμίσεων της roundcube για την ύπαρξη του πρόσθετου που μόλις εγκαταστάθηκε. Ανοίγουμε λοιπόν για επεξεργασία το αρχείο main.inc.php:

```
  vi /var/lib/roundcube/config/main.inc.php
```

Οδηγία: Τροποποιούμε τις γραμμές 42 και 66 όπως παρακάτω:

```
  [...]
  $rcmail_config['plugins'] = array('fail2ban');
  [...]
  $rcmail_config['default_host'] = 'localhost';
  [...]
```

Οδηγία: Για να ισχύσουν άμεσα οι παραπάνω αλλαγές, επανεκκινούμε τον Apache:

```
  /etc/init.d/apache2 restart
```

Εγκατάσταση ISPConfig

Όπως έχει ήδη αναφερθεί, το ISPConfig είναι ένας πίνακας ελέγχου ελεύθερου λογισμικού / λογισμικού ανοιχτού κώδικα, που αναπτύσσεται και εγκαθίσταται σε εξυπηρετητές διαδικτύου με λειτουργικό σύστημα Linux και έχει ως στόχο το να παρέχει στους υπευθύνους των συστημάτων αυτών τη δυνατότητα απλοποιημένης εποπτείας και διαχείρισής τους. Η εν λόγω εφαρμογή διανέμεται κάτω από τη BSD άδεια χρήσης και υποστηρίζει την ταυτόχρονη διαχείριση πολλαπλών εξυπηρετητών διαδικτύου. Έχει

σχεδιαστεί ώστε να απλοποιεί επίπονες και χρονοβόρες διαδικασίες, όπως η ρύθμιση του εξυπηρετητή ονομάτων τομέα, πολλαπλών διαφορετικών ιστοτόπων στον ίδιο εξυπηρετητή, πολλαπλών λογαριασμών ηλεκτρονικού ταχυδρομείου για τους χρήστες αυτών κτλ. Είναι σε θέση να παρέχει υποστήριξη των εξυπηρετητών Παγκοσμίου Ιστού Apache2 και Nginx, ενός μεγάλου αριθμού εξυπηρετητών FTP, των εξυπηρετητών ονομάτων τομέα BIND, MyDNS και PowerDNS, καθώς και του εξυπηρετητή βάσεων δεδομένων MySQL. Παράλληλα, ο πίνακας ελέγχου ISPConfig είναι σε θέση να διαχειριστεί υπηρεσίες ηλεκτρονικού ταχυδρομείου (διαχείριση ηλεκτρονικής αλληλογραφίας, ανίχνευση και διαχείριση ανεπιθύμητης αλληλογραφίας, ανίχνευση και διαχείριση κακόβουλου λογισμικού κτλ), υπηρεσίες ασφαλείας (SSL, διαχείριση πιστοποιητικών κτλ), υπηρεσίες τείχους προστασίας, υπηρεσίες εικονικών εξυπηρετητών (virtual servers) κτλ, ενώ ταυτόχρονα είναι σε θέση να παρουσιάζει στατιστικά σχετικά με τον ανά χρήστη χρησιμοποιούμενο αποθηκευτικό χώρο και διαμεταγωγή δεδομένων.

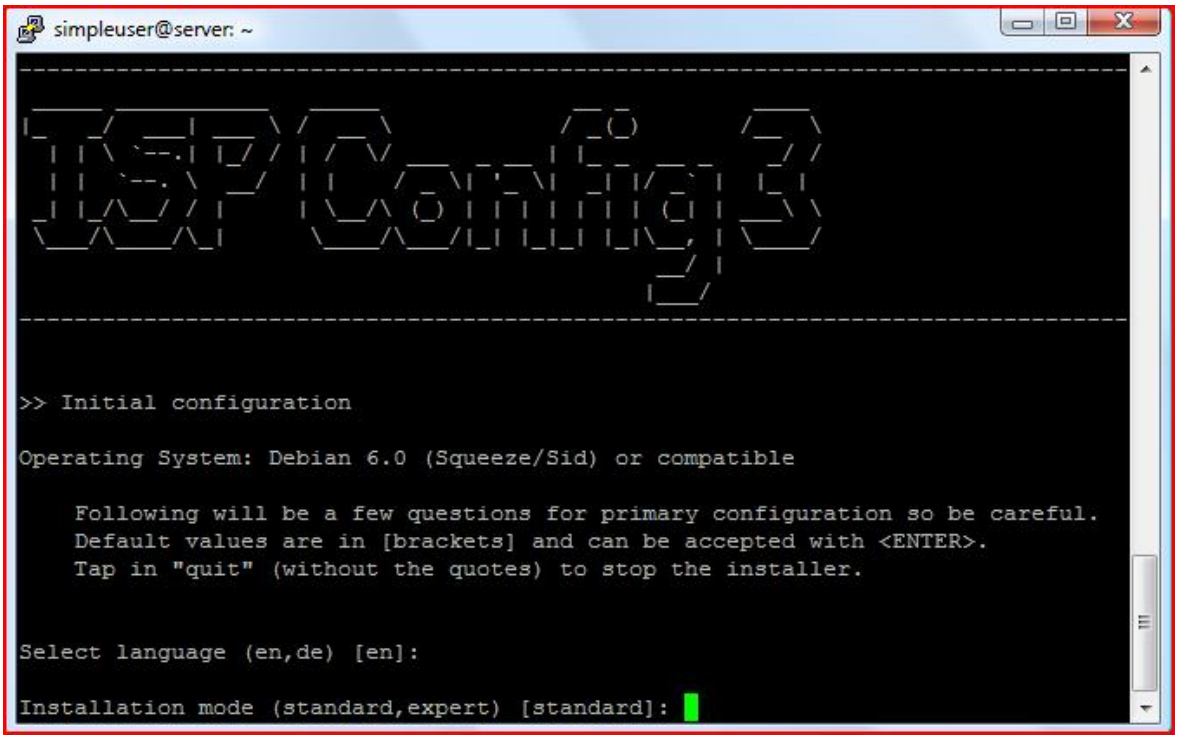
Η εφαρμογή ISPConfig αποτελεί τον ακρογωνιαίο λίθο της παρούσας πτυχιακής εργασίας και έχει για λόγους συμβατότητας καθορίσει σε πολύ μεγάλο βαθμό όλο το υπόλοιπο λογισμικό που ενεπλάκη στον παρών οδηγό. Μάλιστα, ορισμένα από τα πακέτα του λογισμικού που λαμβάνουν μέρος στην όλη διαδικασία προαπαιτούνται, ώστε να περατωθεί χωρίς προβλήματα η εγκατάσταση του ISPConfig. Στο τρέχων βήμα, όλες οι σχετικές ενέργειες έχουν ολοκληρωθεί και έτσι, αυτό που απομένει να πραγματοποιηθεί στα αμέσως επόμενα βήματα είναι η μεταφόρτωση, εγκατάσταση και ρύθμιση του πίνακα ελέγχου ISPConfig.

Οδηγία: Για τη μεταφόρτωση στον εξυπηρετητή του πακέτου εγκατάστασης, καθώς και για την εκκίνηση αυτής εκτελούμε τις παρακάτω εντολές:

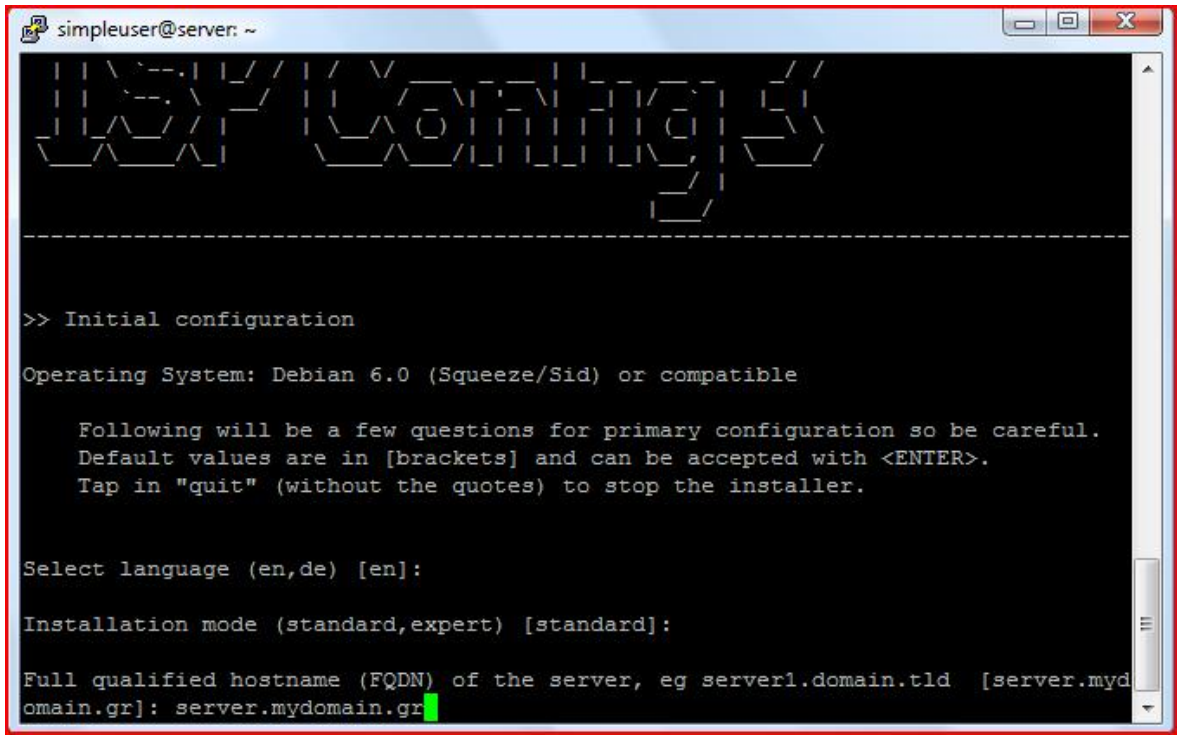
```
  cd /tmp
  wget http://www.ispconfig.org/downloads/ISPConfig-3-
stable.tar.gz
  tar xfz ISPConfig-3-stable.tar.gz
  cd ispconfig3_install/install/
  php -q install.php
```

Οδηγία: Η διαδικασία εγκατάστασης ξεκινά με τον καθορισμό της γλώσσας. Επιβεβαιώνουμε χρήση της προκαθορισμένης Αγγλικής γλώσσας με «enter»:

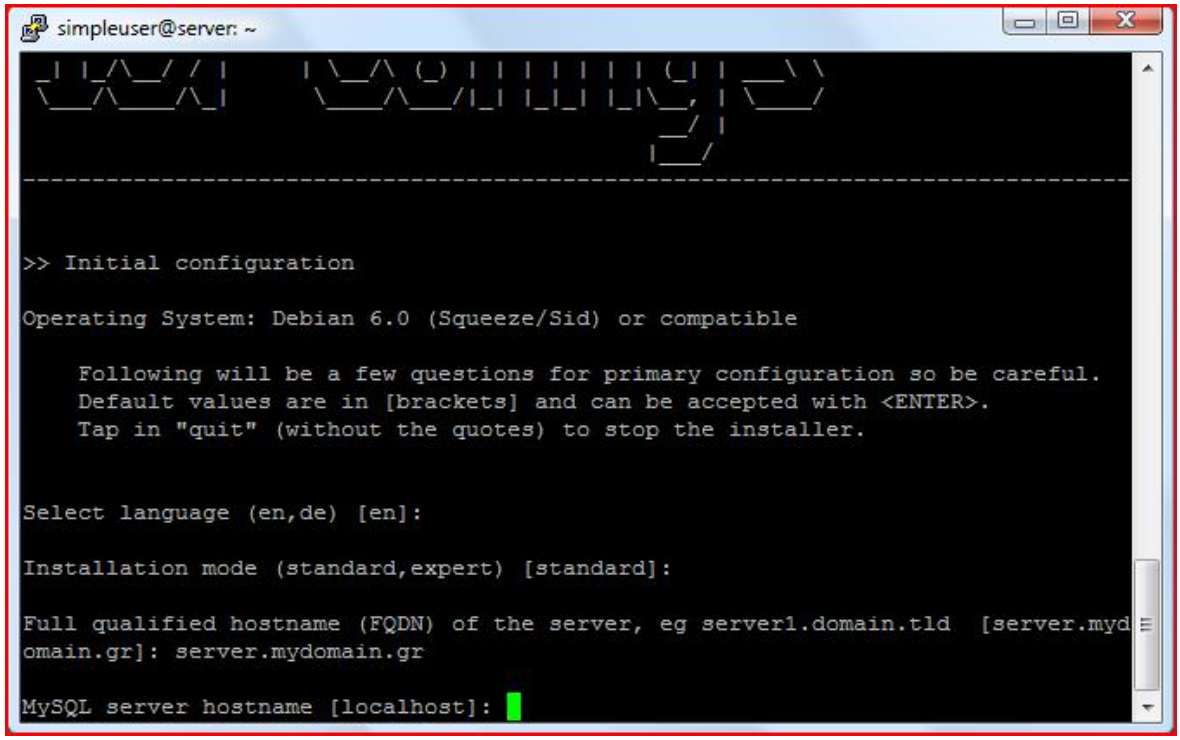
Οδηγία: Στη συνέχεια επιβεβαιώνουμε χρήση της προκαθορισμένης, τυπικής (standard) εγκατάστασης με «enter»:



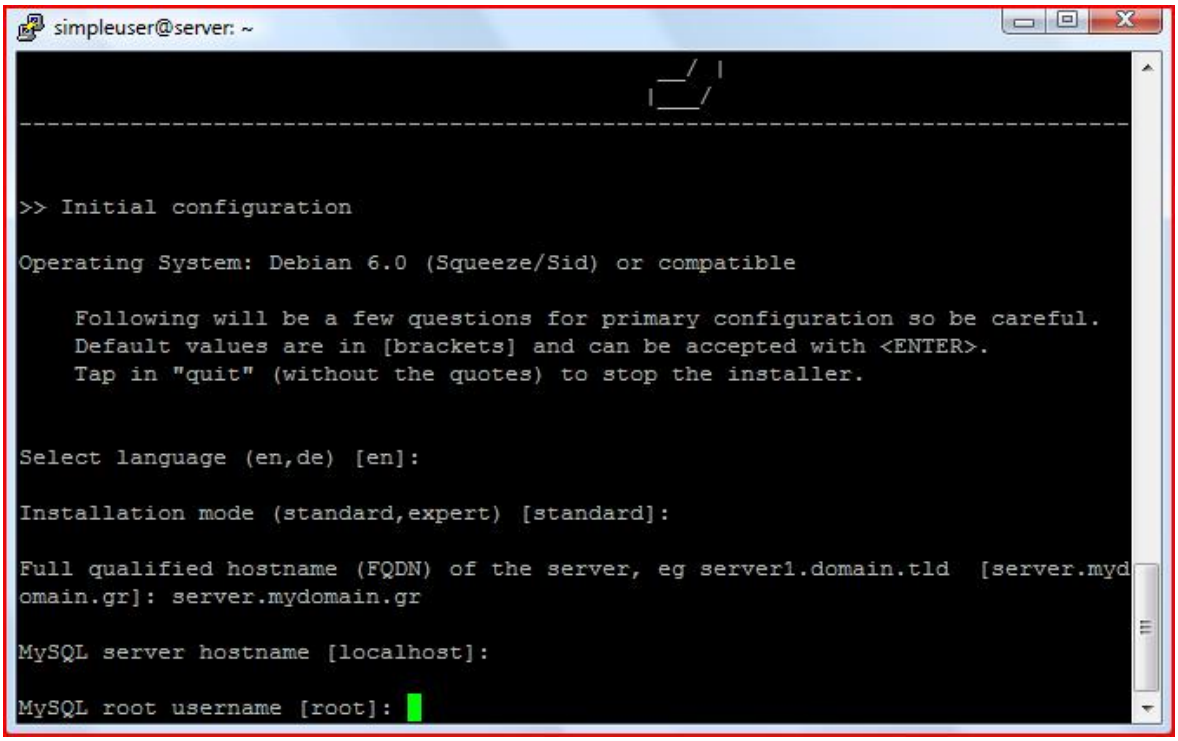
Οδηγία: Εισάγουμε το πλήρες κανονικοποιημένο όνομα του εξυπηρετητή (στο παράδειγμα του οδηγού χρησιμοποιείται το server.mydomain.gr):



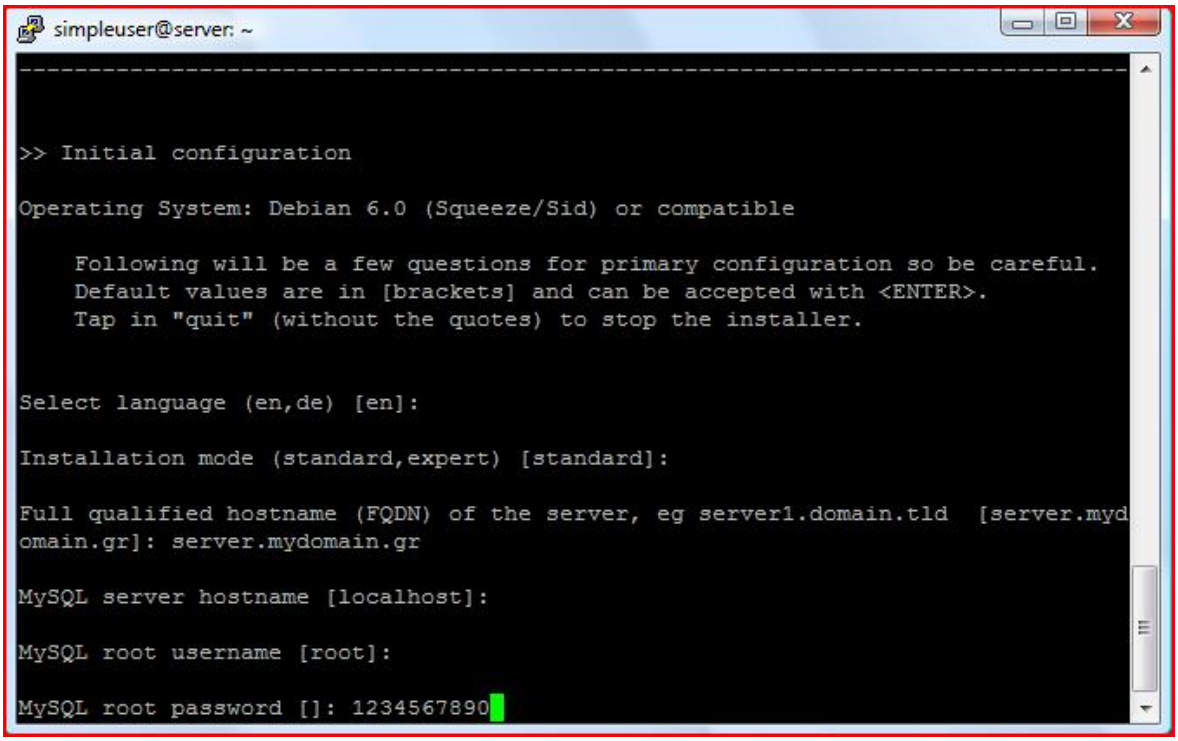
Οδηγία: Επιβεβαιώνουμε με «enter» χρήση του προεπιλεγμένου «localhost», ως το όνομα εξυπηρετητή για τον εξυπηρετητή MySQL:



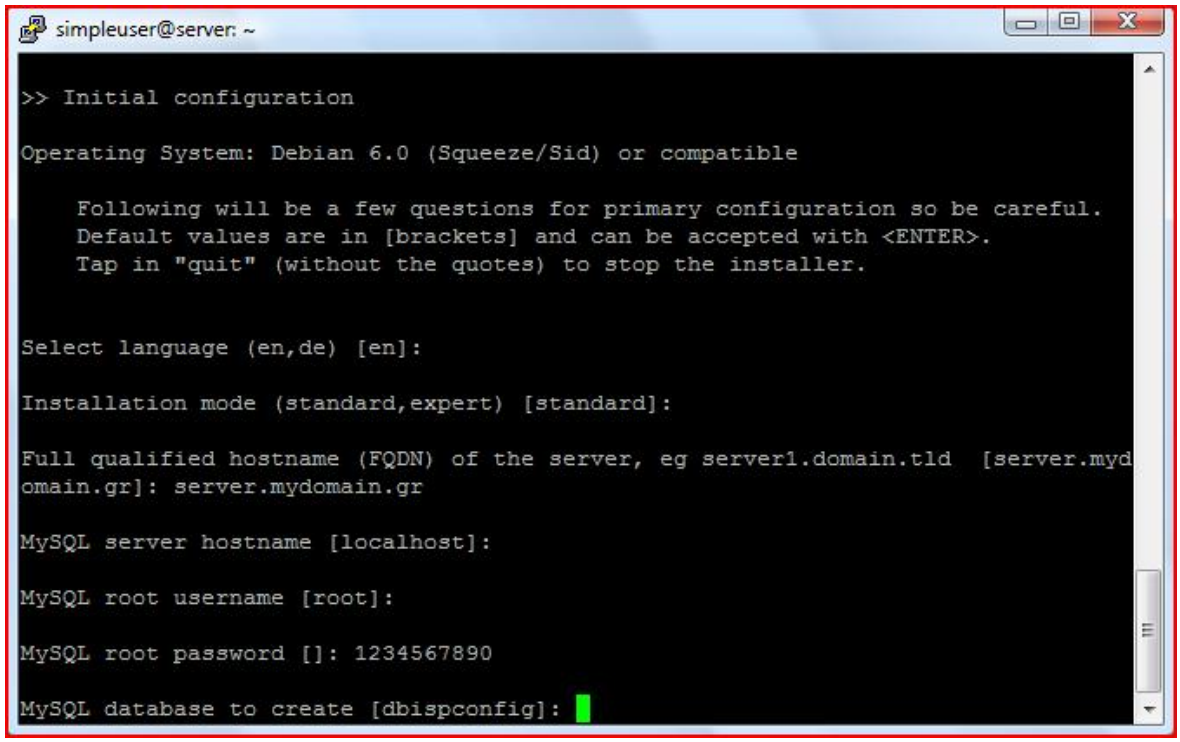
Οδηγία: Επιβεβαιώνουμε με «enter» χρήση του προεπιλεγμένου «root», ως το όνομα του διαχειριστή της MySQL:



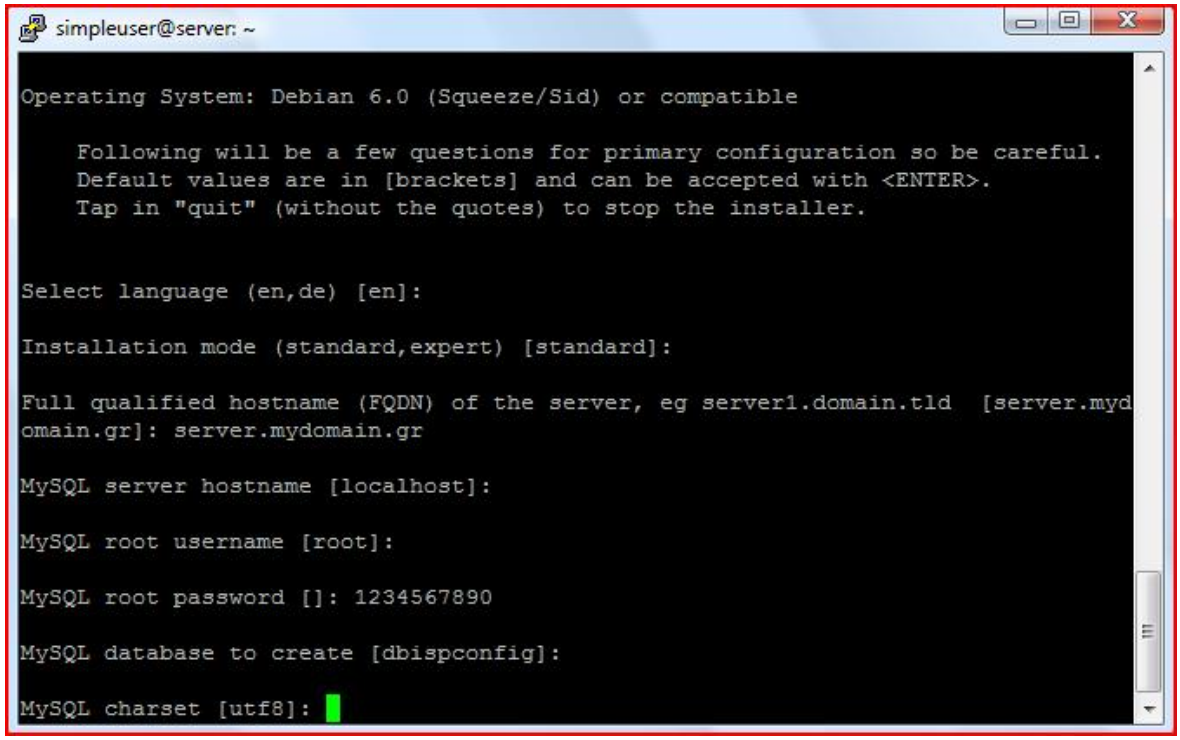
Οδηγία: Εισάγουμε τον κωδικό του διαχειριστή της MySQL:



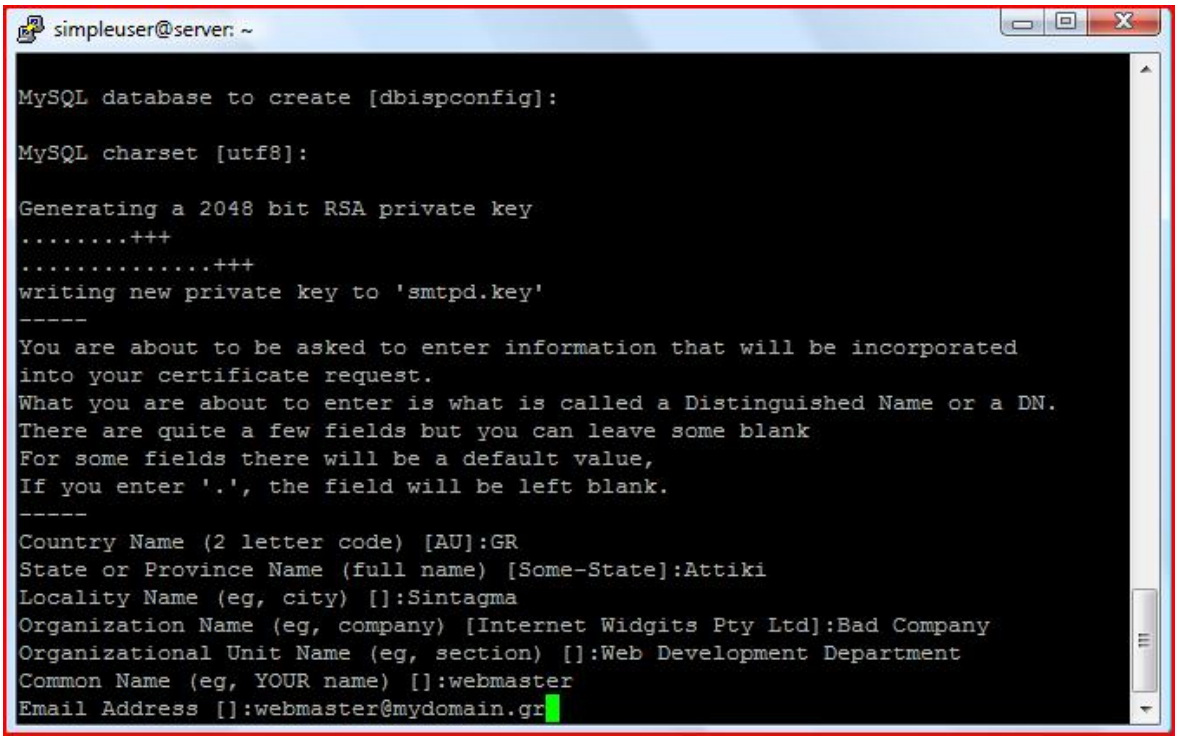
Οδηγία: Επιβεβαιώνουμε χρήση του προεπιλεγμένου ονόματος «dbispconfig», ως όνομα της βάσης δεδομένων που θα δημιουργηθεί για την εφαρμογή ISPConfig:



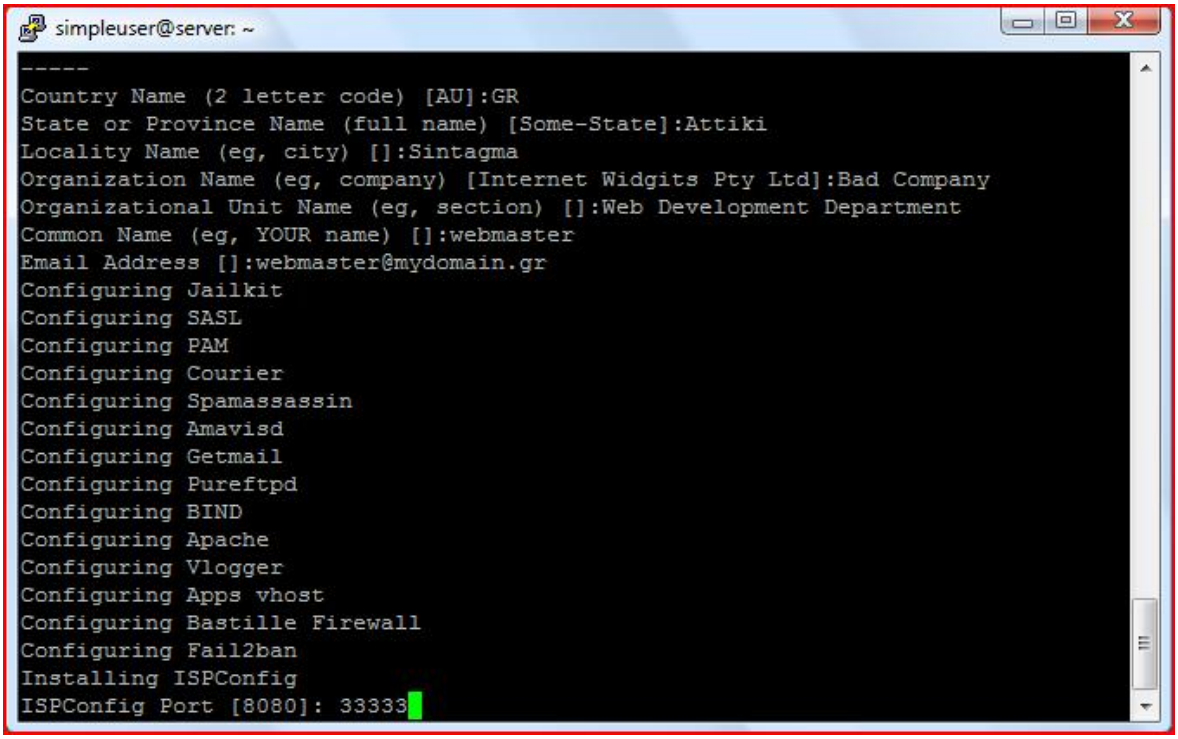
Οδηγία: Επιβεβαιώνουμε χρήση της προεπιλεγμένης κωδικοσελίδας «UTF8»:



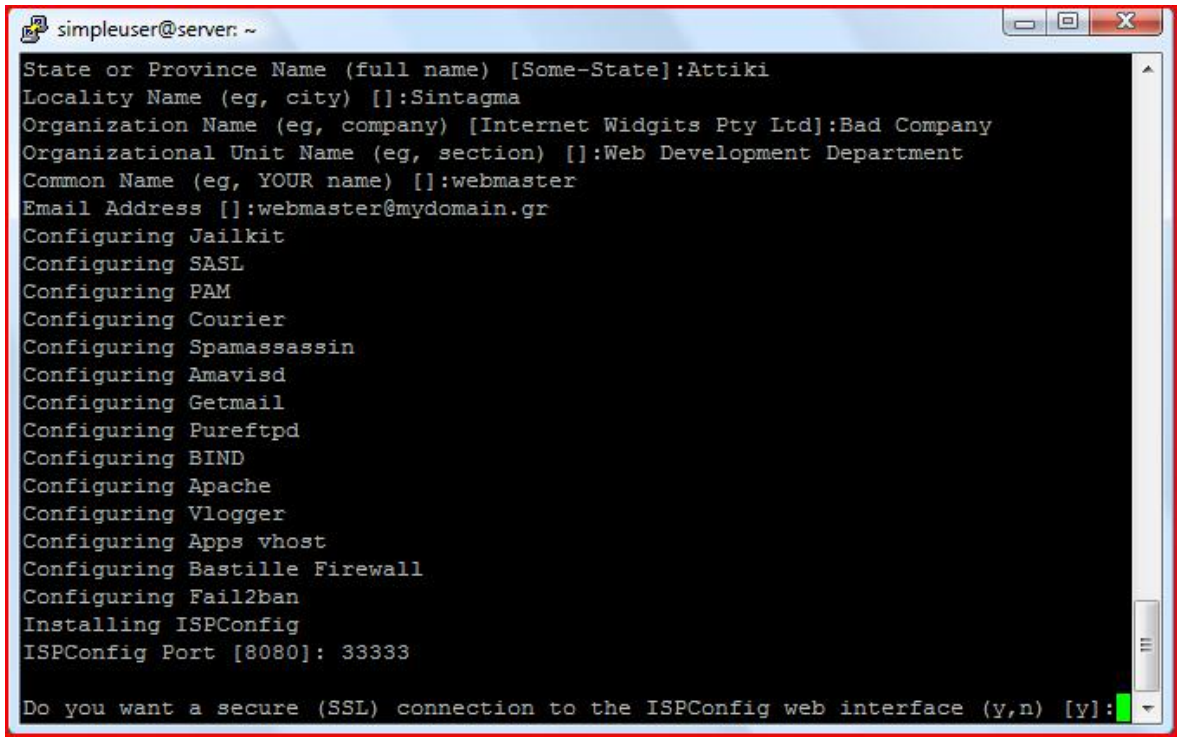
Οδηγία: Εισάγουμε τις πληροφορίες που είναι απαραίτητες για τη δημιουργία αίτησης υπογραφής πιστοποιητικού (CSR), όπως στο παράδειγμα:



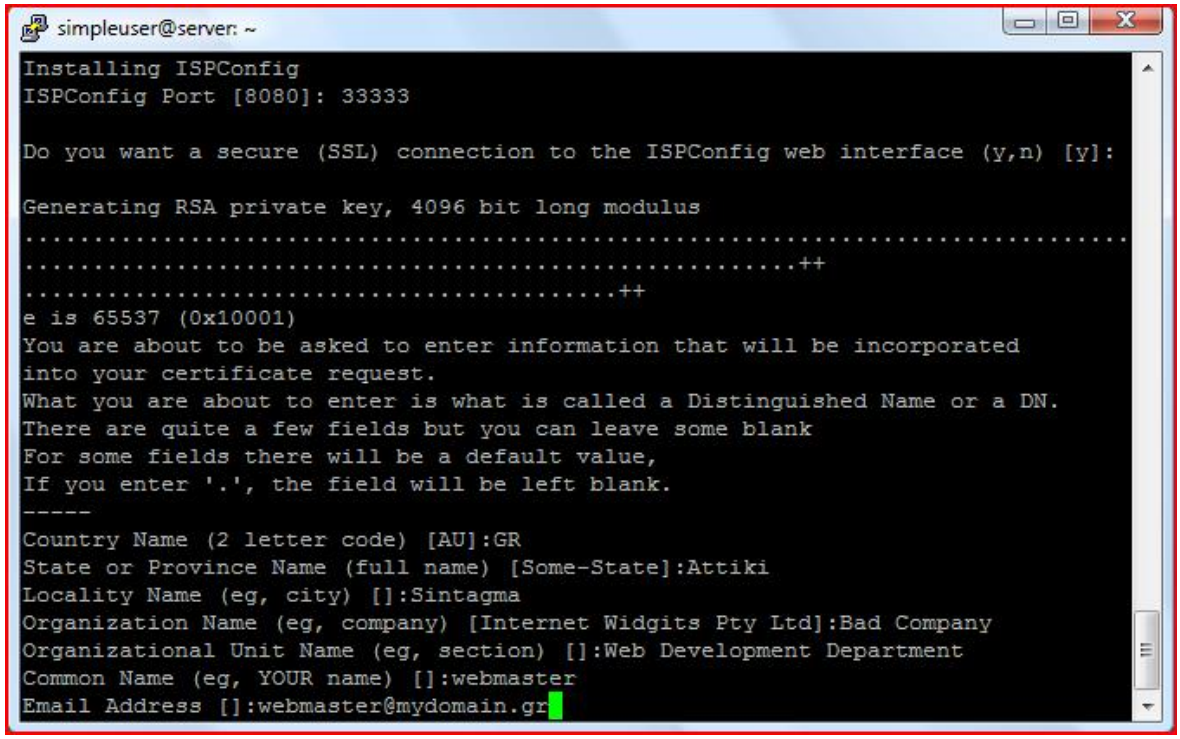
Οδηγία: Εισάγουμε την πόρτα στην οποία θα «ακούει» η εφαρμογή ISPConfig. Για λόγους ασφαλείας δε θα χρησιμοποιηθεί η προκαθορισμένη πόρτα (8080), αλλά η πόρτα που χρησιμοποιήθηκε και στην εφαρμογή roundcube (στο παράδειγμα του οδηγού, η 33333):



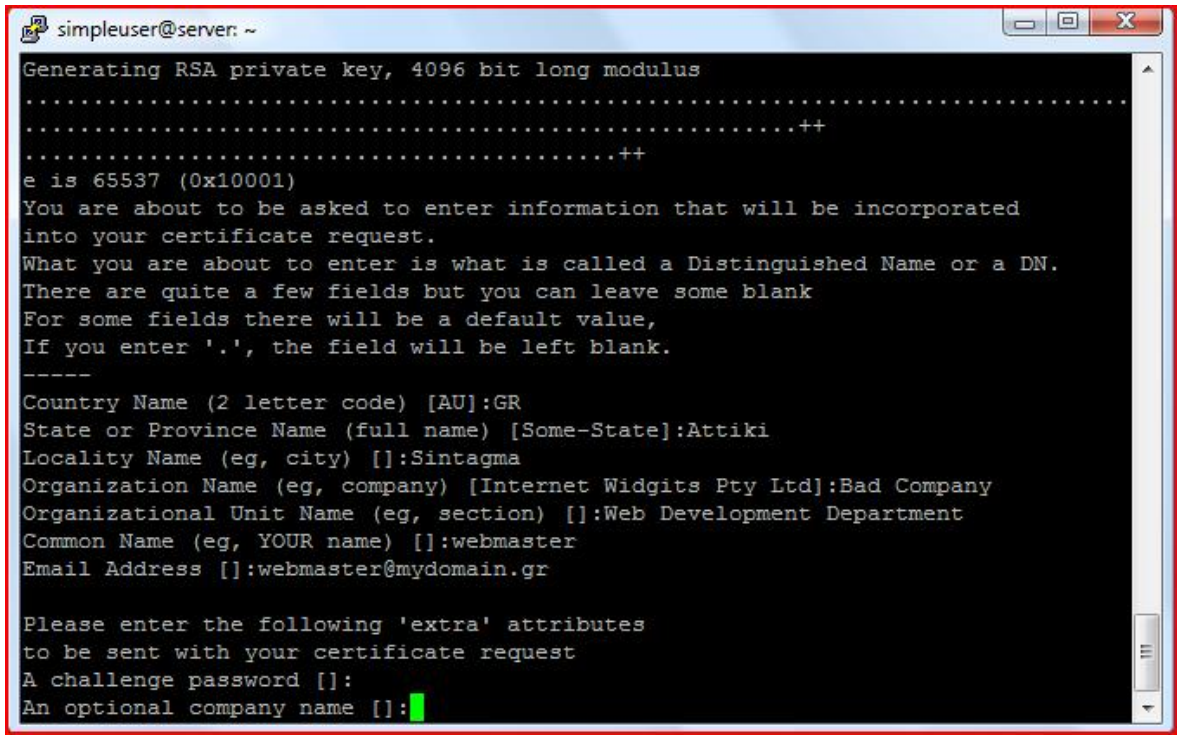
Οδηγία: Επιβεβαιώνουμε χρήση της προεπιλεγμένης, ασφαλούς σύνδεσης με τη διεπαφή της εφαρμογής ISPConfig, εισάγοντας «enter»:



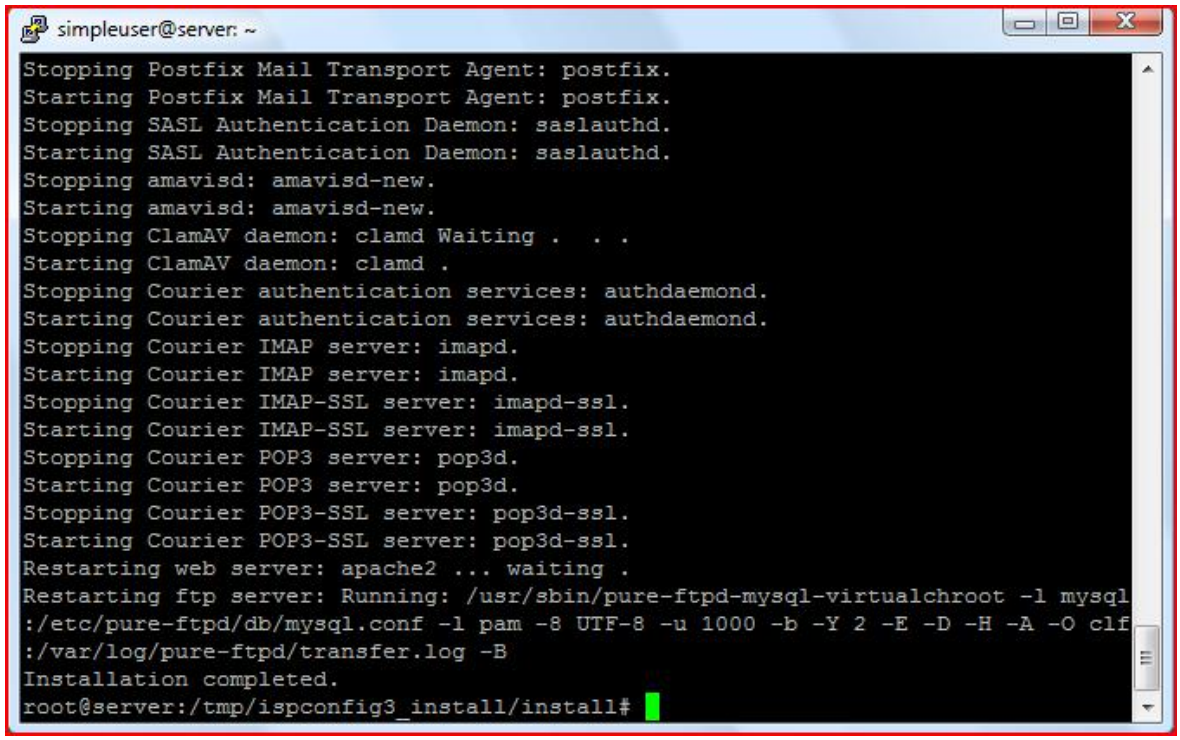
Οδηγία: Εισάγουμε τις πληροφορίες που απαιτούνται για τη δημιουργία του πιστοποιητικού, που θα χρησιμοποιηθεί για την ασφαλή σύνδεση, όπως στο παράδειγμα:



Οδηγία: Επιβεβαιώνοντας τις προεπιλογές, αφήνουμε κενά τον προαιρετικό κωδικό, καθώς και το όνομα της εταιρίας και εισάγουμε και στις δύο περιπτώσεις «enter»:

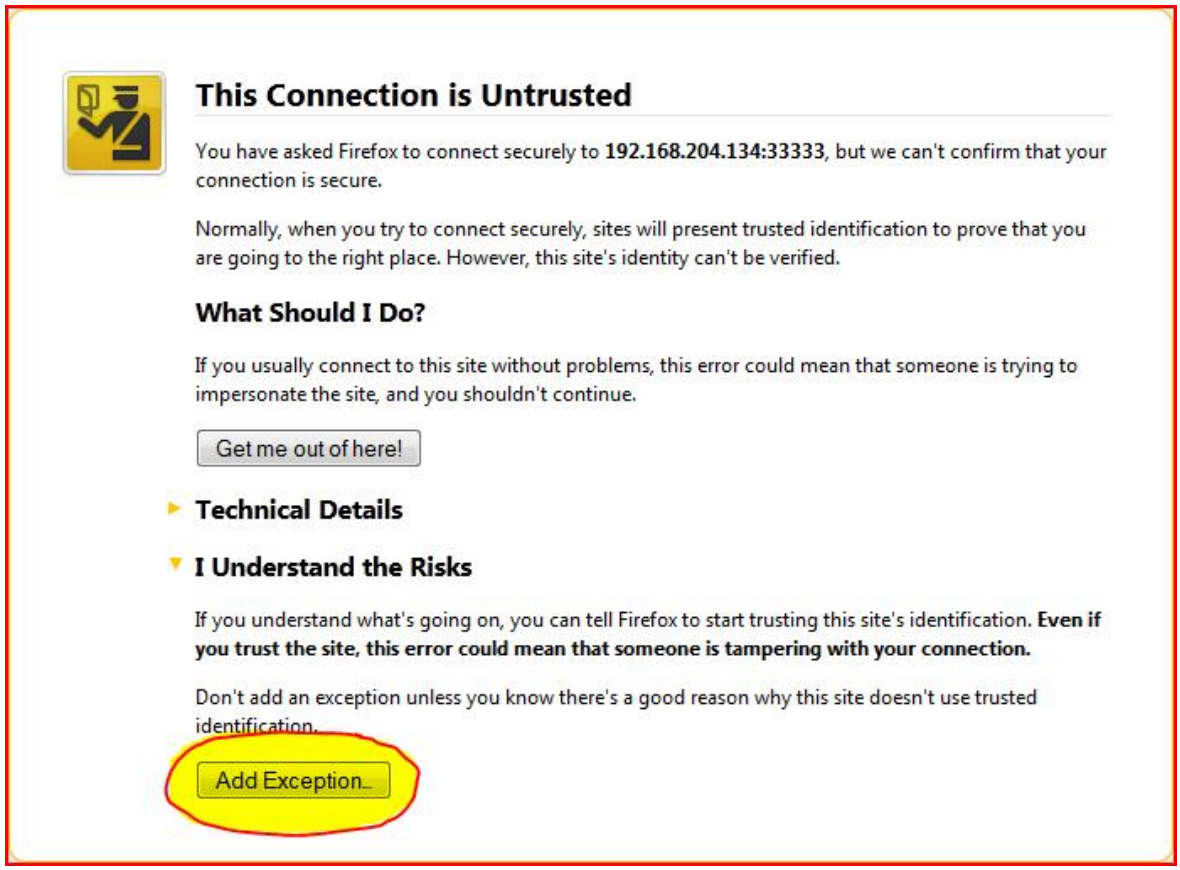


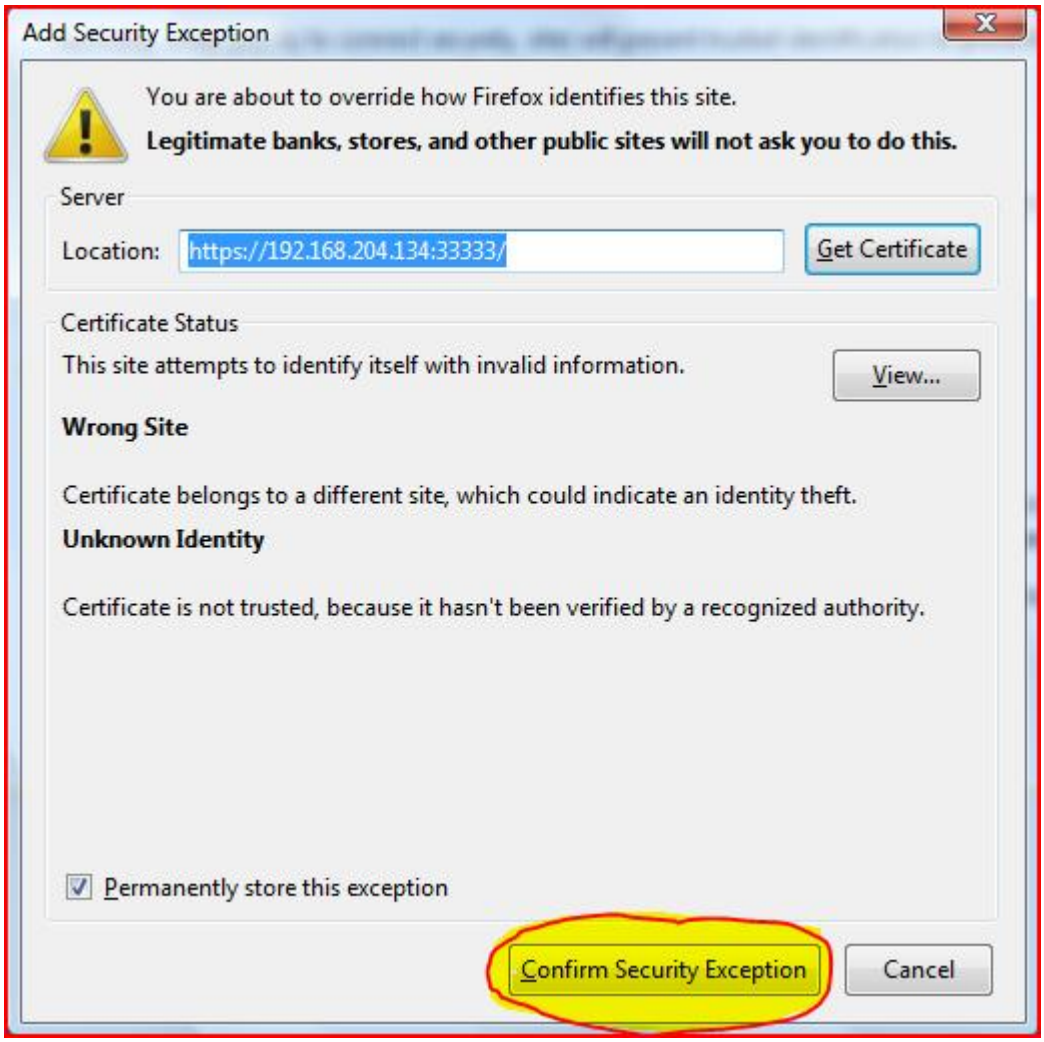
Οδηγία: Η διαδικασία εγκατάστασης ολοκληρώνεται και για την ενημέρωσή μας εμφανίζεται το μήνυμα «installation completed»:



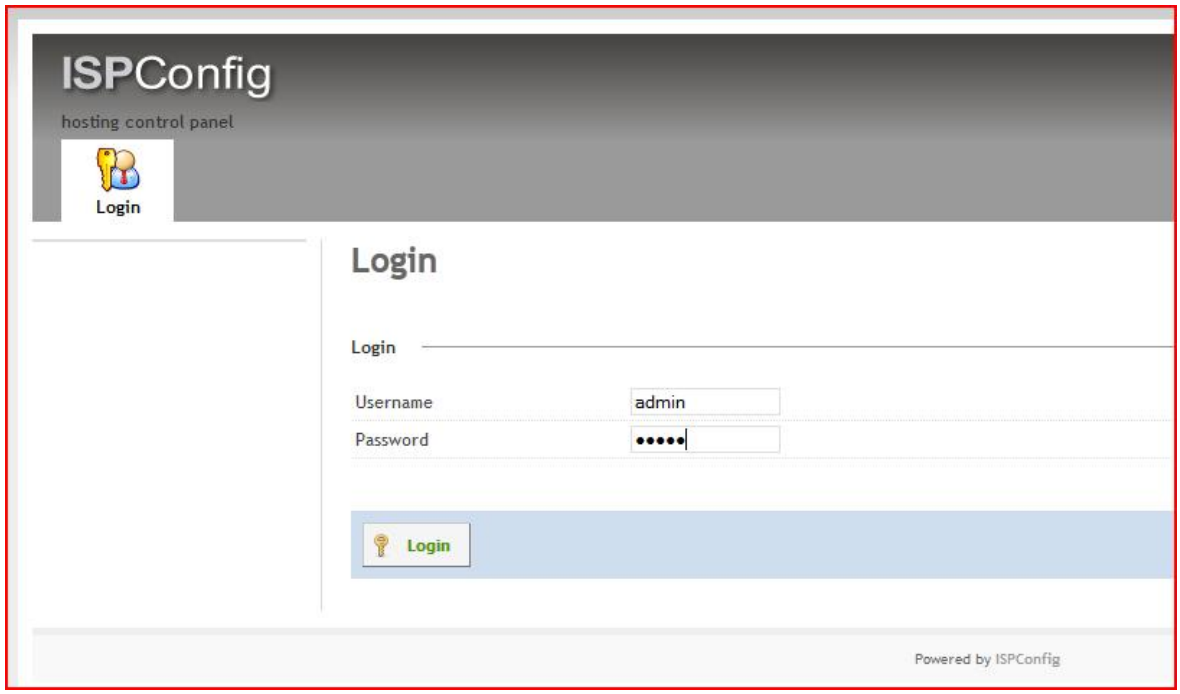
Πλέον υπάρχει η δυνατότητα σύνδεσης στο περιβάλλον διεπαφής της εφαρμογής ISPConfig, μέσω ενός περιηγητή, στη διεύθυνση https://www.mydomain.gr:33333 ή, στην περίπτωση που το domain δεν είναι επιλύσιμο (επειδή για παράδειγμα δεν έχει ολοκληρωθεί η ενημέρωση των εξυπηρετητών ονομάτων τομέα), χρησιμοποιώντας τη διεύθυνση IP του εξυπηρετητή, https://192.168.204.134:33333.

Σημείωση: Επειδή το πιστοποιητικό SSL, που έχουμε δημιουργήσει για την ασφαλή σύνδεση, δεν είναι υπογεγραμμένο από κάποια αναγνωρισμένη, ανεξάρτητη αρχή, αυτό θεωρείται «μη εμπιστεύσιμο» και για να ολοκληρωθεί η σύνδεσή μας, θα πρέπει με τα παρακάτω δύο βήματα να προστεθεί η σχετική εξαίρεση:

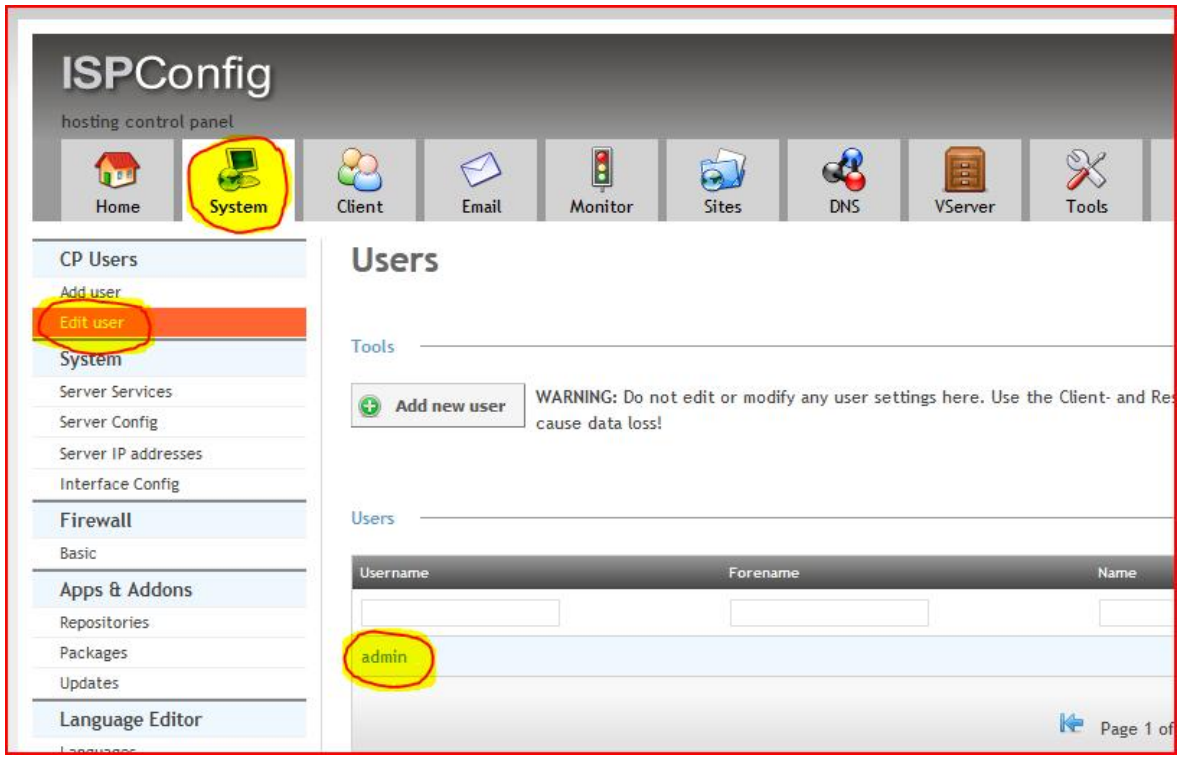




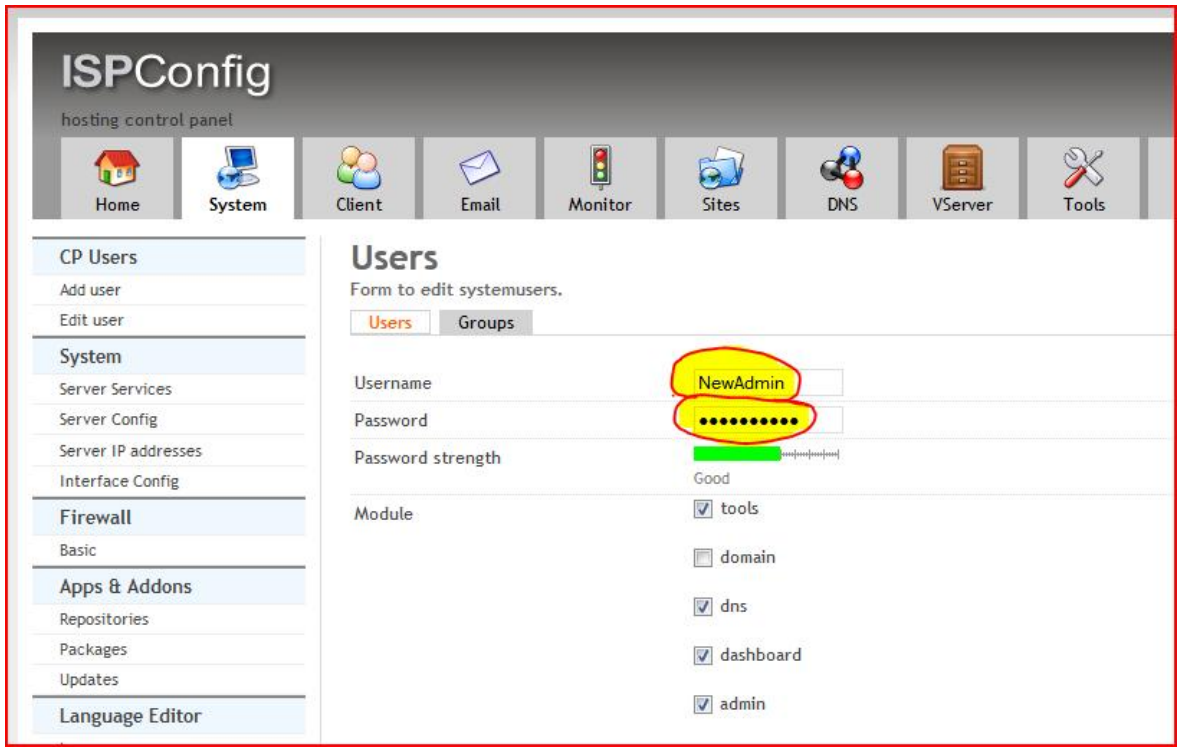
Μετά την προσθήκη της παραπάνω εξαίρεσης ασφαλείας, απομένει να εισάγουμε το όνομα χρήστη καθώς και τον αντίστοιχο κωδικό ώστε να «εισέλθουμε» στην εφαρμογή ISPConfig. Οι προκαθορισμένες τιμές είναι και για τις δύο παραμέτρους «admin» και, όπως είναι προφανές, αυτές θα πρέπει να τροποποιηθούν άμεσα!



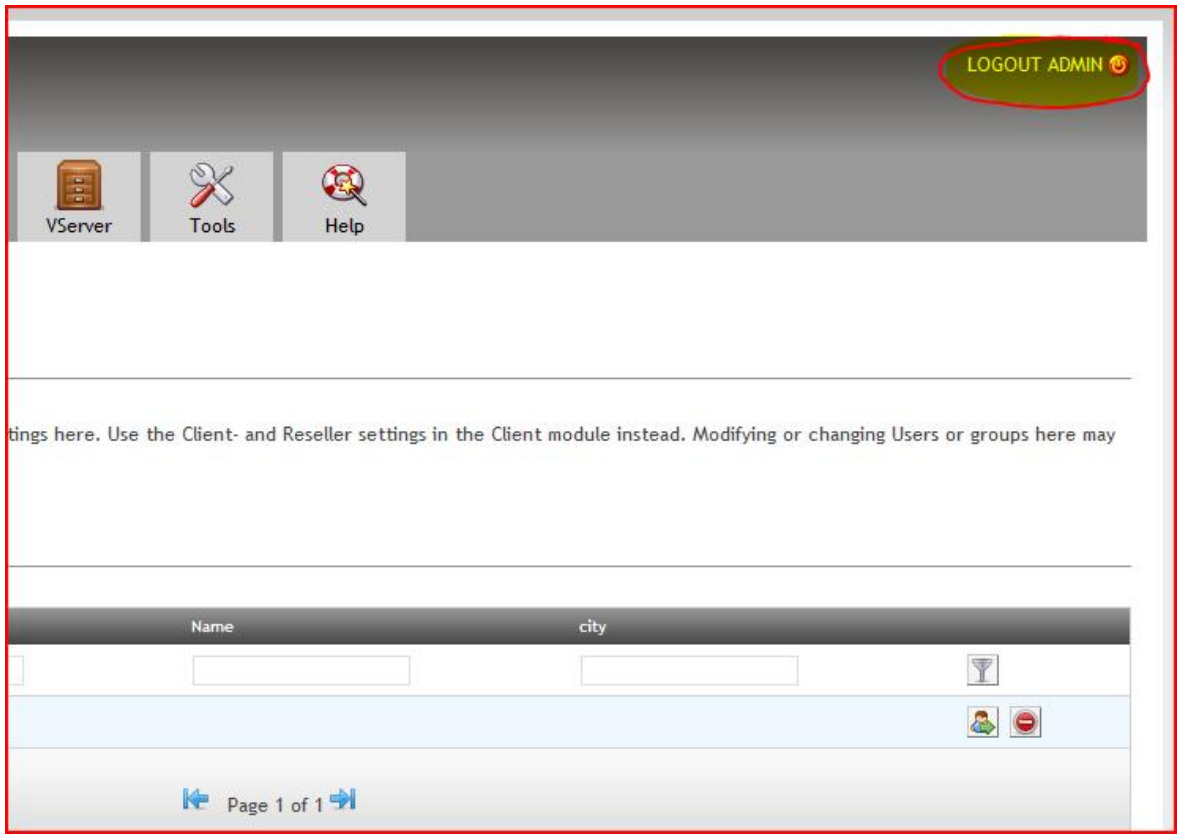
Οδηγία: Επιλέγουμε, με τη συγκεκριμένη σειρά, την καρτέλα με τις ρυθμίσεις του συστήματος (System), την περιοχή επεξεργασίας υπαρχόντων χρηστών (Edit user) και τέλος τον προκαθορισμένο χρήστη (admin):



Οδηγία: Εισάγουμε το νέο, επιθυμητό όνομα του διαχειριστή της εφαρμογής (στο παράδειγμα του οδηγού NewAdmin), καθώς και τον κωδικό αυτού (η εφαρμογή μας ενημερώνει αυτόματα για την πολυπλοκότητα του κωδικού πρόσβασης):



Οδηγία: Αποθηκεύουμε τις τροποποιήσεις κάνοντας κλικ στην επιλογή «Save» και, για να ισχύσουν άμεσα αυτές, αποσυνδεόμαστε χρησιμοποιώντας την αντίστοιχη επιλογή «LOGOUT ADMIN»:



Σε αυτό το σημείο η εγκατάσταση της εφαρμογής ISPConfig έχει ολοκληρωθεί και μαζί με αυτή έχει περατωθεί και το δεύτερο στάδιο εγκατάστασης και παραμετροποίησης του λογισμικού που απαιτείται, ώστε αφενός να παρέχονται οι υπηρεσίες του συστήματος, αφετέρου να είναι στο μέγιστο βαθμό απλοποιημένη η διαδικασία εποπτείας και διαχείρισης αυτού. Ο εξυπηρετητής είναι τώρα σχεδόν έτοιμος να τεθεί σε επιχειρησιακή λειτουργία, αφού πλέον είναι σε θέση να προσφέρει στο διαχειριστή του τη δυνατότητα να εισάγει με απλοποιημένο τρόπο νέους χρήστες, να ρυθμίζει εύκολα τις παραμέτρους που τους αφορούν και να εποπτεύει χωρίς καμία δυσκολία τη λειτουργία των διαδικτυακών υπηρεσιών που παρέχονται σε αυτούς.

Πάραυτα, ο οδηγός δε θα περατωθεί στο σημείο αυτό. Θα συνεχιστεί στο αμέσως επόμενο κεφάλαιο με την παρουσίαση βασικών λειτουργιών του πίνακα ελέγχου ISPConfig, καθώς και ορισμένων επιπλέον ρυθμίσεων και ενεργειών που είναι ωφέλιμο να λάβουν χώρα πριν από την έναρξη χρήσης του συστήματος, μιας και αφορούν στη βελτιστοποίηση του επιπέδου ασφάλειας του εξυπηρετητή.

ΚΕΦΑΛΑΙΟ 4

Στο προηγούμενο κεφάλαιο ολοκληρώθηκε το δεύτερο στάδιο του οδηγού της παρούσας εργασίας, που αφορά στην εγκατάσταση και παραμετροποίηση όλου του λογισμικού που απαιτείται για την παροχή των υπηρεσιών του εξυπηρετητή, αλλά και της δυνατότητας εποπτείας καθώς και διαχείρισης αυτού, μέσα από τον πίνακα ελέγχου ISPConfig. Το σύστημα είναι πλέον πολύ κοντά στο να δύναται να χρησιμοποιηθεί επιχειρησιακά, αφού απομένουν ελάχιστες ακόμη ενέργειες που θα πρέπει να λάβουν χώρα στο παρών κεφάλαιο και οι οποίες αφενός αφορούν στη ρύθμιση υπηρεσιών του συστήματος, αφετέρου αποσκοπούν στην αύξηση του επιπέδου της παρεχόμενης ασφάλειας αυτού.

Στο πρώτο στάδιο του τρέχοντος κεφαλαίου, θα αναλυθεί η διαδικασία με την οποία γίνεται η προσθήκη του βασικού, διαχειριστικού χρήστη – πελάτη του συστήματος, ώστε στη συνέχεια να είναι δυνατή η πραγματοποίηση ρυθμίσεων όπως η ρύθμιση παραμέτρων του ονόματος τομέα, του ιστοτόπου, καθώς και του ηλεκτρονικού ταχυδρομείου του βασικού χρήστη – πελάτη, του εξυπηρετητή ονομάτων τομέα του συστήματος κτλ. Μετά την ολοκλήρωση αυτών των ρυθμίσεων, το σύστημα θα είναι καθ’ όλα έτοιμο να υποδεχθεί την εισαγωγή των νέων χρηστών και να προσφέρει σε αυτούς όλες τις αναμενόμενες υπηρεσίες διαδικτύου.

Ελάχιστα πριν από την επιχειρησιακή χρήση του συστήματος θα ακολουθήσει ένα από τα τελευταία στάδια του οδηγού της παρούσας πτυχιακής εργασίας το οποίο αφορά στη διαδικασία του system hardening [89]. Η συγκεκριμένη διαδικασία περιλαμβάνει περαιτέρω ρυθμίσεις, καθώς και σχετικές ενέργειες που θα πρέπει να λάβουν χώρα ώστε να βελτιστοποιηθεί η προστασία του συστήματος απέναντι σε κακόβουλες προς αυτό ενέργειες. Για να γίνει κατανοητή η φύση της συγκεκριμένης διαδικασίας, αρκεί το να αναλογιστεί κανείς την προκαθορισμένη διεύθυνση διεπαφής του περιβάλλοντος διαχείρισης της υπηρεσίας MySQL (http://www.mydomain.gr/**phpmyadmin**). Όπως είναι φυσικό, εάν η εν λόγω διεύθυνση δεν τροποποιηθεί κατάλληλα, είναι περισσότερο από πιθανό να χρησιμοποιηθεί σε «μηχανικές», αυτοματοποιημένες επιθέσεις που στηρίζονται σε σχετικά κακόβουλα script, υποβαθμίζοντας με αυτό τον τρόπο το επίπεδο ασφαλείας του συστήματος.

Τέλος, το μόνο που απομένει για την ολοκλήρωση του παρόντος οδηγού είναι το να ληφθεί μέριμνα για τη λήψη αντιγράφων ασφαλείας και του λογισμικού του συστήματος, αλλά και των περιεχομένων του φακέλου των χρηστών αυτού. Όπως έχει ήδη αναφερθεί, το αντίγραφο ασφαλείας του λογισμικού του καθ' όλα επιχειρησιακού συστήματος θα δημιουργηθεί στην κατάτμηση του δίσκου που στερείται σημείου προσάρτησης και θα προστεθεί στο λογισμικό εκκίνησης του συστήματος, ώστε μετά από πιθανή βλάβη στο υλικό ή/και το λογισμικό ο εξυπηρετητής θα είναι σε θέση να λειτουργήσει και πάλι μετά από μια απλή επανεκκίνηση. Ο φάκελος χρηστών θα χρησιμοποιείται κοινόχρηστα ανάμεσα στα δύο αντίγραφα του λογισμικού του συστήματος και θα δρομολογηθεί η αυτόματη λήψη αντίγραφων ασφαλείας και του συγκεκριμένου φακέλου στην ίδια κατάτμηση με το αντίγραφο του συστήματος.

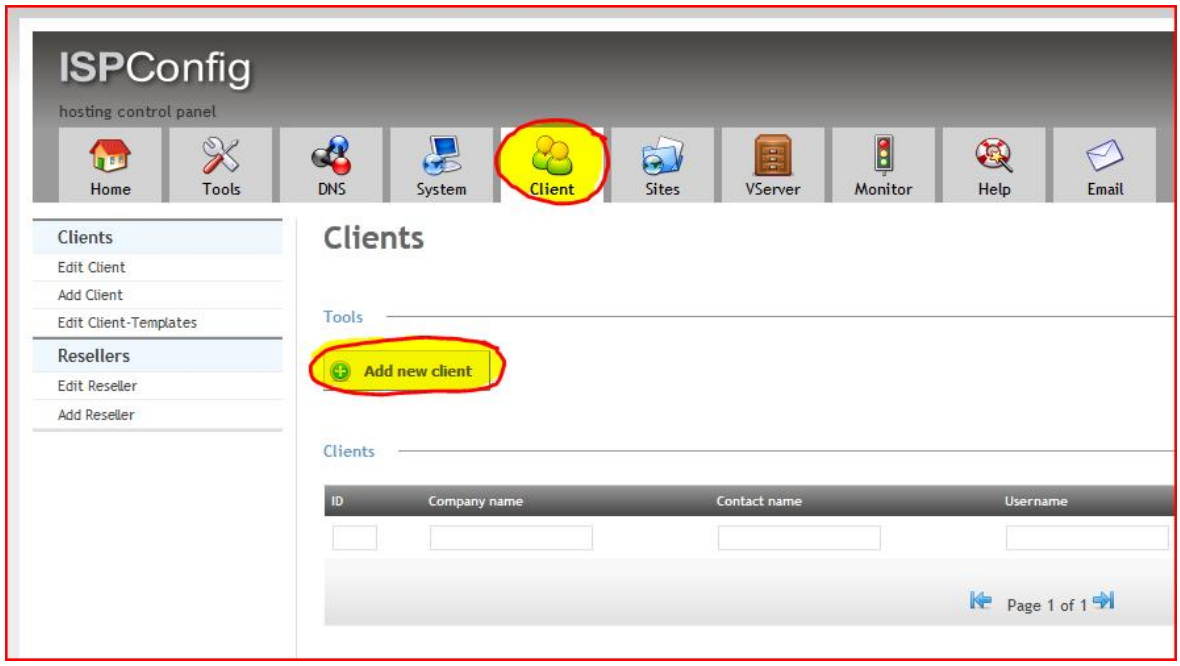
Προσθήκη διαχειριστικού χρήστη

Τα βήματα εισαγωγής του βασικού, διαχειριστικού χρήστη – πελάτη στο σύστημα είναι πανομοιότυπα με αυτά που απαιτούνται για την εισαγωγή όλων των υπολοίπων χρηστών αυτού, έτσι, η διαδικασία θα αναφερθεί συγκεντρωτικά στα αμέσως επόμενα βήματα. Ο συγκεκριμένος ξεχωριστός λογαριασμός χρήστη «διαχείρισης» απαιτείται να δημιουργηθεί ώστε να είναι δυνατή η ρύθμιση ορισμένων παραμέτρων του συστήματος (όπως αυτών του εξυπηρετητή ονομάτων τομέα του συστήματος), η οποία θα λάβει χώρα ακολούθως.

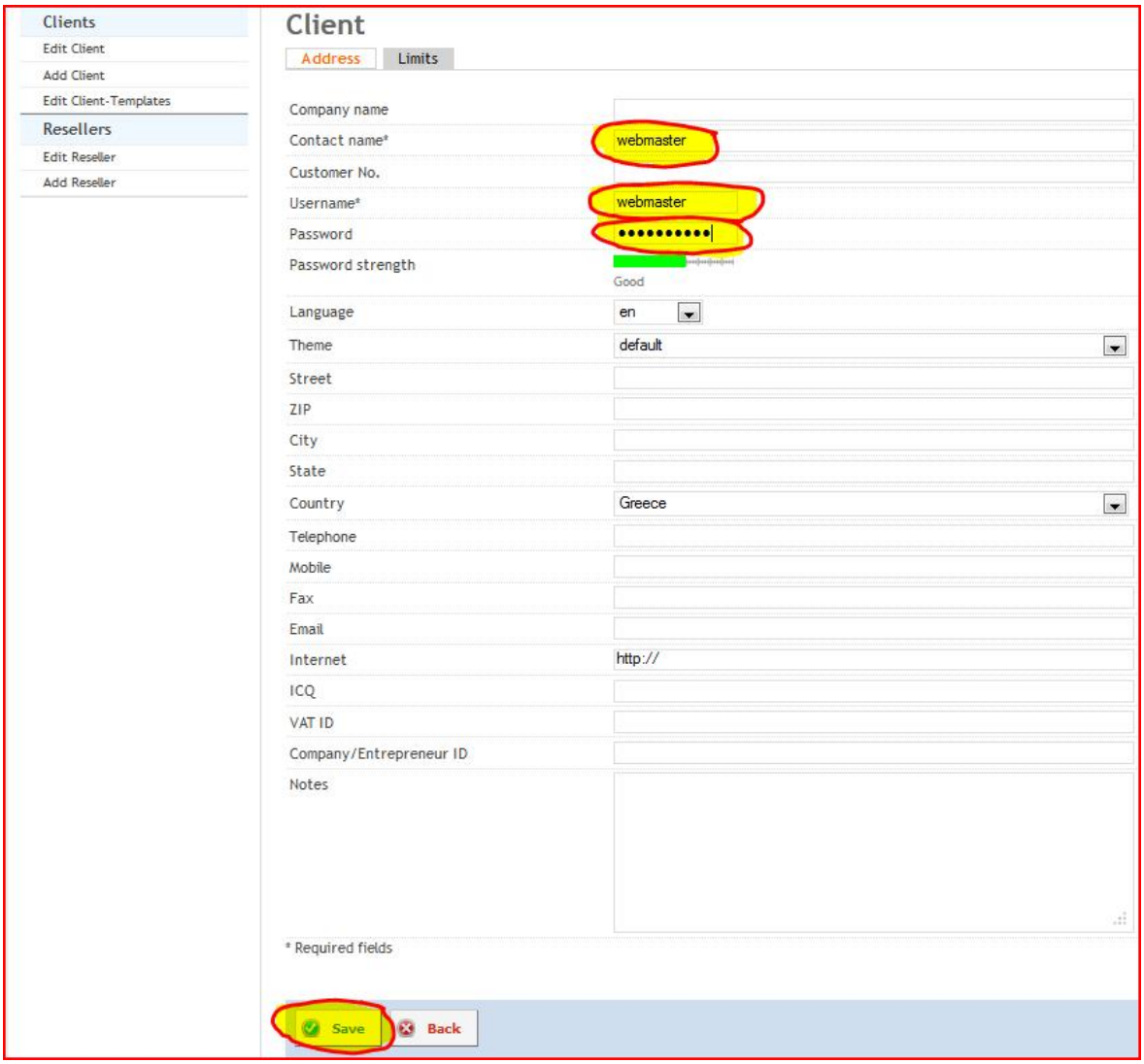
Η διαδικασία εισαγωγής νέου χρήστη – πελάτη στο σύστημα περιλαμβάνει την προσθήκη του πελάτη, του ονόματος τομέα, του ιστοτόπου, του χρήστη FTP, της ζώνης ονομάτων τομέα και των λογαριασμών ηλεκτρονικού ταχυδρομείου αυτού, όπως παρακάτω:

Προσθήκη πελάτη

Οδηγία: Επιλέγουμε, με τη συγκεκριμένη σειρά, την καρτέλα με τις ρυθμίσεις των χρηστών – πελατών (Client), και στη συνέχεια την επιλογή προσθήκης νέου πελάτη (add new client):



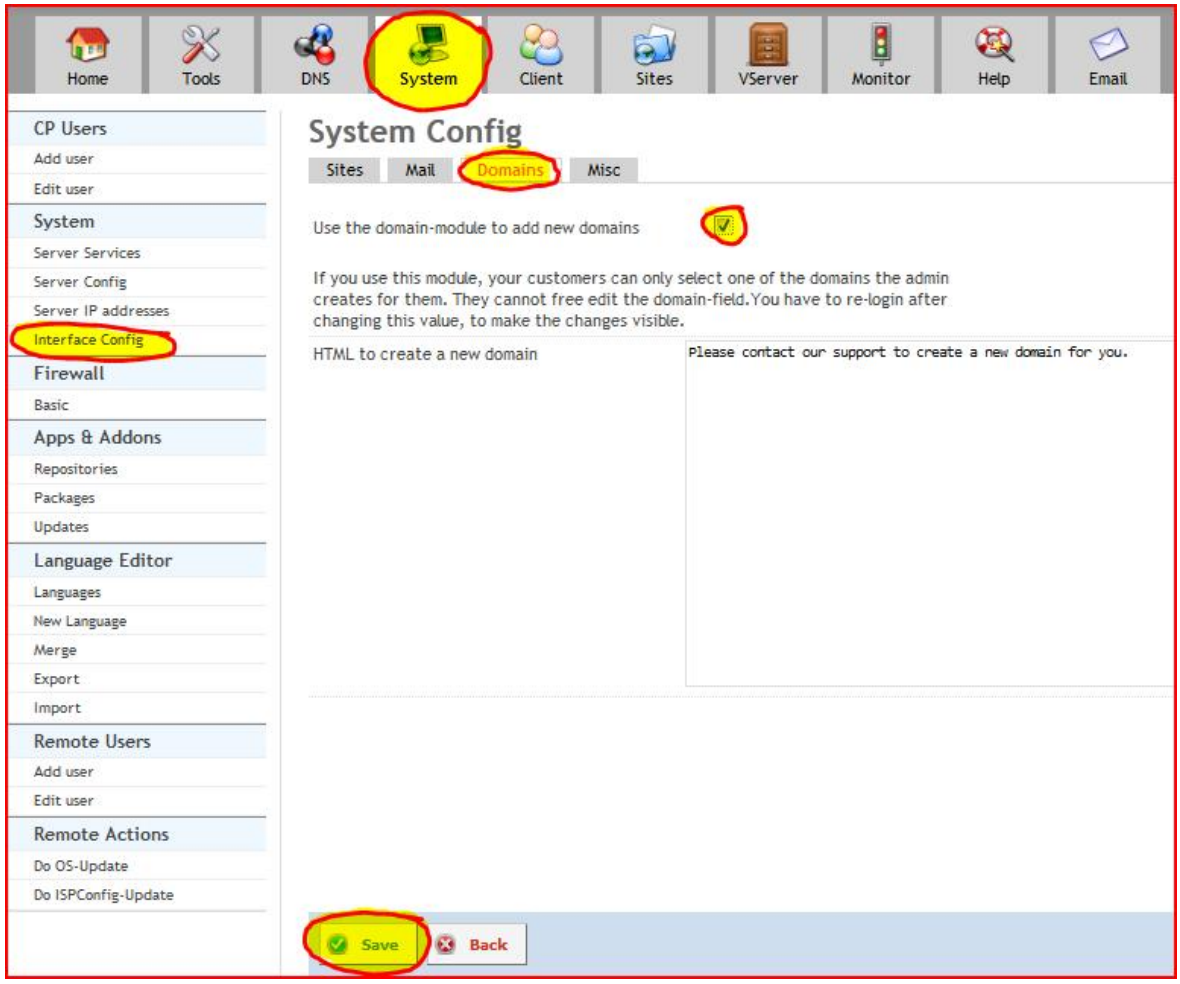
Οδηγία: Στη νέα σελίδα που εμφανίζεται εισάγουμε τα στοιχεία που αφορούν στο διαχειριστικό χρήστη – πελάτη του συστήματος. Για να αποθηκευθεί ο νέος χρήστης με χρήση της επιλογής (Save) είναι απαραίτητη η εισαγωγή του ονόματος της επαφής (Contact name), του ονόματος του χρήστη (Username), καθώς και του κωδικού πρόσβασης (Password) αυτού. Τα υπόλοιπα πεδία είναι μεν αυτονόητα, όχι όμως και αναγκαία για την προσθήκη του πελάτη:



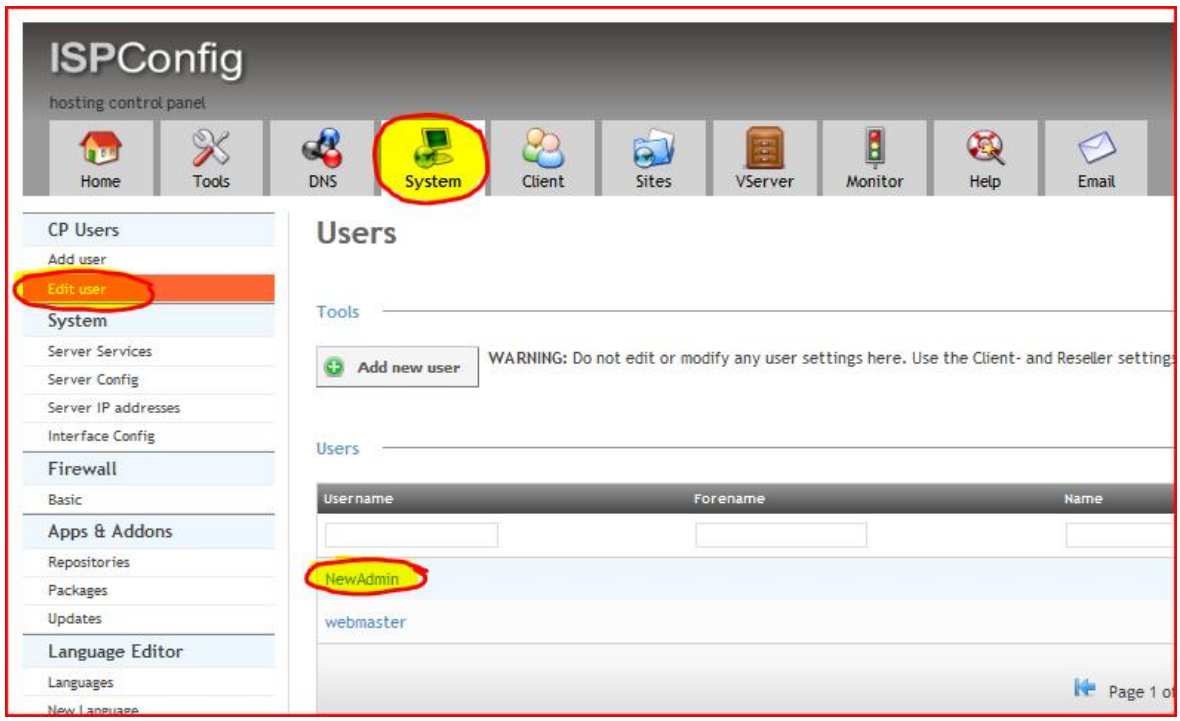
Προσθήκη ονόματος τομέα

Σημείωση: Για την προσθήκη ονόματος τομέα θα πρέπει αρχικά να πραγματοποιηθούν οι ρυθμίσεις που απαιτούνται για την εμφάνιση της καρτέλας του αρθρώματος ονομάτων τομέα στον πίνακα ελέγχου ISPConfig. Η συγκεκριμένη διαδικασία θα λάβει χώρα με τα αμέσως παρακάτω βήματα και θα πρέπει να παραλείπεται στις μετέπειτα εισαγωγές ονομάτων τομέα.

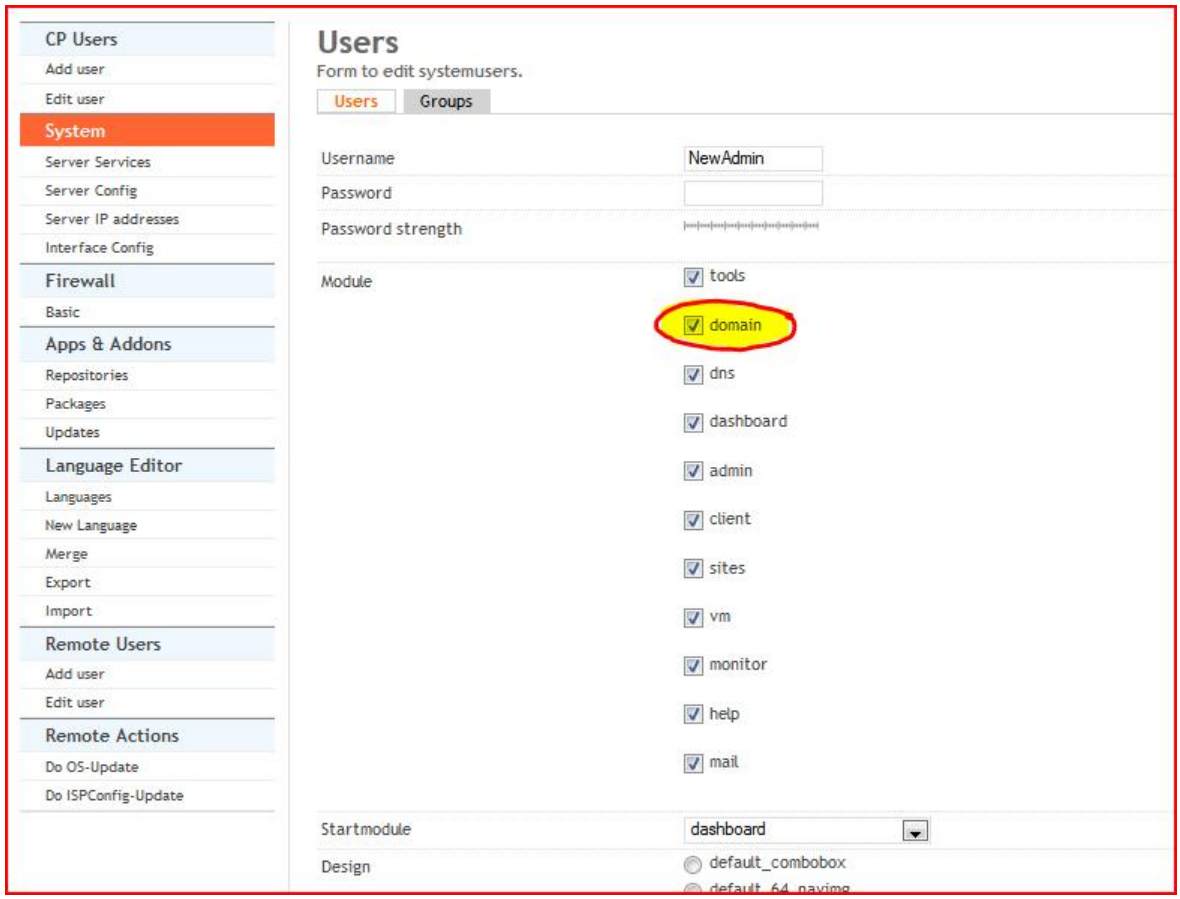
Οδηγία: Επιλέγουμε, με τη συγκεκριμένη σειρά, την καρτέλα με τις ρυθμίσεις του συστήματος (System), την περιοχή επιλογών των ρυθμίσεων του περιβάλλοντος διεπαφής (Interface Config) και τέλος την καρτέλα με τις ρυθμίσεις των ονομάτων τομέα (Domains). Στην εν λόγω καρτέλα, ενεργοποιούμε τη χρήση του αρθρώματος ονομάτων τομέα για την εισαγωγή νέων ονομάτων τομέα (Use the domain-module to add new domains) και τέλος, αποθηκεύουμε τις ρυθμίσεις με χρήση της αντίστοιχης επιλογής (Save):



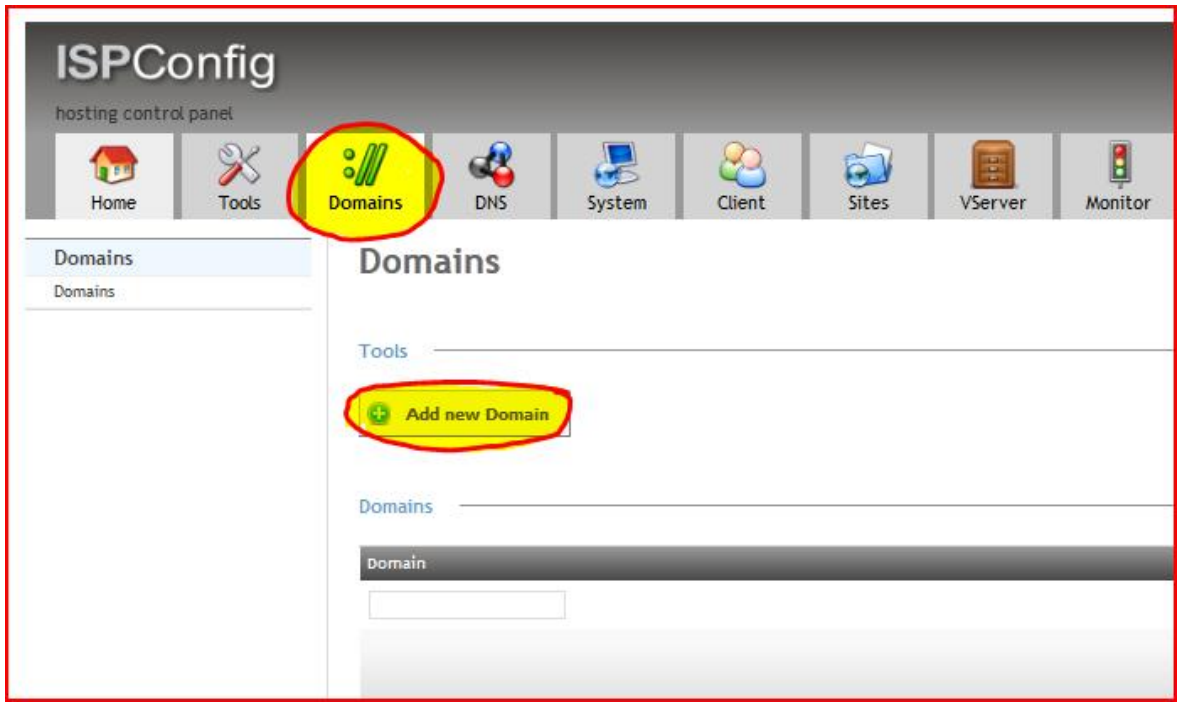
Οδηγία: Για να ενεργοποιηθεί η παραπάνω επιλογή θα πρέπει να πραγματοποιήσουμε μια επιπλέον ρύθμιση, για την οποία επιλέγουμε την καρτέλα με τις ρυθμίσεις του συστήματος (System), την περιοχή επιλογών επεξεργασίας των χρηστών του πίνακα ελέγχου (Edit user) και τέλος το διαχειριστή του πίνακα ελέγχου (NewAdmin):



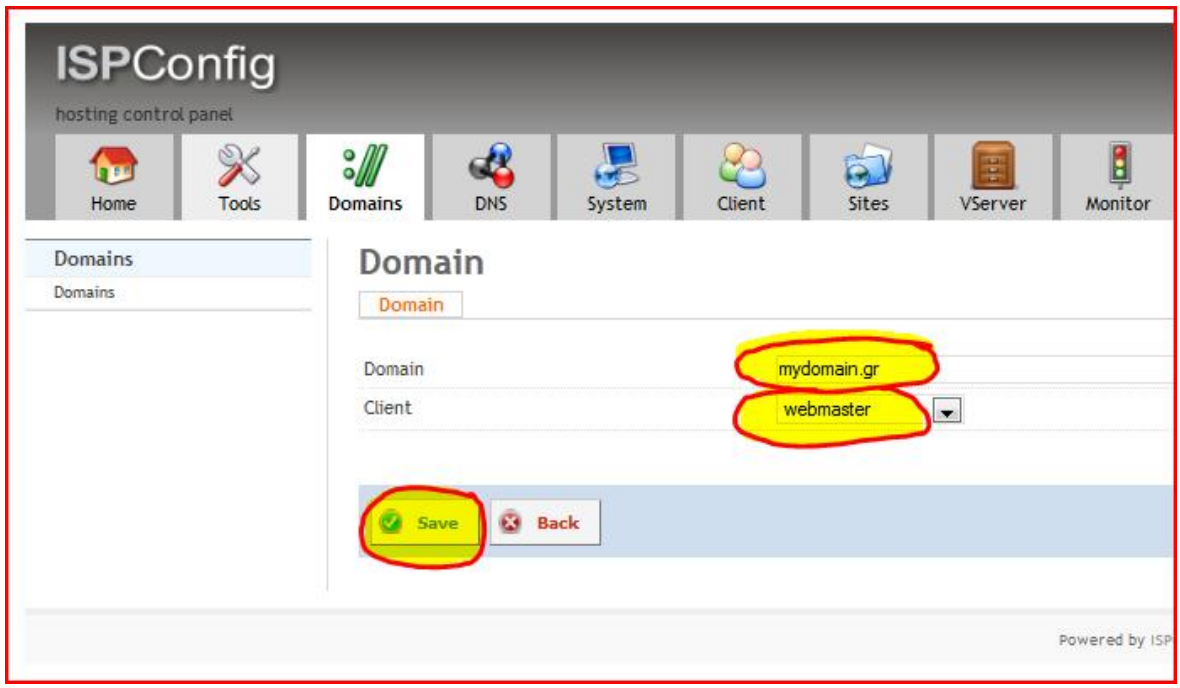
Οδηγία: Στη νέα σελίδα επιλέγουμε να εμφανίζεται το άρθρωμα ονομάτων τομέα (domain), αποθηκεύουμε την αλλαγή και στη συνέχεια αποσυνδεόμαστε και συνδεόμαστε εκ νέου στον πίνακα ελέγχου, ώστε η αλλαγή αυτή να ενεργοποιηθεί:



Οδηγία: Μετά την επανασύνδεση παρατηρούμε ότι είναι πλέον διαθέσιμη και η καρτέλα του αρθρώματος ονομάτων τομέα (Domains), την οποία επιλέγουμε, ώστε να είμαστε σε θέση να προσθέσουμε το νέο όνομα τομέα (Add new Domain) του διαχειριστικού χρήστη. Το παρών είναι και το μόνο βήμα που θα πρέπει από τώρα και στο εξής να εκτελείται για την εισαγωγή νέων ονομάτων τομέα:



Οδηγία: Στη νέα σελίδα ρυθμίσεων, εισάγουμε το όνομα τομέα (Domain) του συστήματος και στη συνέχεια επιλέγουμε από τη διαθέσιμη λίστα το διαχειριστικό χρήστη – πελάτη (Client). Τέλος, αποθηκεύουμε τις αλλαγές με χρήση της αντίστοιχης επιλογής (Save):



Προσθήκη ζώνης ονομάτων τομέα

Η δικτυακή επικοινωνία των πληροφοριακών συστημάτων είναι γνωστό ότι επιτυγχάνεται με ανταλλαγή δεδομένων σε μορφή πακέτων. Στο καθένα από αυτά τα πακέτα περιλαμβάνεται μια «επικεφαλίδα» (header), στην οποία μεταξύ των υπολοίπων παραμέτρων αναφέρονται οι διευθύνσεις δικτύου του συστήματος αποστολέα, καθώς και του συστήματος παραλήπτη του πακέτου. Ο χρήστης λοιπόν οποιασδήποτε υπηρεσίας ενός απομακρυσμένου δικτυακού συστήματος θα πρέπει απαραίτητα να γνωρίζει τη διεύθυνση δικτύου αυτού.

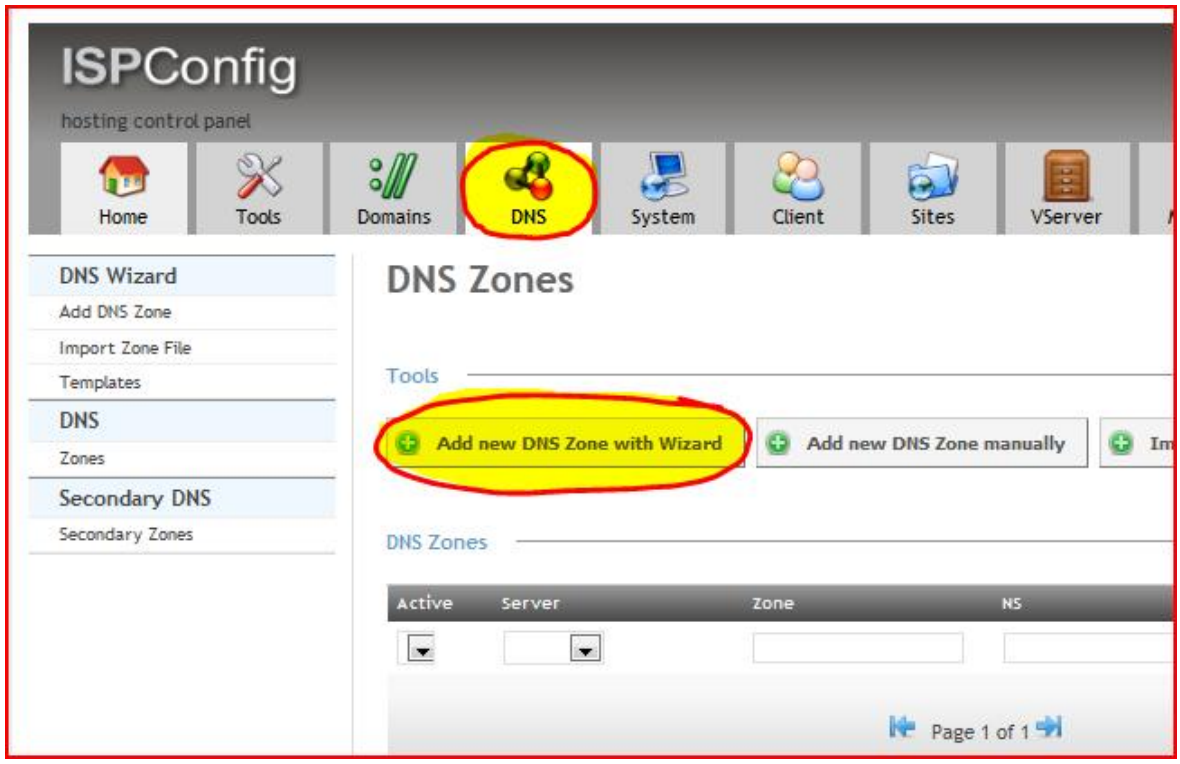
Ο ανθρώπινος εγκέφαλος όμως απομνημονεύει ευκολότερα ένα όνομα τομέα της μορφής google.gr, παρά μια διεύθυνση δικτύου της μορφής 173.194.35.159. Με στόχο την απλοποίηση της διαδικασίας από τη μεριά των χρηστών, έχουν δημιουργηθεί οι εξυπηρετητές ονομάτων τομέα (DNS), οι οποίοι είναι υπεύθυνοι να διατηρούν ενημερωμένους πίνακες με τα ονόματα τομέα και τις διευθύνσεις δικτύου διαδικτυακών συστημάτων και να αντιστοιχούν τη μία παράμετρο με την άλλη. Έτσι, ο χρήστης τελικά

ζητά να επικοινωνήσει με το πληροφοριακό σύστημα χρησιμοποιώντας το όνομα αυτού και ο εξυπηρετητής ονομάτων τομέα είναι αρμόδιος να το αντικαταστήσει με την αντίστοιχη διεύθυνση δικτύου.

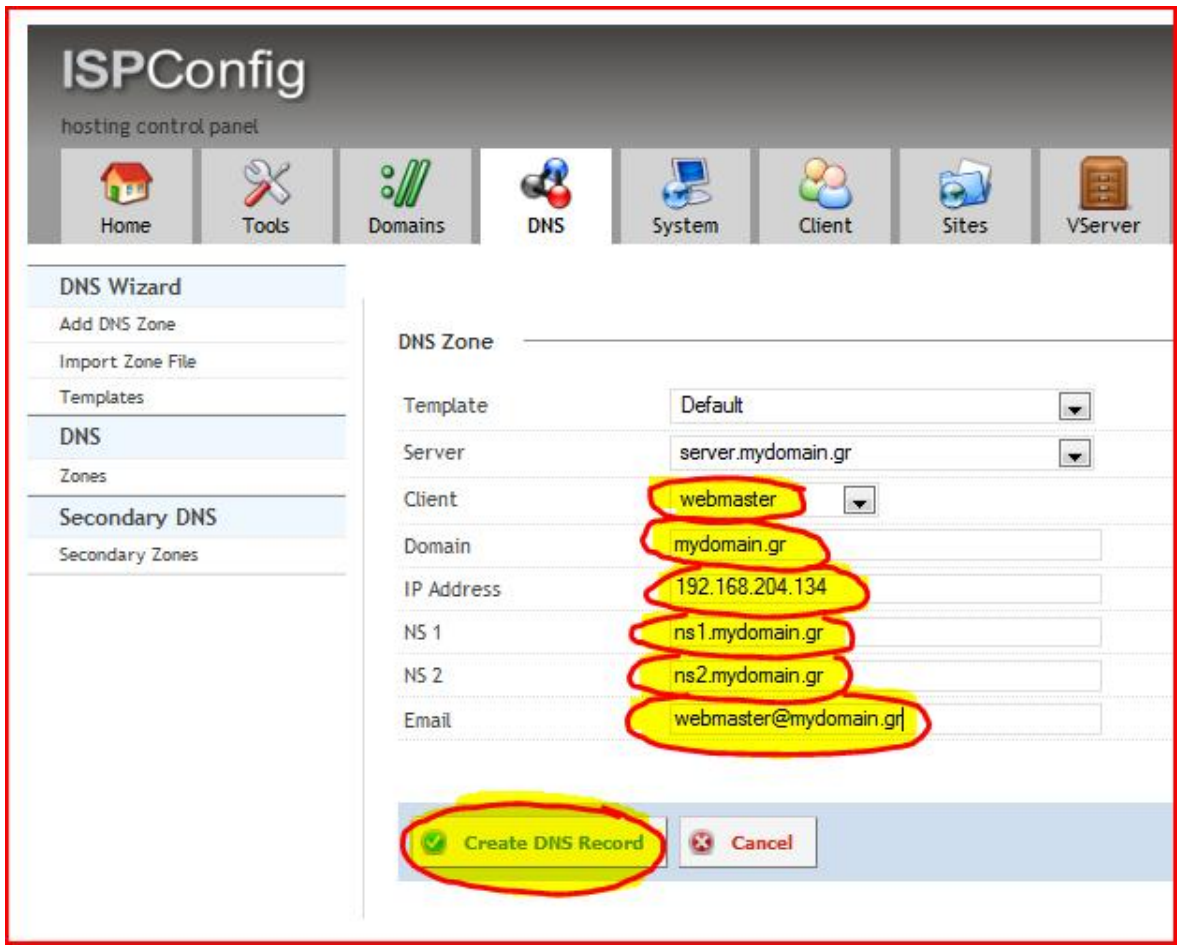
Στον εξυπηρετητή της παρούσας εργασίας έχει εγκατασταθεί και ήδη λειτουργεί η υπηρεσία ονομάτων τομέα και έτσι μπορούν να δημιουργηθούν οι αντίστοιχες εγγραφές για τις ζώνες ονομάτων τομέα των διευθύνσεων που αφορούν στους χρήστες του συστήματος. Αυτό σημαίνει ότι θα δημιουργηθούν αφενός οι πίνακες αντιστοίχισης των ονομάτων τομέα με τη διεύθυνση δικτύου του εξυπηρετητή, αφετέρου όμως θα πρέπει να δημιουργηθούν και οι εγγραφές για τους διακομιστές ονομάτων (nameservers) που θα παρέχουν αυτή την υπηρεσία. Οι εν λόγω διακομιστές θα πρέπει να είναι τουλάχιστον δύο ξεχωριστά συστήματα (ns1 και ns2), στην περίπτωση του οδηγού όμως, για λόγους απλούστευσης της διαδικασίας, θα χρησιμοποιηθεί το ίδιο και το αυτό σύστημα.

Σημείωση: Σημαντικό είναι λαμβάνεται υπόψη το απαιτείται χρονικό διάστημα που μπορεί να φτάσει και τις 24-48 ώρες (μερικές φορές ακόμη και περισσότερο), μέχρι να ενημερωθούν αυτόματα όλοι οι εξυπηρετητές ονομάτων τομέα ανά την υφήλιο για τις αλλαγές που πραγματοποιήθηκαν τοπικά, στον εξυπηρετητή της εργασίας.

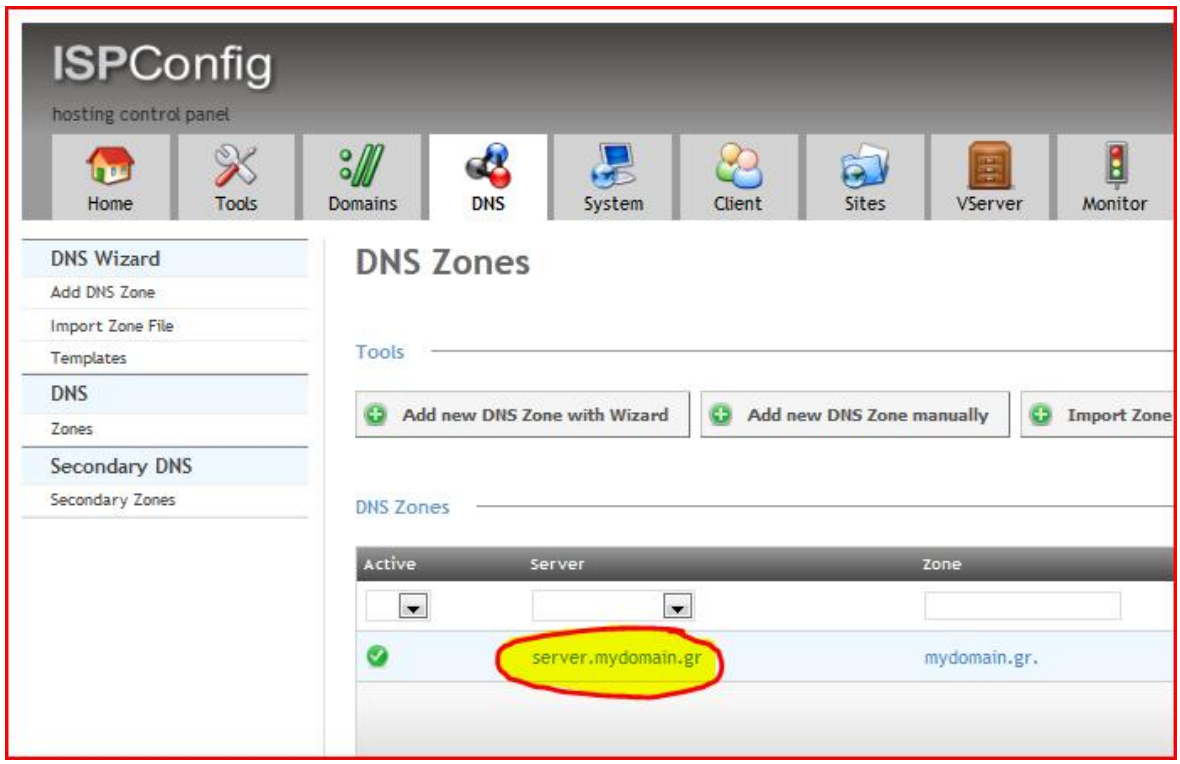
Οδηγία: Ενεργοποιούμε την καρτέλα των ρυθμίσεων της υπηρεσίας ονομάτων τομέα (DNS) και στη συνέχεια επιλέγουμε την προσθήκη νέας ζώνης ονομάτων τομέα με τη βοήθεια μάγου (Add new DNS zone with Wizard):



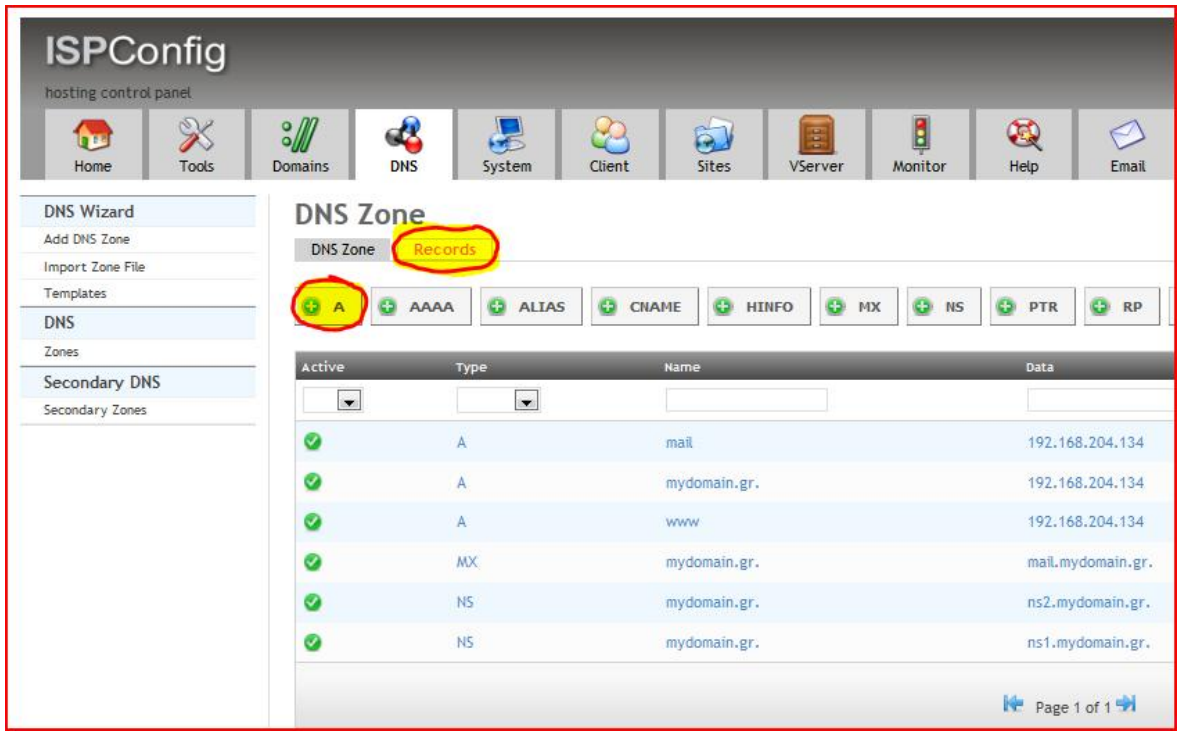
Οδηγία: Επιλέγουμε το διαχειριστή – πελάτη από τη λίστα πελατών (Client) και στη συνέχεια εισάγουμε στα αντίστοιχα πεδία το όνομα τομέα (Domain), τη διεύθυνση δικτύου του εξυπηρετητή (IP Address), τους διακομιστές ονομάτων (NS1, NS2) και τέλος, το λογαριασμό ηλεκτρονικού ταχυδρομείου του διαχειριστή του συστήματος (Email), ο οποίος θα δημιουργηθεί σε επόμενο βήμα. Τέλος, επιλέγουμε τη δημιουργία της εγγραφής της υπηρεσίας ονομάτων τομέα (Create DNS Record):



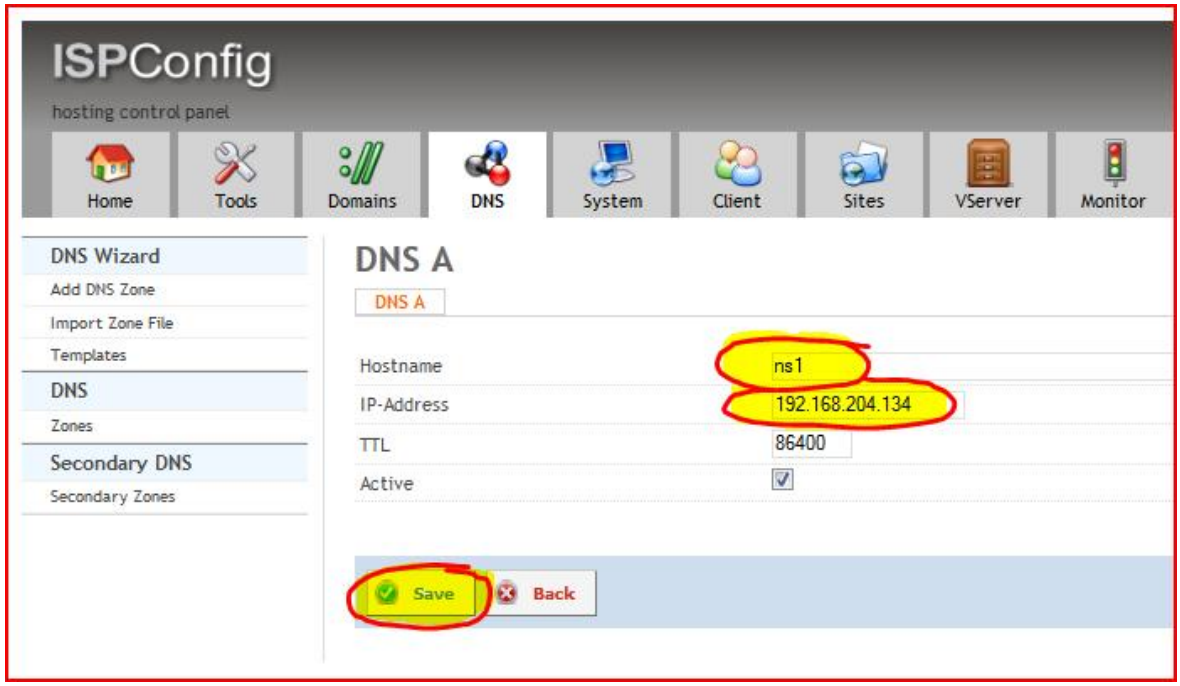
Οδηγία: Πέρα από τις εγγραφές που δημιουργήθηκαν αυτόματα από το μάγο της προσθήκης νέας ζώνης ονομάτων τομέα, θα πρέπει να πραγματοποιηθούν χειρωνακτικά ορισμένες ακόμη. Για να επιτευχθεί αυτό ανοίγουμε τη ζώνη ονομάτων τομέα που μόλις δημιουργήσαμε κάνοντας κλικ πάνω της:



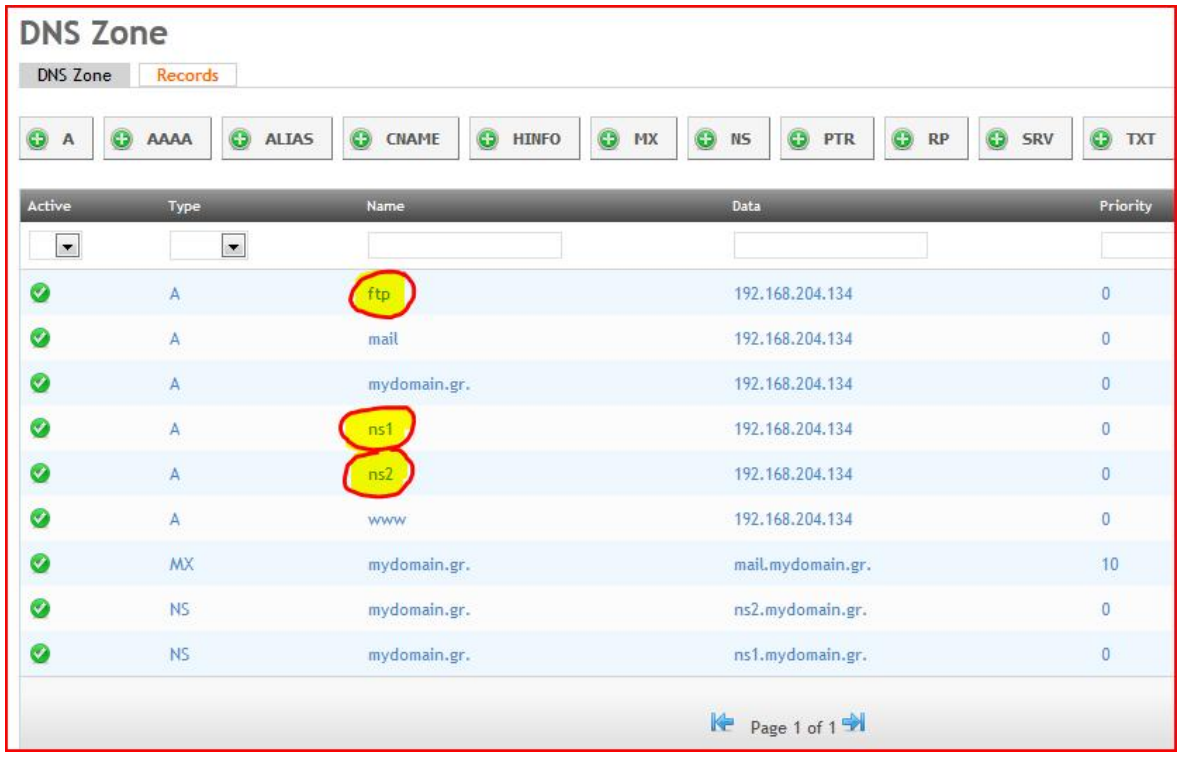
Οδηγία: Επιλέγουμε την καρτέλα των εγγραφών της ζώνης ονομάτων τομέα και στη συνέχεια κάνουμε κλικ στην επιλογή προσθήκης νέας εγγραφής τύπου «A»:



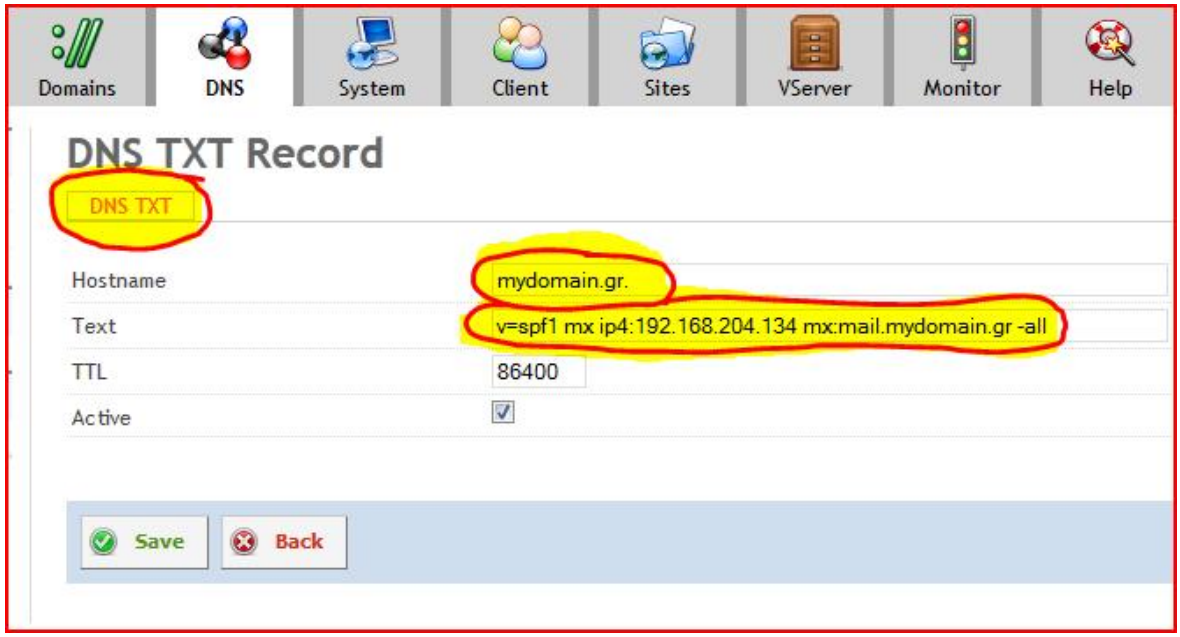
Οδηγία: Εισάγουμε στα αντίστοιχα πεδία το όνομα της υπηρεσίας του συστήματος (Hostname), καθώς και τη διεύθυνση δικτύου αυτού (IP-Address) και αποθηκεύουμε τις αλλαγές (Save):



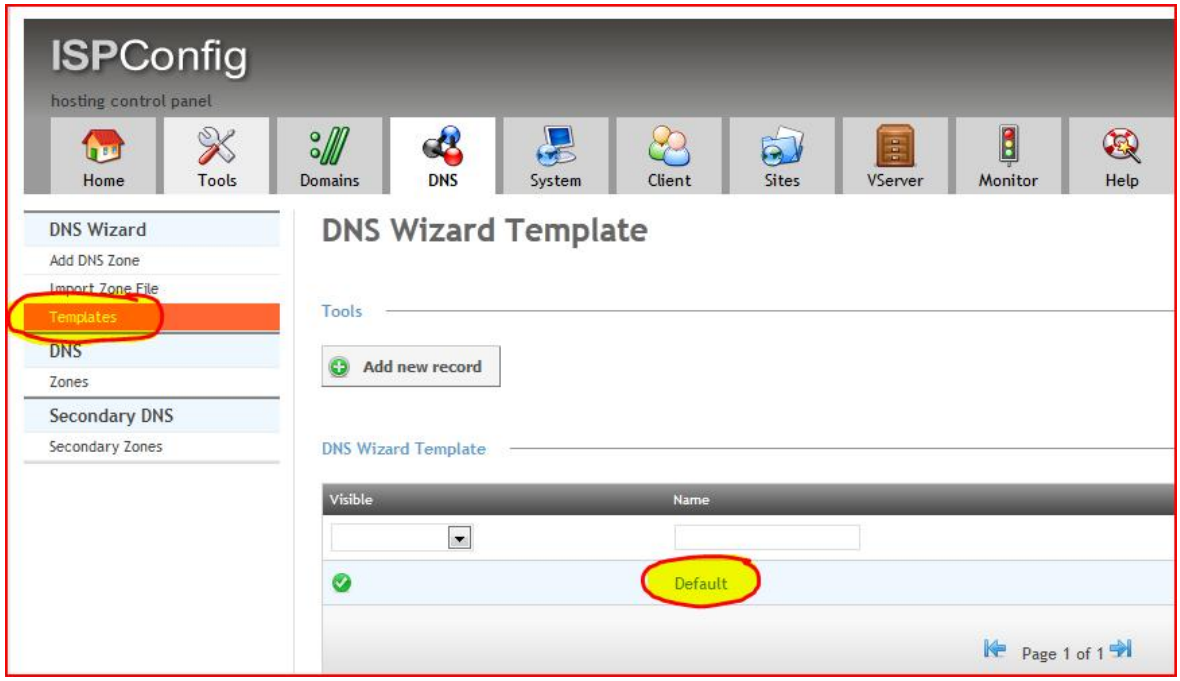
Οδηγία: Με την παραπάνω διαδικασία προσθέτουμε εγγραφές τύπου «A» για τις υπηρεσίες ns1, ns2 και ftp, ώστε τελικά να αποκτήσουμε το παρακάτω αποτέλεσμα:



Οδηγία: Για την ολοκλήρωση της διαδικασίας, απομένει η προσθήκη μιας εγγραφής τύπου «TXT» η οποία θα αντιστοιχεί τον εξυπηρετητή ηλεκτρονικού ταχυδρομείου του συστήματος με τη διεύθυνση δικτύου αυτού, όπως προβλέπεται στο πλαίσιο πολιτικής αποστολέα (SPF) [90]. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στην περίοδο (τελεία), που θα πρέπει να υπάρχει μετά το όνομα τομέα στο αντίστοιχο πεδίο:



Οδηγία: Βέβαια, σε κάθε επανάληψη της διαδικασίας προσθήκης της ζώνης ονομάτων τομέα για τον εκάστοτε νέο χρήστη, θα πρέπει οι παραπάνω FTP και SPF εγγραφές που αφορούν στους υπόλοιπους μη διαχειριστικούς χρήστες – πελάτες να γίνονται αυτόματα από το σχετικό μάγο (οι εγγραφές ns1 και ns2 αφορούν στο διαχειριστικό χρήστη και μόνο). Έτσι, με σκοπό να πραγματοποιήσουμε τις απαιτούμενες τροποποιήσεις, επιλέγουμε την περιοχή προτύπων (Templates) και ανοίγουμε το προκαθορισμένο πρότυπο (Default) για επεξεργασία:



Οδηγία: Στο πεδίο εγγραφών του προτύπου αντικαθιστούμε τις προκαθορισμένες εγγραφές με νέες, όπως στον παρακάτω πίνακα:

Προκαθορισμένες εγγραφές	Νέες εγγραφές
[ZONE] origin={DOMAIN}. ns={NS1}. mbox={EMAIL}. refresh=7200 retry=540 expire=604800 minimum=86400 ttl=3600 [DNS_RECORDS] A|{DOMAIN}.|{IP}|0|3600 A|www|{IP}|0|3600 A|mail|{IP}|0|3600 NS|{DOMAIN}.|{NS1}.|0|3600 NS|{DOMAIN}.|{NS2}.|0|3600 MX|{DOMAIN}.|mail.{DOMAIN}.|10|3600	[ZONE] origin={DOMAIN}. ns={NS1}. mbox={EMAIL}. refresh=7200 retry=540 expire=604800 minimum=86400 ttl=3600 [DNS_RECORDS] A|{DOMAIN}.|{IP}|0|3600 A|www|{IP}|0|3600 A|mail|{IP}|0|3600 A|ftp|{IP}|0|3600 NS|{DOMAIN}.|{NS1}.|0|3600 NS|{DOMAIN}.|{NS2}.|0|3600 MX|{DOMAIN}.|mail.{DOMAIN}.|10|3600 TXT|{DOMAIN}.|v=spf1 mx ip4:{IP} mx:mail.{DOMAIN} -all|0|86400

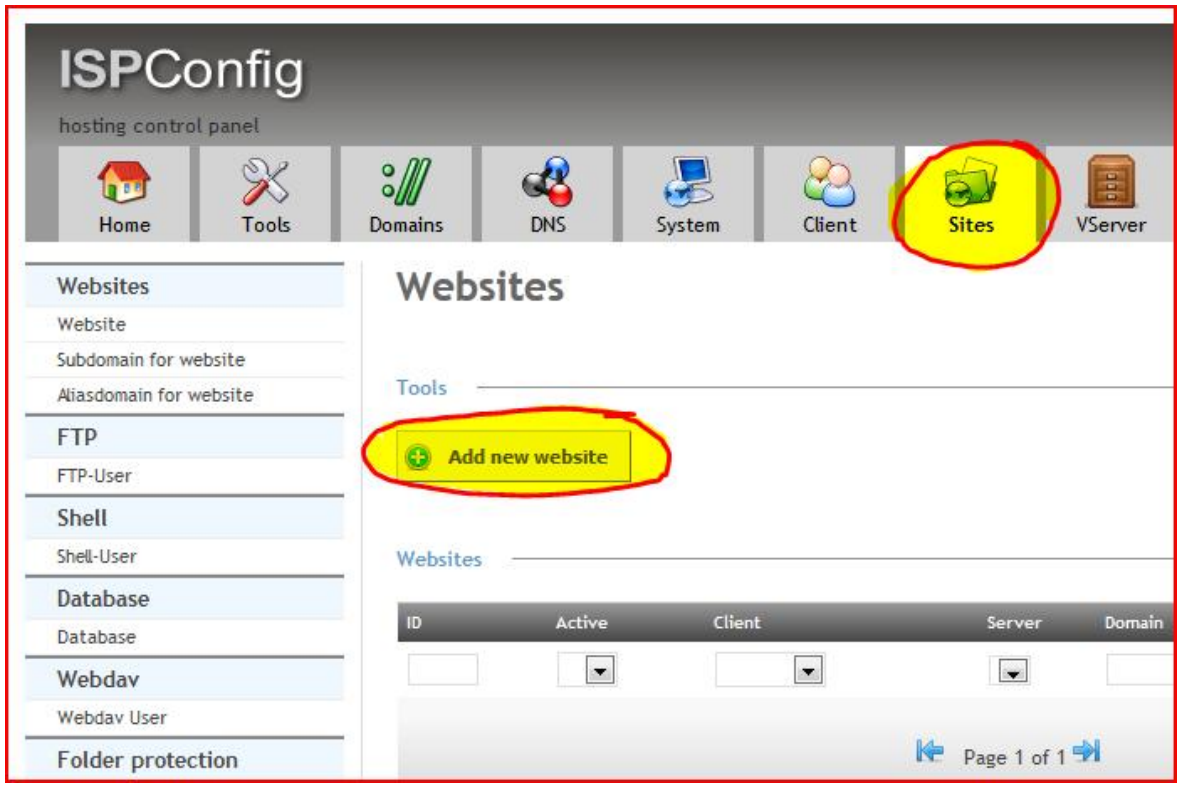
Σημείωση: Με την ολοκλήρωση των παραπάνω τροποποιήσεων, υπολείπεται μόνο η αυτόματη ενημέρωση όλων των εξυπηρετητών ονομάτων τομέα σχετικά με τη λειτουργία του διακομιστή ονομάτων στον εξυπηρετητή του οδηγού, ώστε να δρομολογούνται οι αιτήσεις που θα γίνονται παγκοσμίως και θα αφορούν υπηρεσίες χρήστη πελάτη του συστήματος, στη αντίστοιχη διεύθυνση δικτύου αυτού.

Προσθήκη ιστοτόπου

Εάν για το διαχειριστικό χρήστη – πελάτη απαιτείται η φιλοξενία ιστοτόπου, τότε θα πρέπει να πραγματοποιηθεί η αντίστοιχη προσθήκη μέσω του πίνακα ελέγχου. Έτσι, θα μπορεί να χρησιμοποιηθεί το όνομα τομέα του εξυπηρετητή (στο παράδειγμα το mydomain.gr) για την μέσω του εξυπηρετητή ονομάτων τομέα αντιστοίχιση με τη διεύθυνση του εξυπηρετητή και την απόκτηση πρόσβασης στις ιστοσελίδες, οι οποίες και

θα αναρτηθούν στο σχετικό φάκελο του εν λόγω χρήστη. Το ίδιο φυσικά ισχύει και για τους ιστοτόπους των υπόλοιπων χρηστών που θα εισαχθούν αργότερα στον εξυπηρετητή.

Οδηγία: Επιλέγουμε την καρτέλα των ιστοτόπων (Sites) και την εντολή προσθήκης νέου ιστοτόπου (Add new website):



Οδηγία: Στη νέα σελίδα επιλέγουμε από τη σχετική λίστα το χρήστη – πελάτη (Client) και στη συνέχεια τροποποιούμε τις υπόλοιπες ρυθμίσεις ανάλογα με την περίπτωση. Για το διαχειριστικό χρήστη – πελάτη λογικά δεν απαιτούνται περιορισμοί χρήσης του αποθηκευτικού χώρου του δίσκου (Harddisk Quota), ή του μηνιαίου όγκου διαμεταγωγής δεδομένων (Traffic Quota), όπως ίσως για τους υπόλοιπους, απλούς χρήστες. Οι σημαντικότερες από τις επιλογές που πρέπει να γίνουν για την προσθήκη του νέου ιστοτόπου αφορούν στα παρακάτω:

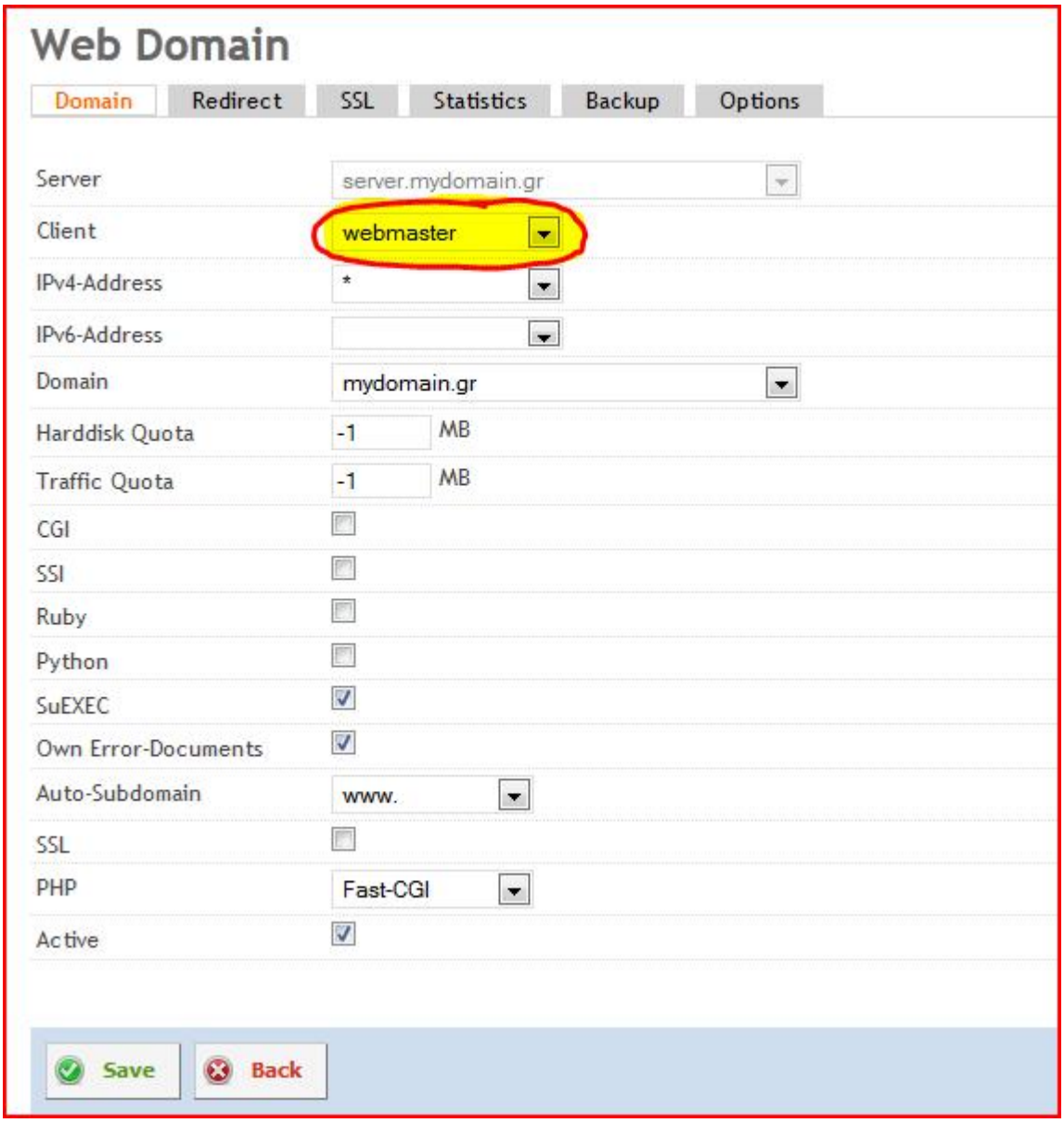
- CGI: Καθορίζει εάν θα επιτρέπεται ή εκτέλεση CGI script.
- SSI: Ενεργοποιεί το Server Side Includes (αρχεία τύπου *.shtml).
- SuEXEC: Καθορίζει εάν τα CGI script (καθώς και τα PHP script που εκτελούνται ως Fast-CGI ή CGI) θα εκτελούνται ως χρήστης / ομάδα χρηστών του τρέχοντος ιστοτόπου. Για λόγους ασφαλείας αυτή η επιλογή θα πρέπει να είναι πάντα ενεργοποιημένη.

- PHP: Ενεργοποιεί την PHP για το συγκεκριμένο ιστοτόπο. Οι επιλογές είναι Fast-CGI, CGI, Mod-PHP και SuPHP. Η κάθε μία έχει τα δικά της πλεονεκτήματα και μειονεκτήματα όπως παρακάτω:

Επιλογή	Πλεονεκτήματα	Μειονεκτήματα
Fast-CGI	ü Τα script θα εκτελούνται με τα δικαιώματα του χρήστη του ιστοτόπου. ü Μπορούν να χρησιμοποιηθούν περισσότερες από μία εκδόσεις PHP. ü Είναι ταχύτερη σε σύγκριση με τις επιλογές CGI και SuPHP.	ü Το αρχείο ρυθμίσεων php.ini δεν είναι δυνατό να τροποποιηθεί με PHP script, αρχεία vhost και .htaccess.
CGI	ü Τα script θα εκτελούνται με τα δικαιώματα του χρήστη του ιστοτόπου. ü Μπορούν να χρησιμοποιηθούν περισσότερες από μία εκδόσεις PHP.	ü Απαιτεί περισσότερη φυσική μνήμη RAM και για το λόγο αυτό δε συνιστάται σε «αργά» συστήματα. ü Το αρχείο ρυθμίσεων php.ini δεν είναι δυνατό να τροποποιηθεί με PHP script, αρχεία vhost και .htaccess.

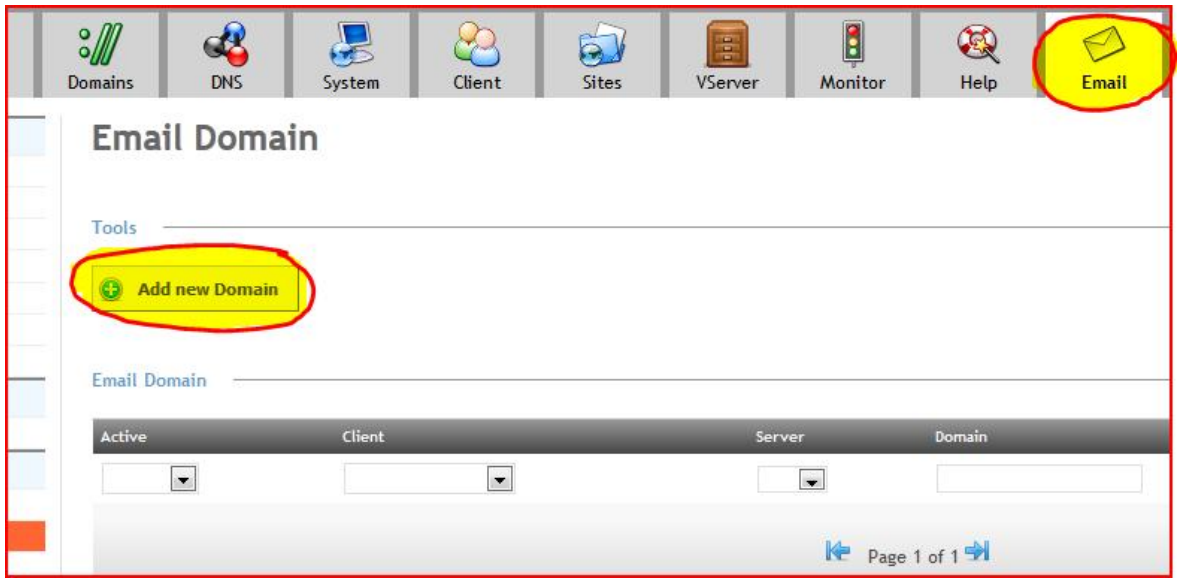
Mod-PHP	ü Είναι ταχύτατη. ü Απαιτεί λιγότερη φυσική μνήμη από την επιλογή CGI. ü Το αρχείο ρυθμίσεων php.ini είναι δυνατό να τροποποιηθεί με PHP script, αρχεία vhost και .htaccess.	ü Τα script εκτελούνται με δικαιώματα του εξυπηρετητή Apache (πιθανά προβλήματα ασφαλείας). ü Μόνο μία έκδοση της PHP μπορεί να εγκατασταθεί ως άρθρωμα του εξυπηρετητή Apache.
SuPHP	ü Τα script θα εκτελούνται με τα δικαιώματα του χρήστη του ιστοτόπου. ü Κάθε vhost μπορεί να έχει το δικό του php.ini αρχείο ρυθμίσεων. ü Απαιτεί λιγότερη φυσική μνήμη RAM σε σχέση με την επιλογή CGI. ü Μπορούν να χρησιμοποιηθούν περισσότερες από μία εκδόσεις PHP.	ü Το αρχείο ρυθμίσεων php.ini δεν είναι δυνατό να τροποποιηθεί με PHP script, αρχεία vhost και .htaccess. ü Η επιλογή SuPHP μπορεί να είναι λίγο πιο αργή σε σχέση με τη Mod-PHP

- ü Σε γενικές γραμμές συνιστώνται τα εξής:
- ü Για ιστοτόπους μεγάλης επισκεψιμότητας: Fast-CGI + suEXEC
- ü Για ιστοτόπους μικρής επισκεψιμότητας: CGI + suEXEC ή SuPHP

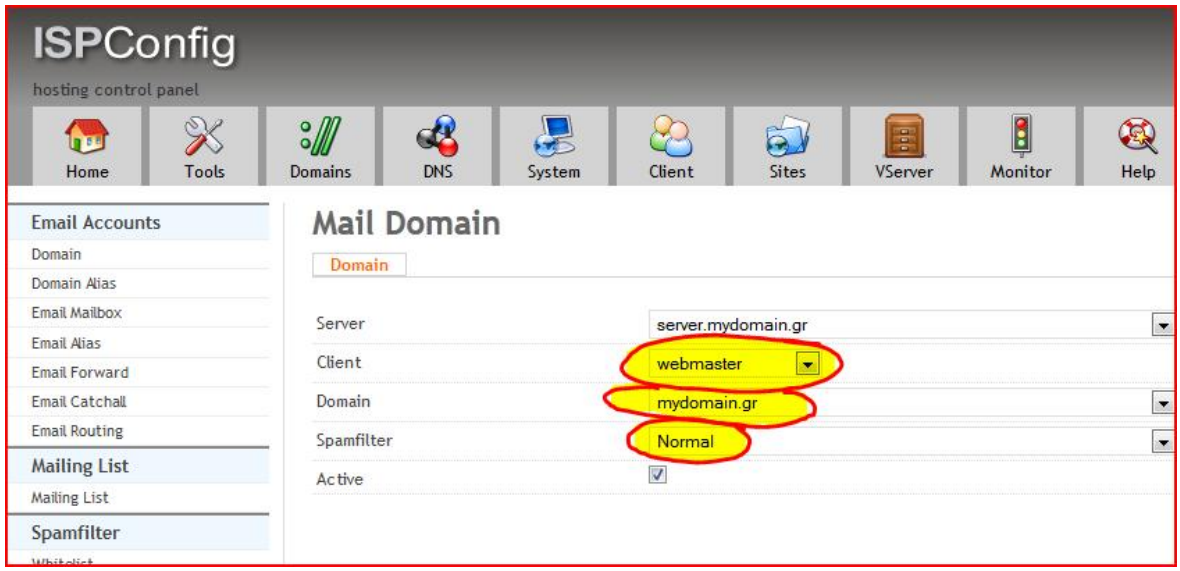

Web Domain
Domain
Redirect
SSL
Statistics
Backup
Options
Server
server.mydomain.gr
Client
webmaster
IPv4-Address
*
IPv6-Address
Domain
mydomain.gr
Harddisk Quota
-1
MB
Traffic Quota
-1
MB
CGI
SSI
Ruby
Python
SuEXEC
Own Error-Documents
Auto-Subdomain
www.
SSL
PHP
Fast-CGI
Active
Save
Back

Προσθήκη λογαριασμών ηλεκτρονικού ταχυδρομείου

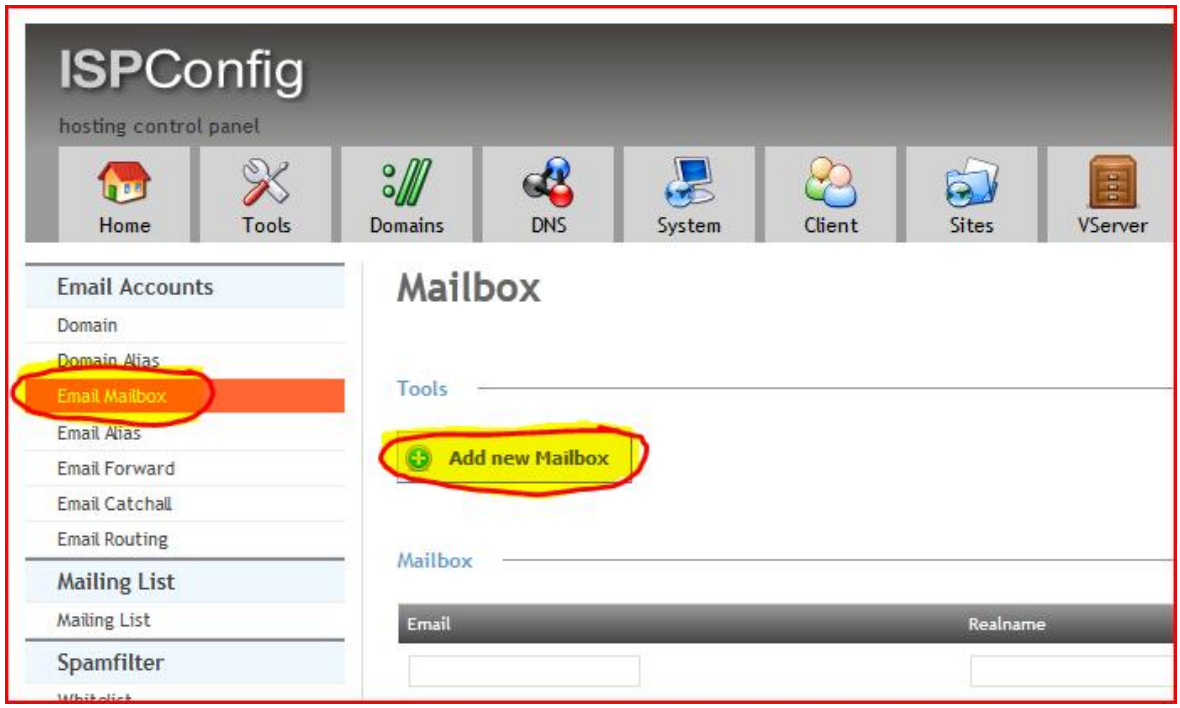
Οδηγία: Για να υπάρξει η δυνατότητα προσθήκης λογαριασμών ηλεκτρονικού ταχυδρομείου απαιτείται αρχικά η προσθήκη του ονόματος τομέα ηλεκτρονικού ταχυδρομείου αυτών. Επιλέγουμε για το λόγο αυτό την καρτέλα με τις ρυθμίσεις του ηλεκτρονικού ταχυδρομείου (Email) και στη συνέχεια την προσθήκη νέου ονόματος τομέα (Add new Domain):



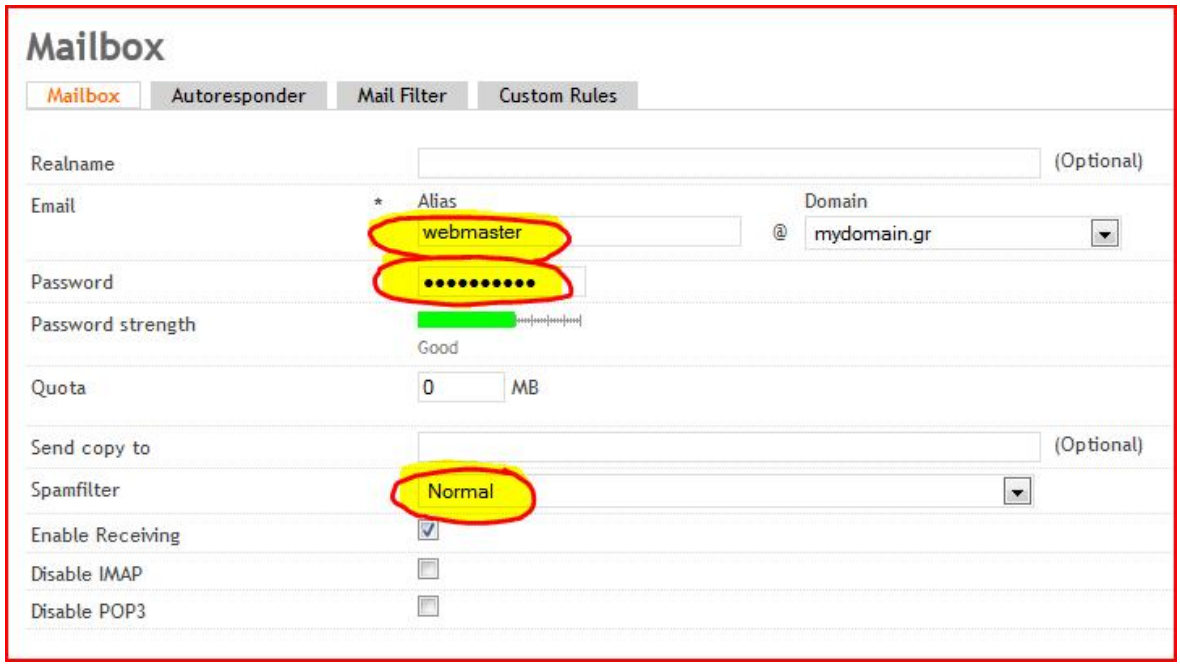
Οδηγία: Στη νέα σελίδα που εμφανίζεται επιλέγουμε από τις αντίστοιχες λίστες το χρήστη – πελάτη, το όνομα τομέα, καθώς και το αν θα χρησιμοποιηθεί το φίλτρο ανεπιθύμητης αλληλογραφίας (προτιμώμενη επιλογή το Normal) και στη συνέχεια αποθηκεύουμε τις ρυθμίσεις με χρήση της επιλογής αποθήκευσης (Save):



Οδηγία: Για την προσθήκη των λογαριασμών ηλεκτρονικού ταχυδρομείου χρησιμοποιούμε στην ίδια καρτέλα ρυθμίσεων την περιοχή επιλογών των κυτίων ηλεκτρονικής αλληλογραφίας (Email Mailbox) και στη συνέχεια την προσθήκη νέου κυτίου αλληλογραφίας (Add new Mailbox):



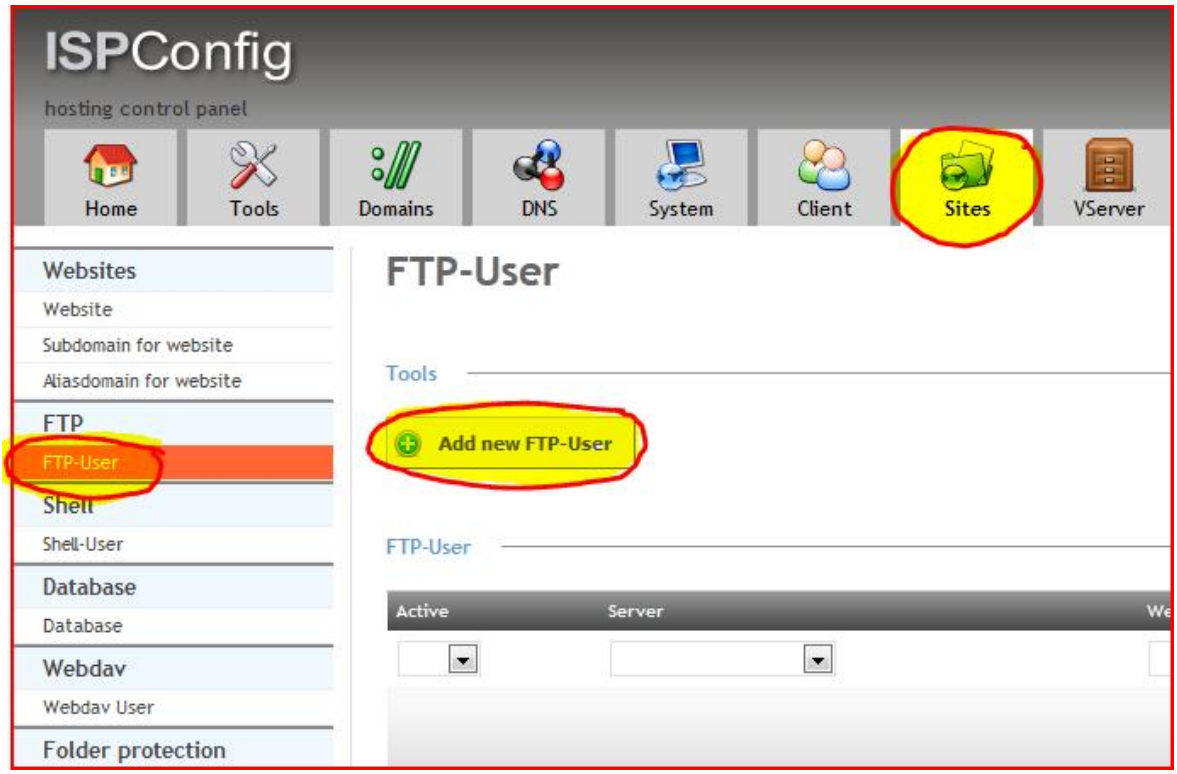
Οδηγία: Εισάγουμε τον επιθυμητό λογαριασμό ηλεκτρονικού ταχυδρομείου (Alias) για το συγκεκριμένο όνομα τομέα (Domain), καθώς και τον κωδικό πρόσβασης αυτού (Password). Επίσης, επιλέγουμε εάν για το συγκεκριμένο λογαριασμό θα είναι ενεργοποιημένο το φίλτρο ανεπιθύμητης αλληλογραφίας (προτιμώμενη επιλογή το Normal) και τέλος, αποθηκεύουμε τις αλλαγές με χρήση της αντίστοιχης επιλογής (Save):



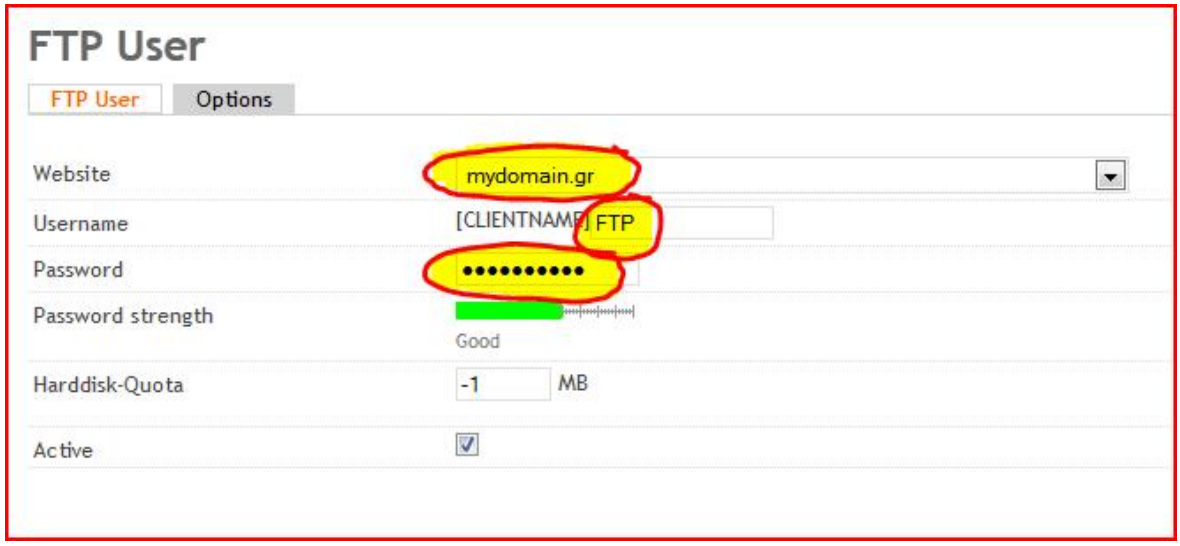
Σημείωση: Είναι αυτονόητο ότι η διαδικασία θα πρέπει να επαναληφθεί εάν απαιτούνται περισσότεροι από έναν λογαριασμοί ηλεκτρονικού ταχυδρομείου.

Προσθήκη λογαριασμού FTP

Οδηγία: Για την προσθήκη λογαριασμού χρήσης της υπηρεσίας FTP επιλέγουμε στην καρτέλα ρυθμίσεων των ιστοτόπων (Sites), την περιοχή επιλογών χρήστη FTP (FTP-User) και τέλος, την προσθήκη νέου χρήστη FTP (Add new FTP-User):



Οδηγία: Στη νέα σελίδα επιλέγουμε από τη σχετική λίστα τον ιστοτόπο και στη συνέχεια καθορίζουμε το επιθυμητό όνομα χρήστη, καθώς και τον κωδικό πρόσβασης για το νέο λογαριασμό FTP. Θα πρέπει να σημειωθεί ότι το όνομα χρήστη δεν είναι δυνατό να καθοριστεί συνολικά από το διαχειριστή, αλλά προκύπτει αυτόματα από το συνδυασμό του ονόματος του χρήστη – πελάτη και του αντίστοιχου πεδίου που εισάγεται στο τρέχων βήμα:



Με το παραπάνω βήμα ολοκληρώθηκε η διαδικασία προσθήκης λογαριασμού για χρησιμοποίηση της υπηρεσίας FTP και μαζί της και η συνολική διαδικασία εισαγωγής ενός νέου χρήστη – πελάτη στο σύστημα. Φυσικά, οι διαθέσιμες επιλογές που αφορούν στις υπηρεσίες του εκάστοτε χρήστη – πελάτη του εξυπηρετητή είναι περισσότερες από αυτές που παρατέθηκαν στα προηγούμενα βήματα. Η ανάλυση αυτών όμως ξεπερνά τα όρια του οδηγού της παρούσας εργασίας και έτσι, εάν αυτό είναι απαραίτητο, περαιτέρω πληροφορίες σχετικά μπορούν να αντληθούν από τον οδηγό χρήσης του ISPConfig, ο οποίος δημιουργήθηκε, συντηρείται και διατίθεται προς πώληση από την ομάδα ανάπτυξης του εν λόγω πίνακα ελέγχου.

Θωράκιση συστήματος (System hardening)

Όπως υποδεικνύεται και από το όνομά της, η θωράκιση του συστήματος αφορά σε ρυθμίσεις, οι οποίες λαμβάνουν χώρα αποσκοπώντας κατά κύριο λόγο στην αύξηση του επιπέδου της ασφάλειας του πληροφοριακού συστήματος ενδιαφέροντος. Η διαδικασία περιλαμβάνει την τροποποίηση συγκεκριμένων προκαθορισμένων παραμέτρων, οι οποίες συνήθως χρησιμοποιούνται από κακόβουλους χρήστες σε επιθέσεις που έχουν στόχο την

εξεύρεση αδυναμιών του συστήματος, καθώς και την εγκατάσταση λογισμικού προστασίας του συστήματος από τέτοιου είδους, κακόβουλες, αυτοματοποιημένες ως επί το πλείστον επιθέσεις.

Τροποποίηση ρυθμίσεων phpmyadmin

Το περιβάλλον διεπαφής της εφαρμογής διαχείρισης της υπηρεσίας MySQL του εξυπηρετητή είναι με τις εξ' ορισμού ρυθμίσεις του συστήματος διαθέσιμο στην προκαθορισμένη διεύθυνση http://www.mydomain.gr/phpmyadmin. Επιπλέον, με τις ίδιες ρυθμίσεις δεν έχει προβλεφθεί κανενός είδους κρυπτοποίηση στα μεταφερόμενα δεδομένα και έτσι, αυτά ίσως είναι προσβάσιμα και από τρίτους. Η υφιστάμενη κατάσταση είναι προφανές ότι υποβαθμίζει το επίπεδο της ασφάλειας του εξυπηρετητή και για το λόγο αυτό, θα πρέπει να πραγματοποιηθούν οι απαιτούμενες διορθωτικές ενέργειες πριν από την επιχειρησιακή χρήση αυτού. Οι εν λόγω ενέργειες αφορούν στην τροποποίηση της προκαθορισμένης διεύθυνσης του περιβάλλοντος διεπαφής της MySQL, ώστε αυτό να μην είναι διαθέσιμο σε αυτοματοποιημένες επιθέσεις, αλλά και των ρυθμίσεων που απαιτούνται, ώστε η εφαρμογή phpmyadmin να είναι προσβάσιμη μέσω ασφαλούς σύνδεσης SSL.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων phpmyadmin:

```
vi /etc/apache2/conf.d/phpmyadmin.conf
```

Οδηγία: Στην τρίτη γραμμή του αρχείου αντικαθιστούμε το προκαθορισμένο alias με το αντίστοιχο επιθυμητό (πχ mysqladmin):

```
[...]
Alias /mysqladmin /usr/share/phpmyadmin
[...]
```

Οδηγία: Στο τέλος του ίδιου αρχείου ρυθμίσεων προσθέτουμε τις παρακάτω γραμμές, μεριμνώντας ώστε να αντικαταστήσουμε την πόρτα σύνδεσης με αυτή που έχει χρησιμοποιηθεί για το περιβάλλον διεπαφής του πίνακα ελέγχου ISPConfig (στο παράδειγμα του οδηγού η πόρτα 33333):

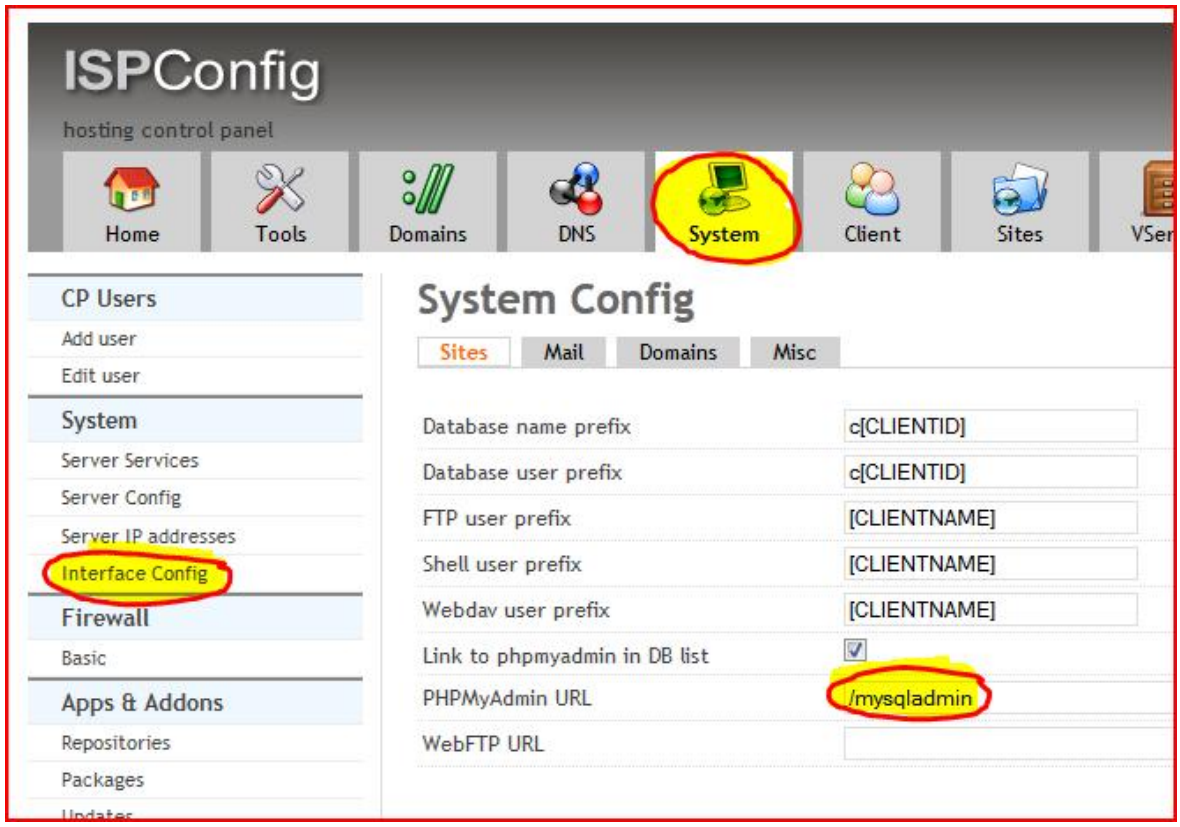
```
[...]
<IfModule mod_rewrite.c>
  <IfModule mod_ssl.c>
    <Location /webtropiadb>
      RewriteEngine on
      RewriteCond %{HTTPS} !^on$ [NC]
      RewriteRule . https://%{HTTP_HOST}:33333%{REQUEST_URI}  [L]
    </Location>
  </IfModule>
</IfModule>
```

Οδηγία: Για να ισχύσουν άμεσα οι παραπάνω αλλαγές, επανεκκινούμε τον Apache:

```
/etc/init.d/apache2 restart
```

Πλέον, σε κάθε προσπάθεια σύνδεσης με την επιφάνεια διεπαφής της phpmyadmin στην παλιά διεύθυνση (http://www.mydomain.gr/phpmyadmin) ο εξυπηρετητής θα αποκρίνεται με το μήνυμα «Not Found! The requested URL /phpmyadmin/ was not found on this server». Έτσι, στο εξής θα πρέπει να χρησιμοποιείται το νέο alias, καθώς και η νέα διεύθυνση ασφαλούς σύνδεσης πάνω από την επιλεγμένη πόρτα (πχ 33333), με τη μορφή http://www.mydomain.gr:33333/mysqladmin.

Οδηγία: Θα πρέπει για την τροποποίηση που πραγματοποιήθηκε στο παραπάνω βήμα να ενημερωθεί και ο πίνακας ελέγχου ISPConfig. Επιλέγουμε, λοιπόν, με τη συγκεκριμένη σειρά, την καρτέλα με τις ρυθμίσεις του συστήματος (System), την περιοχή επιλογών των ρυθμίσεων του περιβάλλοντος διεπαφής (Interface Config) και τέλος την καρτέλα με τις ρυθμίσεις των ιστοτόπων (Sites). Στη συγκεκριμένη καρτέλα, τροποποιούμε κατάλληλα την παράμετρο της διεύθυνσης διεπαφής της εφαρμογής phpmyadmin (PHPMyAdmin URL) και τέλος, αποθηκεύουμε τις ρυθμίσεις με χρήση της αντίστοιχης επιλογής (Save):



Εγκατάσταση Dos Evasive

Από τις πιο γνωστές επιθέσεις που εξαπολύονται σε εξυπηρετητές διαδικτύου είναι οι επιθέσεις άρνησης παροχής υπηρεσιών (DoS attacks) [91]. Επιθέσεις άρνησης εξυπηρέτησης ονομάζονται οι επιθέσεις που έχουν σκοπό να καταστήσουν ένα πληροφοριακό σύστημα μη ικανό να δεχθεί επιπλέον συνδέσεις, ώστε να εξυπηρετήσει νέους πιθανούς πελάτες.

Για την προστασία του εξυπηρετητή από τις συγκεκριμένες επιθέσεις θα εγκατασταθεί η εφαρμογή dos evasive. Η εν λόγω εφαρμογή έχει σχεδιαστεί και αναπτυχθεί με στόχο το να αναγνωρίζει και να εντοπίζει αυτού του είδους τις επιθέσεις και για να προστατέψει το πληροφοριακό σύστημα στο οποίο έχει εγκατασταθεί, να απαγορεύει την επανάληψη των κακόβουλων αιτήσεων σύνδεσης, ενημερώνοντας παράλληλα το διαχειριστή του συστήματος, είτε μέσω μηνύματος ηλεκτρονικού ταχυδρομείου, είτε μέσω των αρχείων καταγραφής.

Οδηγία: Εγκαθιστούμε το άρθρωμα της εφαρμογής dos evasive με την παρακάτω εντολή:

```
apt-get install libapache2-mod-evasive
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων httpd:

```
vi /etc/apache2/httpd.conf
```

Οδηγία: Προσθέτουμε τις παρακάτω γραμμές και αποθηκεύουμε το αρχείο:

```
<IfModule  mod_evasive20.c>
   DOSHashTableSize 3097
   DOSPageCount 2
   DOSSiteCount 50
   DOSPageInterval 1
   DOSSiteInterval 1
   DOSBlockingPeriod 10
   DOSLogDir "/var/lock/mod_evasive"
</IfModule>
```

Οδηγία: Για να ισχύσουν άμεσα οι παραπάνω αλλαγές, επανεκκινούμε τον Apache:

```
/etc/init.d/apache2 force-reload
```

Για να δούμε στην πράξη τα αποτελέσματα της εφαρμογής ανοίγουμε ένα δεύτερο τερματικό, συνδεόμαστε στον εξυπηρετητή και εκτελούμε την παρακάτω εντολή:

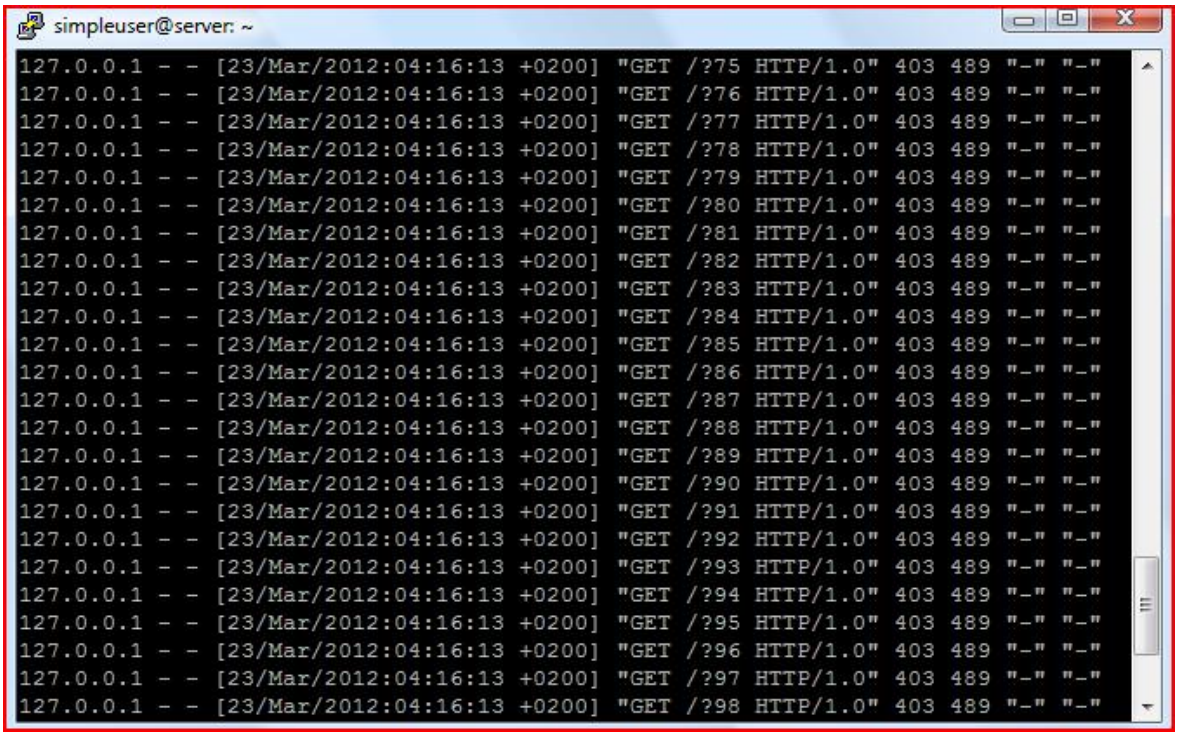
```
tail -f /var/log/apache2/access.log
```

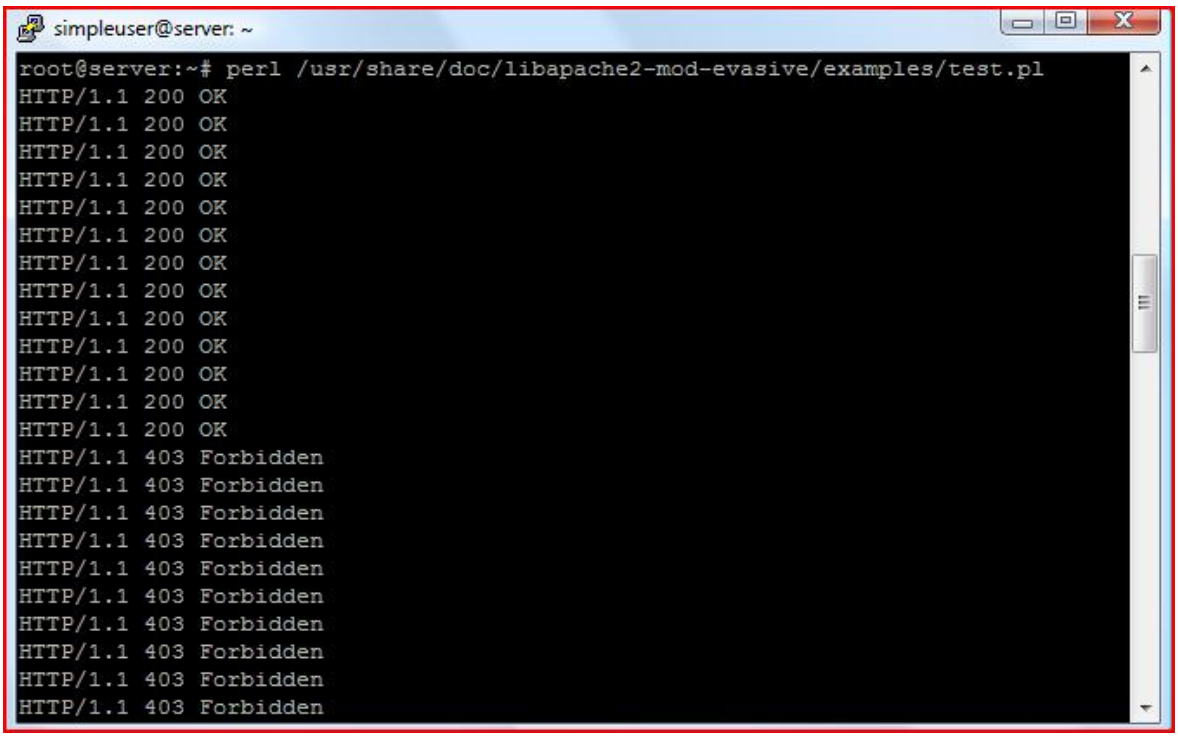
Στο παράθυρο του πρώτου τερματικού εκτελούμε το παρακάτω script επίθεσης:

```
perl /usr/share/doc/libapache2-mod-evasive/examples/test.pl
```

Μετά την εκτέλεση της επίθεσης μπορούμε στο δεύτερο τερματικό να δούμε όλες τις αιτήσεις του script, οι οποίες θα είναι της μορφής «127.0.0.1 - - [23/Mar/2012:04:16:13 +0200] "GET /?100 HTTP/1.0" 403 489 "-" "-"» και την ίδια ακριβώς στιγμή στο πρώτο τερματικό μερικές γραμμές με το μήνυμα «*HTTP/1.1 200 OK*» και ακολούθως πολύ περισσότερες με το μήνυμα «*HTTP/1.1 403 Forbidden*». Αυτό σημαίνει ότι η εφαρμογή

dos evasive λειτουργεί όπως αναμένεται, επιτρέποντας τη σύνδεση του script επίθεσης στο σύστημα, για ορισμένες μόνο φορές και απαγορεύοντάς τη στη συνέχεια.





Εγκατάσταση (D)DoS Deflate

Η εφαρμογή (D)DoS Deflate είναι ίδιας γενικής φιλοσοφίας με την εφαρμογή dos evasive που εγκαταστάθηκε στο προηγούμενο βήμα, όμως έχει τη δυνατότητα να

προστατεύει το σύστημα από κατανεμημένες επιθέσεις άρνησης υπηρεσιών (DDoS). Οι συγκεκριμένες επιθέσεις διαφοροποιούνται από τις απλές επιθέσεις άρνησης υπηρεσιών στο ότι οι κακόβουλες αιτήσεις σύνδεσης πραγματοποιούνται ταυτόχρονα από πολλά πληροφοριακά συστήματα και όχι μόνο από ένα. Τα συστήματα αυτά είναι συνήθως κατανεμημένα ανά την υφήλιο και αποτελούν ένα κακόβουλο σύνολο που καλείται botnet.

Οδηγία: Για να εγκαταστήσουμε την εφαρμογή (D)DoS Deflate, εκτελούμε με τη συγκεκριμένη σειρά τις παρακάτω εντολές:

```
cd /tmp
wget http://www.inetbase.com/scripts/ddos/install.sh
chmod 0700 install.sh
./install.sh
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων ddos.conf της εφαρμογής:

```
vi /usr/local/ddos/ddos.conf
```

Οδηγία: Στη γραμμή 19 του αρχείου αλλάζουμε την παράμετρο APF_BAN από 1 σε 0, ώστε να χρησιμοποιούνται από την εφαρμογή οι πίνακες IP διευθύνσεων αντί του τείχους προστασίας APF:

```
[...]
APF_BAN=0
[...]
```

Οι τροποποιήσεις θα ισχύσουν στην επόμενη εκτέλεση της εφαρμογής (ανά ένα λεπτό σύμφωνα με την εξ' ορισμού ρύθμιση), μέσω της cronjob που δημιουργήθηκε αυτόματα κατά την εγκατάσταση της (D)DoS Deflate.

Ενεργοποίηση τείχους προστασίας

Το τείχος προστασίας (firewall) [92] χρησιμοποιείται ευρέως στα δίκτυα πληροφοριακών συστημάτων και έχει ως κύριο στόχο την πρόληψη απομακρυσμένων επιθέσεων στο εκάστοτε τοπικό δίκτυο. Είναι κατά βάση ένα εργαλείο, με το οποίο μπορούν να επιτρέπονται ή να απορρίπτονται τα πακέτα δεδομένων που κινούνται από ένα

δίκτυο με διαφορετικό επίπεδο εμπιστοσύνης, σε κάποιο άλλο. Είναι διαθέσιμο με τη μορφή αυτόνομης συσκευής, καθώς και «απλής» εφαρμογής που εκτελείται σε κάποιο πληροφοριακό σύστημα. Για βέλτιστη απόδοση συνήθως ρυθμίζεται με την πολιτική default deny, σύμφωνα με την οποία απορρίπτονται όλες οι συνδέσεις, εκτός αυτών που επιλεκτικά έχουν καθοριστεί να επιτρέπονται από το διαχειριστή του συστήματος.

Είναι προφανές ότι για να εφαρμοστεί σωστά η συγκεκριμένη πολιτική, θα πρέπει ο διαχειριστής του εξυπηρετητή να έχει μία σαφή και ολοκληρωμένη εικόνα για τις επικοινωνιακές ανάγκες του συστήματος. Για να καθοριστούν οι συγκεκριμένες απαιτήσεις στον παρών οδηγό, θα γίνει εγκατάσταση και χρήση της εφαρμογής Network Mapper (nMap) [93]. Η εφαρμογή nMap εκμεταλλεύεται με πρωτοποριακό τρόπο τη δομή των πακέτων IP και είναι σε θέση να καθορίσει όλες τις λεπτομέρειες σχετικά με τις υπηρεσίες που παρέχονται από κάποιο πληροφοριακό σύστημα. Έτσι, αφού εγκατασταθεί στον εξυπηρετητή, η συγκεκριμένη εφαρμογή θα εκτελεστεί με τις κατάλληλες παραμέτρους, ώστε να παράγει τη λίστα με τις πόρτες δικτύου που θα πρέπει να παραμείνουν ανοιχτές μετά την ενεργοποίηση του τείχους προστασίας.

Οδηγία: Εκτελούμε με τη συγκεκριμένη σειρά, τις παρακάτω εντολές:

```
apt-get install build-essential
cd /tmp
wget http://nmap.org/dist/nmap-5.51.tar.bz2
bzip2 -cd nmap-5.51.tar.bz2 | tar xvf -
cd ./nmap-5.51
./configure
make
make install
nmap --version
```

Οδηγία: Εκτελούμε τις εντολές δημιουργίας των αρχείων nmapTCPservices και nmapUDPservices, τα οποία θα περιέχουν όλες τις πόρτες που χρησιμοποιούνται από υπηρεσίες του συστήματος:

```
nmap -sSV 127.0.0.1 -p1-65535 > nmapTCPservices
nmap -sUV 127.0.0.1 -p1-65535 > nmapUDPservices
```

Οδηγία: Με τις παρακάτω εντολές μπορούμε να δούμε τα περιεχόμενα των δύο αρχείων που δημιουργήθηκαν στο αμέσως προηγούμενο βήμα:

```
cat nmapTCPservices
cat nmapUDPservices
```

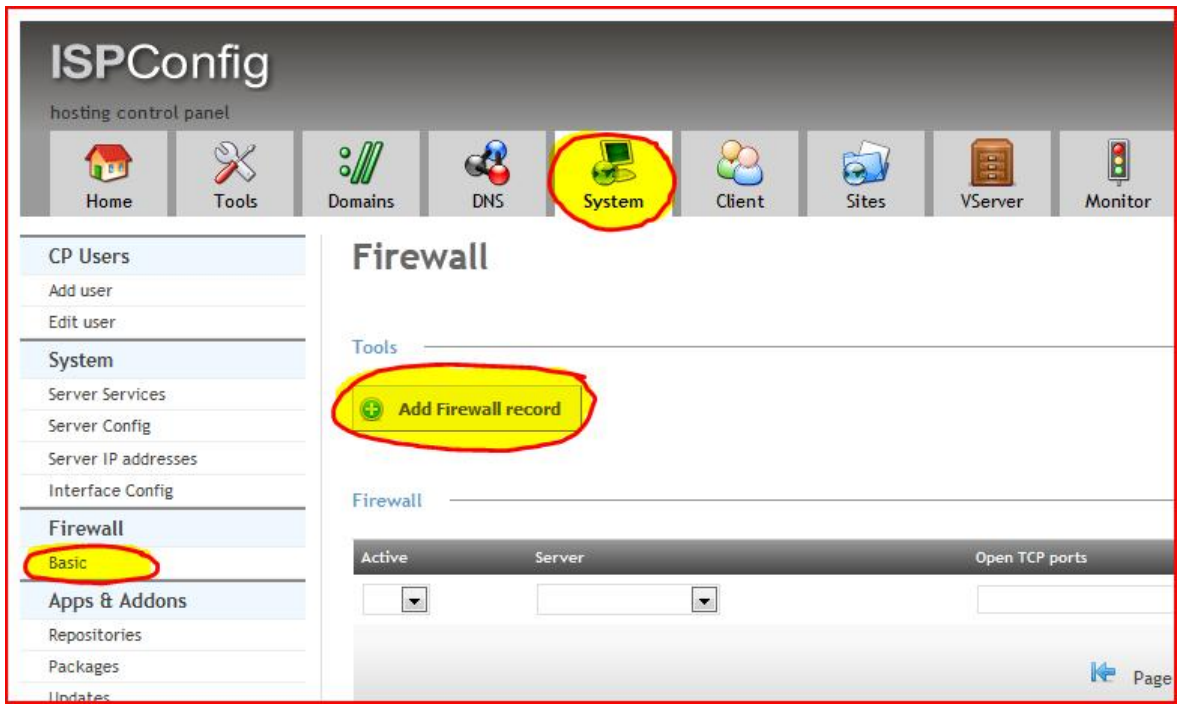
Οδηγία: Τα περιεχόμενα των δύο αυτών αρχείων θα πρέπει να είναι παρόμοια με τα παρακάτω:

```
Starting Nmap 5.51 ( http://nmap.org ) at 2012-03-23 10:32 EET
Nmap scan report for localhost.localdomain (127.0.0.1)
Host is up (0.033s latency).
Not shown: 65516 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Pure-FTPd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.7.3
80/tcp    open  http         Apache httpd 2.2.16 ((Debian))
110/tcp   open  pop3         Courier pop3d
111/tcp   open  rpcbind      2 (rpc #100000)
143/tcp   open  imap         Courier Imapd (released 2010)
443/tcp   open  http         Apache httpd 2.2.16 ((Debian))
783/tcp   open  spamassassin SpamAssassin spamd
953/tcp   open  rndc?
993/tcp   open  ssl          OpenSSL (SSLv3)
995/tcp   open  ssl          OpenSSL (SSLv3)
3306/tcp  open  mysql        MySQL 5.1.61-0+squeeze1
8081/tcp  open  http         Apache httpd 2.2.16 ((Debian))
10024/tcp open  smtp         amavisd smtpd
10025/tcp open  smtp         Postfix smtpd
22222/tcp open  ssh          OpenSSH 5.5p1 Debian 6+squeeze1 (protocol
2.0)
33333/tcp open  http         Apache httpd (SSL-only mode)
36989/tcp open  status       1 (rpc #100024)
Service Info: Hosts:  server.mydomain.gr, 127.0.0.1; OS: Linux

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.98 seconds
```

```
  Starting Nmap 5.51 ( http://nmap.org ) at 2012-03-23 10:40 EET
  Nmap scan report for localhost.localdomain (127.0.0.1)
  Host is up (0.000095s latency).
  Not shown: 65530 closed ports
  PORT      STATE         SERVICE VERSION
  53/udp    open          domain  ISC BIND 9.7.3
  68/udp    open|filtered dhcpc
  111/udp   open          rpcbind 2 (rpc #100000)
  1023/udp  open|filtered unknown
  53449/udp open          status  1 (rpc #100024)

  Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
  Nmap done: 1 IP address (1 host up) scanned in 81.86 seconds
```

Έχοντας πλέον σαφή εικόνα για τις υπηρεσίες που παρέχονται από τον εξυπηρετητή, καθώς και τις πόρτες σύνδεσης σε αυτές, είμαστε σε θέση να ενεργοποιήσουμε το τείχος προστασίας μέσω του πίνακα ελέγχου ISPConfig.

Οδηγία: Επισκεπτόμαστε την καρτέλα ρυθμίσεων του συστήματος (System), την περιοχή βασικών ρυθμίσεων του τείχους προστασίας (Firewall - Basic) και επιλέγουμε να προσθέσουμε νέα εγγραφή τείχους προστασίας (Add Firewall record):



Για τη ρύθμιση του τείχους προστασίας του συστήματος, ο πίνακας ελέγχου ISPConfig χρησιμοποιεί το script bastille-firewall [94], το οποίο με τη σειρά του χρησιμοποιεί πίνακες IP διευθύνσεων (iptables) [95]. Αυτό που απομένει να λάβει χώρα, για να ολοκληρωθεί η αυτοματοποιημένη διαδικασία, είναι το να εισαχθούν στα πεδία πορτών τύπου TCP και UDP οι αντίστοιχες πόρτες που θα πρέπει να παραμείνουν ανοιχτές μετά την ενεργοποίηση του τείχους προστασίας.

Οδηγία: Εισάγουμε στα αντίστοιχα πεδία, τις TCP και UDP πόρτες που είναι απαραίτητο να παραμείνουν ανοιχτές μετά την ενεργοποίηση του τείχους προστασίας και αποθηκεύουμε την εγγραφή με χρήση της αντίστοιχης επιλογής (Save):

Στην περίπτωση που κατά τη διενέργεια των ρυθμίσεων της εφαρμογής pure-ftpd έχουμε ενεργοποιήσει τη δυνατότητα για FTP συνεδρίες πάνω από ασφαλείς συνδέσεις, θα πρέπει να πραγματοποιήσουμε και ορισμένα επιπλέον βήματα, ώστε να λειτουργεί σωστά η συγκεκριμένη υπηρεσία μετά την ενεργοποίηση του τείχους προστασίας.

Οδηγία: Εκτελούμε την παρακάτω εντολή:

```
grep -i ftps /etc/services
```

Οδηγία: Στο αποτέλεσμα της συγκεκριμένης εντολής θα περιέχονται οι αριθμοί δύο πορτών όπως παρακάτω:

```
ftps-data       989/tcp                         # FTP over SSL (data)
ftps            990/tcp
```

Η πρώτη από τις δύο πόρτες χρησιμοποιείται από την υπηρεσία FTP για τα δεδομένα των ασφαλών συνδέσεων και είναι αυτή που θα πρέπει να συμπεριληφθεί ανάμεσα στις

ανοιχτές πόρτες του τείχους προστασίας, ώστε να πραγματοποιούνται χωρίς προβλήματα ασφαλείς συνδέσεις για χρήση της υπηρεσίας FTP.

Σε μεμονωμένες περιπτώσεις έχουν αναφερθεί προβλήματα συνδεσιμότητας ακόμη και μετά την παραπάνω ενέργεια και τότε καθίσταται απαραίτητη η χρήση παθητικών συνδέσεων FTP. Για να ενεργοποιηθούν αυτού του τύπου οι συνδέσεις θα πρέπει αφενός να καθοριστεί ένα εύρος παθητικών πορτών στην υπηρεσία FTP (pure-ftpd), αφετέρου αυτές να συμπεριληφθούν στη λίστα με τις ανοιχτές πόρτες, ώστε να παραμείνουν ανοιχτές μετά την ενεργοποίηση του τείχους προστασίας.

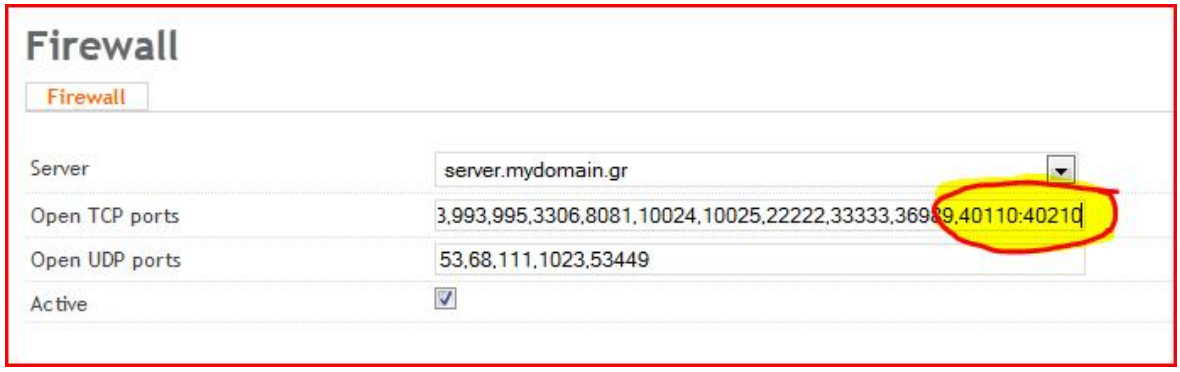
Οδηγία: Συμπεριλαμβάνουμε τις επιλεγμένες πόρτες (για το παράδειγμα του οδηγού έχουν επιλεγεί οι πόρτες με αριθμό από 40110 έως 40210) στις παθητικές πόρτες σύνδεσης της υπηρεσίας FTP:

```
echo "40110 40210" > /etc/pure-ftpd/conf/PassivePortRange
```

Οδηγία: Επανεκκινούμε την υπηρεσία FTP:

```
/etc/init.d/pure-ftpd-mysql restart
```

Οδηγία: Προσθέτουμε το εύρος πορτών για τις παθητικές πόρτες σύνδεσης της υπηρεσίας FTP στις ανοιχτές TCP πόρτες του πίνακα ελέγχου ISPConfig και αποθηκεύουμε τις νέες ρυθμίσεις με χρήση της αντίστοιχης επιλογής (Save):



Τροποποίηση εγγραφής PTR

Στη διαδικασία δημιουργίας της ζώνης ονομάτων τομέα (εισαγωγή διαχειριστικού χρήστη ISPConfig) έγινε ήδη αναφορά στους πίνακες αντιστοίχισης του ονόματος τομέα

με τη διεύθυνση δικτύου του εκάστοτε συστήματος. Στα βήματα που έλαβαν χώρα στη συγκεκριμένη διαδικασία πραγματοποιήθηκαν όλες οι απαραίτητες σχετικές εγγραφές, ώστε να διασφαλίζεται η σωστή λειτουργία του εξυπηρετητή. Στο τρέχων βήμα του οδηγού είναι απαραίτητο να τροποποιηθεί μία ακόμα εγγραφή DNS, η οποία αφορά σε αντεστραμμένη αναζήτηση και έχει σκοπό να συνεισφέρει στην αντιμετώπιση της ανεπιθύμητης αλληλογραφίας. Η εν λόγω εγγραφή καλείται PTR Record [96] και στο μεγαλύτερο ποσοστό των περιπτώσεων τροποποιείται αποκλειστικά από τον πάροχο της δυνατότητας πρόσβασης του εμπλεκόμενου πληροφοριακού συστήματος στο διαδίκτυο.

Στις προδιαγραφές RFC1033, καθώς και RFC1912 προβλέπεται ότι κάθε σύστημα που είναι προσβάσιμο μέσω του διαδικτύου θα πρέπει να έχει ένα όνομα, το οποίο και θα πρέπει να αντιστοιχεί στο όνομα που προκύπτει μετά από αντεστραμμένη αναζήτηση του συστήματος με χρήση της εγγραφής PTR. Έτσι, θα πρέπει να ζητηθεί από το προσωπικό του κέντρου δεδομένων, στο οποίο βρίσκεται εγκατεστημένος ο εξυπηρετητής, η τροποποίηση της συγκεκριμένης εγγραφής, ώστε η διεύθυνση δικτύου του συστήματος να αντιστοιχεί στο πλήρες κανονικοποιημένο όνομα αυτού. Βέβαια, επειδή η αντεστραμμένη αναζήτηση θα γίνει από άλλα πληροφοριακά συστήματα με σκοπό την επιβεβαίωση του ονόματος του συστήματος εξυπηρέτησης ηλεκτρονικής αλληλογραφίας που έχει αποστείλει κάποιο μήνυμα προς τους χρήστες τους, είναι βέλτιστο το να χρησιμοποιηθεί το κανονικοποιημένο όνομα της υπηρεσίας ηλεκτρονικής αλληλογραφίας (πχ mail.mydomain.gr). Σε κάθε περίπτωση το συγκεκριμένο όνομα θα πρέπει να είναι ίδιο με το όνομα που χρησιμοποιήθηκε στην παράμετρο mx της εγγραφής SPF κατά τη δημιουργία της ζώνης ονομάτων τομέα του διαχειριστικού χρήστη. Επιπλέον, θα πρέπει να τροποποιηθεί σχετικά και το αρχείο ρυθμίσεων main.cf της υπηρεσίας postfix, ώστε και η παράμετρος myhostname να γίνει ταυτόσημη με το εν λόγω όνομα.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων main.cf της υπηρεσίας postfix:

```
vi /etc/postfix/main.cf
```

Οδηγία: Στη γραμμή 30 τροποποιούμε την τιμή της παραμέτρου myhostname, αλλάζοντάς την από server.mydomain.gr στο όνομα που χρησιμοποιήθηκε στην εγγραφή PTR (πχ mail.mydomain.gr):

```
[...]
myhostname = mail.mydomain.gr
[...]
```

Οδηγία: Επανεκκινούμε την υπηρεσία postfix, ώστε να ισχύσουν άμεσα οι αλλαγές:

```
/etc/init.d/postfix restart
```

Σημείωση: Μετά την πάροδο του χρονικού διαστήματος που απαιτείται ώστε να ενημερωθούν όλοι οι εξυπηρετητές ονομάτων τομέα ανά την υφήλιο, μπορούμε να ελέγξουμε την επιτυχημένη τροποποίηση της εγγραφής PTR, εκτελώντας την ακόλουθη εντολή (θα πρέπει φυσικά να αντικατασταθεί η διεύθυνση δικτύου με αυτή του πραγματικού πληροφοριακού συστήματος στο οποίο εφαρμόζεται ο οδηγός):

```
host 192.168.204.134
```

Τροποποίηση ρυθμίσεων BIND

Σε στόχο την αύξηση του υφιστάμενου επιπέδου ασφαλείας του εξυπηρετητή θα πρέπει να πραγματοποιηθούν οι κατάλληλες ρυθμίσεις, ώστε ο διακομιστής ονομάτων να μην κοινοποιεί την έκδοση του εγκατεστημένου λογισμικού στα σχετικά ερωτήματα που μπορεί να του γίνονται. Η απαραίτητη τροποποίηση είναι σχετικά απλή και αφορά στην προσθήκη μιας παραμέτρου με την επιθυμητή τιμή αυτής στο αρχείο ρυθμίσεων της υπηρεσίας BIND (ή named).

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων named.conf.options της υπηρεσίας BIND:

```
vi /etc/bind/named.conf.options
```

Οδηγία: Στο τέλος του αρχείου προσθέτουμε την παρακάτω γραμμή:

```
[...]
version "unknown";
```

Οδηγία: Επανεκκινούμε την υπηρεσία BIND, ώστε να ισχύσουν άμεσα οι αλλαγές:

```
/etc/init.d/bind9 restart
```

Τροποποίηση ρυθμίσεων sysctl

Η εφαρμογή sysctl έχει αναπτυχθεί για τον έλεγχο και τη ρύθμιση παραμέτρων του πυρήνα σε συστήματα BSD και Linux. Στο αρχείο ρυθμίσεων της συγκεκριμένης εφαρμογής θα πρέπει να γίνουν οι κατάλληλες τροποποιήσεις, ώστε:

- να προστατευθεί το σύστημα απέναντι σε επιθέσεις τύπου Syn flooding
- να μην επιτρέπονται αποστολές πακέτων με μη έγκυρες διευθύνσεις δικτύου
- να μην επιτρέπεται ο εντοπισμός της πηγής εισερχομένων αρχείων
- να μη γίνονται αποδεκτά πακέτα ανακατεύθυνσης ICMP
- να γίνεται καταγραφή ύποπτων πακέτων (martian)

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων sysctl.conf:

```
vi /etc/sysctl.conf
```

Οδηγία: Αποσχολιάζουμε τις γραμμές 19, 20, 25, 44, 45, 52, 55, 56 και 59 διαγράφοντας τον πρώτο χαρακτήρα (#):

```
[...]
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1
[...]
net.ipv4.tcp_syncookies=1
[...]
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
[...]
net.ipv4.conf.all.send_redirects = 0
[...]
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
[...]
net.ipv4.conf.all.log_martians = 1
[...]
```

Οδηγία: Εκτελούμε την παρακάτω εντολή ώστε να ισχύσουν άμεσα οι αλλαγές:

```
sysctl -p
```

Φιλτράρισμα ανεπιθύμητης αλληλογραφίας

Μέρος της διαδικασίας αύξησης του επιπέδου θωράκισης του εξυπηρετητή απέναντι σε πιθανή κακόβουλη χρήση αυτού είναι και η τροποποίηση των αυτοματοποιημένων ελέγχων που γίνονται από την υπηρεσία ηλεκτρονικού ταχυδρομείου, ώστε να απορρίπτεται η εισερχόμενη ανεπιθύμητη αλληλογραφία, μάλιστα πριν ακόμα αυτή εισέλθει στο σύστημα. Με επιτυχημένη εφαρμογή μιας τέτοιας πολιτικής, οι πόροι του εξυπηρετητή δε θα αναλώνονται σε περαιτέρω ελέγχους και έτσι, αυτό θα είναι ανθεκτικό απέναντι σε επίδοξους spammers, καθώς και spam botnets. Η τεχνική πίσω από τον αυτοματοποιημένο έλεγχο της αλληλογραφίας περιλαμβάνει επιμέρους ελέγχους, που πραγματοποιούνται σε τρία στάδια, με τους λιγότερο απαιτητικούς να γίνονται πριν από αυτούς που απαιτούν μεγαλύτερο ποσοστό των πόρων του συστήματος.

Στο πρώτο στάδιο φιλτραρίσματος της εισερχόμενης αλληλογραφίας γίνεται έλεγχος γνησιότητας του πληροφοριακού συστήματος που αποστέλλει το υπό εξέταση μήνυμα ηλεκτρονικής αλληλογραφίας. Στο πρωτόκολλο Simple Mail Transfer Protocol [97] καθορίζεται ότι κάθε φορά που μια εφαρμογή – πελάτης συνδέεται με την αντίστοιχη εφαρμογή – εξυπηρετητή στο διακομιστή ηλεκτρονικής αλληλογραφίας, αυτή θα πρέπει να «παρουσιάζεται» χρησιμοποιώντας την εντολή HELO. Στο μεγαλύτερο αριθμό περιπτώσεων ανεπιθύμητης αλληλογραφίας το συγκεκριμένο βήμα είτε παρακάμπτεται εντελώς, είτε στέλνονται από την εφαρμογή – πελάτη μη έγκυρες πληροφορίες. Έτσι, παρά την ευκολία υλοποίησης του συγκεκριμένου ελέγχου, τα αποτελέσματα φιλτραρίσματος ανεπιθύμητης αλληλογραφίας μέσω αυτού είναι εντυπωσιακά. Οι σχετικές παράμετροι που απαιτούνται για τον έλεγχο του πρώτου σταδίου είναι σχετικά απλές στη χρήση τους και περιλαμβάνονται στον τομέα «HELO restrictions» του αρχείου σχετικών ρυθμίσεων της εφαρμογής postfix (main.cf).

Το αμέσως επόμενο στάδιο φιλτραρίσματος των μηνυμάτων ηλεκτρονικής αλληλογραφίας αφορά στον έλεγχο του αποστολέα του εισερχομένου μηνύματος. Είναι αυτονόητο ότι, από τη στιγμή που η διεύθυνση ηλεκτρονικού ταχυδρομείου του

αποστολέα είναι ανύπαρκτη ή διαμορφωμένη λανθασμένα, δεν υπάρχει λόγος αποδοχής μηνυμάτων αλληλογραφίας από αυτόν. Οι σχετικές παράμετροι που απαιτούνται για τον έλεγχο του δεύτερου σταδίου είναι επίσης απλές στη χρήση τους και περιλαμβάνονται στον τομέα «Sender restrictions» του αρχείου ρυθμίσεων main.cf.

Στο τρίτο και τελευταίο στάδιο της διαδικασίας φιλτραρίσματος της ηλεκτρονικής αλληλογραφίας γίνεται έλεγχος του παραλήπτη του εισερχομένου μηνύματος, καθώς και όλοι οι επιπλέον έλεγχοι, που απαιτούν περισσότερη επεξεργασία (φόρτο συστήματος). Σε αυτό το στάδιο εμπλέκονται σημαντικές παράμετροι, όπως η reject_unauth_destination που αποτρέπει τη χρήση του εξυπηρετητή για «αναμετάδοση» αλληλογραφίας, καθώς και η reject_rbl_client που χρησιμοποιεί Realtime Blackhole λίστες για τον προσδιορισμό διευθύνσεων δικτύου πληροφοριακών συστημάτων, τα οποία έχουν πρόσφατα εμπλακεί σε εκτεταμένη αποστολή ανεπιθύμητης αλληλογραφίας. Όλες οι εμπλεκόμενες παράμετροι εξακολουθούν να είναι απλές στη χρήση τους και περιλαμβάνονται στον τομέα «Recipient restrictions» του αρχείου ρυθμίσεων της εφαρμογής Postfix.

Σημείωση: Είναι ιδιαίτερα σημαντικό το να πραγματοποιούνται οι έλεγχοι με σειρά προτεραιότητας που να έχει ως στόχο αφενός την ελαχιστοποίηση των περιστατικών λανθασμένου χαρακτηρισμού αλληλογραφίας ως ανεπιθύμητης, αφετέρου την ελαχιστοποίηση του φόρτου εργασίας του συστήματος, ειδικά εάν το τελευταίο είναι επιφορτισμένο και με επιπλέον αρμοδιότητες εκτός της υπηρεσίας ηλεκτρονικής αλληλογραφίας. Σε κάθε περίπτωση οι ρυθμίσεις είναι εφικτό να δοκιμάζονται στην πράξη χωρίς να κινδυνεύει η πραγματική αλληλογραφία ενός επιχειρησιακού συστήματος, εάν χρησιμοποιηθεί η παράμετρος warn_if_reject, η οποία απλά ενεργοποιεί την αποστολή πληροφοριών αποσφαλμάτωσης στο αρχείο καταγραφής ηλεκτρονικής αλληλογραφίας (maillog) και παρακάμπτει τον περαιτέρω έλεγχο του μηνύματος. Περισσότερα σχετικά με τις ρυθμίσεις της εφαρμογής Postfix για τον περιορισμό της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (Unsolicited Commercial Email) μπορούν να αντληθούν από την επίσημη ιστοσελίδα της εφαρμογής [98].

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων main.cf:

```
vi /etc/postfix/main.cf
```

Οδηγία: Στο τέλος του αρχείου προσθέτουμε τις παρακάτω γραμμές:

```
[...]
disable_vrfy_command = yes
strict_rfc821_envelopes = yes

# HELO restrictions:
smtpd_delay_reject = yes
smtpd_helo_required = yes
smtpd_helo_restrictions = permit_mynetworks,
                          permit_sasl_authenticated,
                          reject_invalid_helo_hostname,
                          reject_non_fqdn_helo_hostname,
                          reject_unknown_helo_hostname,
                          permit

# Sender restrictions:
smtpd_sender_restrictions = permit_mynetworks,
                            permit_sasl_authenticated,
                            reject_non_fqdn_sender,
                            reject_unknown_sender_domain,
                            permit

# Recipient restrictions:
smtpd_recipient_restrictions = permit_mynetworks,
                               permit_sasl_authenticated,
                               reject_unauth_pipelining,
                               reject_unauth_destination,
                               reject_non_fqdn_recipient,
                               reject_unknown_recipient_domain,
                               reject_rbl_client zen.spamhaus.org,
                               reject_rbl_client bl.spamcop.net,
                               reject_rbl_client dnsbl.sorbs.net,
                               reject_rbl_client cbl.abuseat.org,
                               reject_rbl_client ix.dnsbl.manitu.net,
                               permit
```

Οδηγία: Επανεκκινούμε την εφαρμογή postfix, ώστε να ισχύσουν άμεσα οι αλλαγές:

```
/etc/init.d/postfix restart
```

Εκτός από τις ρυθμίσεις που ολοκληρώθηκαν στα αμέσως προηγούμενα βήματα, υπάρχει η δυνατότητα ενεργοποίησης δύο επιπλέον τεχνικών ελέγχου της ηλεκτρονικής αλληλογραφίας για ανεπιθύμητα μηνύματα. Η πρώτη τεχνική αφορά στην εκμετάλλευση της εγγραφής του πλαισίου πολιτικής αποστολέα (spf), η οποία μπορεί να χρησιμοποιηθεί για την πιστοποίηση της εξουσιοδότησης του αποστολέα του μηνύματος και η δεύτερη στην όχι άμεση αποδοχή των μηνυμάτων που προέρχονται από μη αναγνωρισμένο αποστολέα (greylisting).

Αναλυτικά, το πλαίσιο πολιτικής αποστολέα (spf) είναι μια τεχνολογία προστασίας από την πλαστογράφηση της ηλεκτρονικής αλληλογραφίας. Επιτρέπει στους υπευθύνους τομέα να διατηρούν στις ζώνες ονομάτων του τομέα τους, λίστες με εξουσιοδοτημένες πηγές αποστολής ηλεκτρονικής αλληλογραφίας και, συνεπώς, στους παραλήπτες αλληλογραφίας να απορρίπτουν μηνύματα, τα οποία δεν προέρχονται από τις πηγές αυτές. Όλες οι σχετικές προδιαγραφές καθορίζονται στο έγγραφο RFC4408 και εφαρμόζονται στα πληροφοριακά συστήματα με ειδικό λογισμικό εξυπηρετητή πολιτικής. Για την εφαρμογή postfix υπάρχουν δύο εξυπηρετητές πολιτικής που εναρμονίζονται πλήρως με τις προδιαγραφές RFC4408 και που μπορούν να εγκατασταθούν στο Debian GNU/Linux. Ο ένας είναι γραμμένος σε γλώσσα Python και ο άλλος σε Perl. Επειδή ο πρώτος προσφέρει πολύ περισσότερες δυνατότητες σε σχέση με το δεύτερο, χωρίς να παρουσιάζει κάποια ιδιαιτερότητα στην εγκατάστασή του, έχει επιλεγεί να χρησιμοποιηθεί στην παρούσα πτυχιακή εργασία.

Οδηγία: Επιβεβαιώνουμε με «enter» την πρόθεσή μας για εγκατάσταση των πακέτων λογισμικού που απαιτούνται για τον έλεγχο εγγραφών spf μέσω της εφαρμογής Postfix:

```
apt-get install postfix-policyd-spf-python
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων main.cf:

```
vi /etc/postfix/main.cf
```

Οδηγία: Στο αρχείο προσθέτουμε την παράμετρο «spf-policyd_time_limit» με τιμή «3600s»:

```
[...]
spf-policyd_time_limit = 3600s
[...]
```

Οδηγία: Στο ίδιο αρχείο, στον τομέα των ρυθμίσεων παραλήπτη (smtpd_recipient_restrictions), προσθέτουμε αμέσως μετά τη μεταβλητή «reject_unauth_destination», τη νέα μεταβλητή «check_policy_service» με τιμή «unix: private/policy-spf»:

```
[...]
smtpd_recipient_restrictions = permit_mynetworks,
                               permit_sasl_authenticated,
                               reject_unauth_pipelining,
                               reject_unauth_destination,
                               check_policy_service
unix:private/policy-spf,
                               reject_non_fqdn_recipient,
[...]
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων master.cf:

```
vi /etc/postfix/master.cf
```

Οδηγία: Στο τέλος του αρχείου προσθέτουμε τα παρακάτω:

```
[...]
policy-spf  unix  -       n       n       -       -       spawn
     user=nobody argv=/usr/bin/policyd-spf
```

Οδηγία: Επανεκκινούμε την εφαρμογή postfix, ώστε να ισχύσουν άμεσα οι αλλαγές:

```
/etc/init.d/postfix restart
```

Στη δεύτερη προαιρετική μέθοδο φιλτραρίσματος της ηλεκτρονικής αλληλογραφίας (greylisting) εφαρμόζεται μια διαφορετική προσέγγιση του προβλήματος. Κάθε εξυπηρετητής ηλεκτρονικής αλληλογραφίας που εφαρμόζει τη συγκεκριμένη τεχνική διατηρεί αρχείο με τρία δεδομένα για κάθε εισερχόμενο μήνυμα ηλεκτρονικής αλληλογραφίας:

- ü τη διεύθυνση δικτύου του πληροφοριακού συστήματος από το οποίο προέρχεται το μήνυμα
- ü τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα
- ü τη διεύθυνση ηλεκτρονικού ταχυδρομείου του παραλήπτη (ή παραληπτών)

Η συγκεκριμένη «τριπλέτα» κάθε νέου εισερχομένου μηνύματος ηλεκτρονικής αλληλογραφίας αναζητείται μεταξύ των αντίστοιχων «τριπλετών» που υπάρχουν ήδη στο αρχείο του εξυπηρετητή και στην περίπτωση που δε βρεθεί, τότε το μήνυμα εμπίπτει στην κατηγορία «greylist» και απορρίπτεται για κάποιο προκαθορισμένο χρονικό διάστημα. Ο εξυπηρετητής αποστολής του μηνύματος ενημερώνεται για την προσωρινή απόρριψη με ένα μήνυμα σφάλματος SMTP 4XX και έτσι, μετά την πάροδο κάποιου επίσης προκαθορισμένου χρονικού διαστήματος, η αποστολή του μηνύματος επιχειρείται εκ νέου. Στην περίπτωση της ανεπιθύμητης αλληλογραφίας ο αποστολέας συνήθως δεν έχει στη διάθεσή του πόρους που θα του επιτρέψουν να επαναδρομολογήσει την αποστολή του προσωρινά απορριφθέντος μηνύματος. Έτσι, με χρήση της συγκεκριμένης τεχνικής, τα σχετικά μηνύματα αντιμετωπίζονται επιτυχώς στο μεγαλύτερο ποσοστό των περιπτώσεων ανεπιθύμητης ηλεκτρονικής αλληλογραφίας.

Οδηγία: Επιβεβαιώνουμε με «enter» την πρόθεσή μας για εγκατάσταση των πακέτων λογισμικού που απαιτούνται για τη λειτουργία της εφαρμογής postgrey:

```
apt-get install postgrey
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο ρυθμίσεων main.cf:

```
vi /etc/postfix/main.cf
```

Οδηγία: Στο αρχείο προσθέτουμε τη νέα τιμή για την παράμετρο «check_policy_service», όπως παρακάτω:

```
  [...]
  smtpd_recipient_restrictions = permit_mynetworks,
                                 permit_sasl_authenticated,
                                 reject_unauth_pipelining,
                                 reject_unauth_destination,
                                 check_policy_service
unix:private/policy-spf,
                                 check_policy_service
inet:127.0.0.1:10023,
                                 reject_non_fqdn_recipient,
  [...]
```

Οδηγία: Επανεκκινούμε την εφαρμογή postfix, ώστε να ισχύσουν άμεσα οι αλλαγές:

```
  /etc/init.d/postfix restart
```

Αποκλεισμός προσπαθειών μη ασφαλών FTP συνδέσεων

Εάν η πολιτική ασφαλείας του εξυπηρετητή δεν επιτρέπει τις μη ασφαλείς FTP συνδέσεις (έχει δηλαδή επιλεγεί και χρησιμοποιηθεί η τιμή «2» για τη ρύθμιση του σχετικού αρχείου ρυθμίσεων /etc/pure-ftpd/conf/TLS), τότε θα πρέπει να προστεθεί μια κανονική έκφραση καθώς και η αντίστοιχη «φυλακή», ώστε να αποκλείονται μέσω της εφαρμογής fail2ban οι προσπάθειες για FTP σύνδεση απλού κειμένου.

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο pureftpd.conf:

```
  vi /etc/fail2ban/filter.d/pureftpd.conf
```

Οδηγία: Προσθέτουμε τη νέα failregex:

```
  [...]
  failregex = pure-ftpd: \(.*@<HOST>\) \[WARNING\] Sorry, cleartext
sessions are not accepted.*
  [...]
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο jail.local:

```
vi /etc/fail2ban/jail.local
```

Οδηγία: Τροποποιούμε τη «φυλακή» του pureftpd, προσθέτοντας τις επιπλέον πόρτες ασφαλούς σύνδεσης, όπως παρακάτω:

```
[...]
    [pureftpd]
    enabled  = true
    port     = ftp,ftp-data,ftps,ftps-data
    filter   = pureftpd
    logpath  = /var/log/syslog
    maxretry = 3
[...]
```

Οδηγία: Επανεκκινούμε την εφαρμογή fail2ban για να ισχύσουν άμεσα οι αλλαγές:

```
/etc/init.d/fail2ban restart
```

Με την ολοκλήρωση της διαδικασίας αποκλεισμού των μη ασφαλών συνδέσεων FPT, ολοκληρώθηκε η διαδικασία θωράκισης του συστήματος, τουλάχιστον όσον αφορά στον οδηγό της παρούσας εργασίας. Η συγκεκριμένη διαδικασία του system hardening αποτελεί μια σειρά ενεργειών, η οποία δεν είναι δυνατό να περατωθεί. Αυτό συμβαίνει επειδή οι προσπάθειες των κακόβουλων χρηστών για εξεύρεση και εκμετάλλευση αδυναμιών των πληροφοριακών συστημάτων που χρησιμοποιούν είναι αδιάκοπες και φέρνουν συνεχώς στην επιφάνεια νέα προβλήματα ασφαλείας, τα οποία με τη σειρά τους επιλύουν οι διαχειριστές των συστημάτων αυτών με νέες ενέργειες ή/και ρυθμίσεις που θα πρέπει κάθε φορά να εκτελέσουν. Έτσι, στα επιχειρησιακά συστήματα θα πρέπει να γίνεται από τους υπεύθυνους αυτών συνεχής προσπάθεια για διατήρηση του μέγιστου δυνατού επιπέδου ασφαλείας.

Βελτιστοποίηση συστήματος

Στη διαδικασία θωράκισης του εξυπηρετητή που μόλις ολοκληρώθηκε δεν έχει γίνει καμία μνεία για ενέργειες, οι οποίες αφορούν στη βελτιστοποίηση της λειτουργίας του. Σε τέτοιου είδους πληροφοριακά συστήματα, όπου οι απαιτήσεις είναι αφενός εξειδικευμένες,

αφετέρου αρκετά υψηλές, η βέλτιστη λειτουργικότητα αποτελεί μια συνεχή επιδίωξη των υπευθύνων και δεν είναι δυνατό να καλυφθεί από μια εργασία όπως η παρούσα. Για το λόγο αυτό παρακάτω θα αναλυθούν ορισμένες και μόνο ενέργειες που μπορούν να λάβουν χώρα, συνεισφέροντας στη βελτιστοποίηση του συστήματος και που αφορούν στην εγκατάσταση της Ελληνικής τοπικοποίησης του συστήματος, την εγκατάσταση ενός πιστοποιητικού, υπογεγραμμένου από ανεξάρτητη και αναγνωρισμένη αρχή και, τέλος, ρυθμίσεις που θα πρέπει να λάβουν χώρα ώστε να βελτιστοποιηθεί η λειτουργία του εξυπηρετητή βάσεων δεδομένων (MySQL).

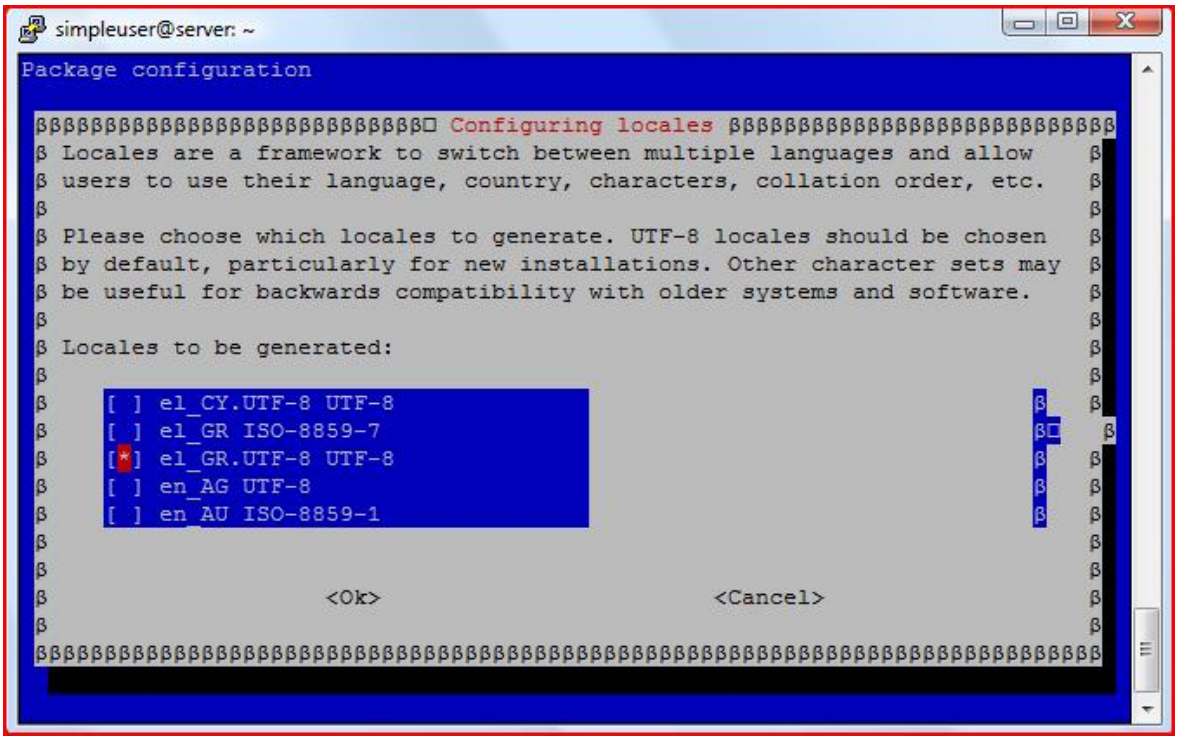
Εγκατάσταση Ελληνικού locale

Στη διαδικασία της εγκατάστασης του συστήματος έχει επιλεγεί ως προκαθορισμένη παράμετρος τοπικοποίησης η en_US.UTF-8. Αυτό έγινε για να μεγιστοποιηθεί η συμβατότητα και να αποφευχθούν τυχόν προβλήματα με το υπόλοιπο προς εγκατάσταση λογισμικό. Έχοντας πλέον ολοκληρωθεί η διαδικασία εγκατάστασης, είναι εφικτό να εγκατασταθεί και οριστεί ως δεύτερη παράμετρος τοπικοποίησης η Ελληνική, χωρίς να αλλοιωθεί η προεπιλεγμένη ρύθμιση της Αγγλικής Ηνωμένων Πολιτειών. Η παράλληλη εγκατάσταση του Ελληνικού locale θα επιτρέπει την επιλεκτική χρήση και των δύο παραμέτρων τοπικοποίησης, ανάλογα με την εκάστοτε περίσταση.

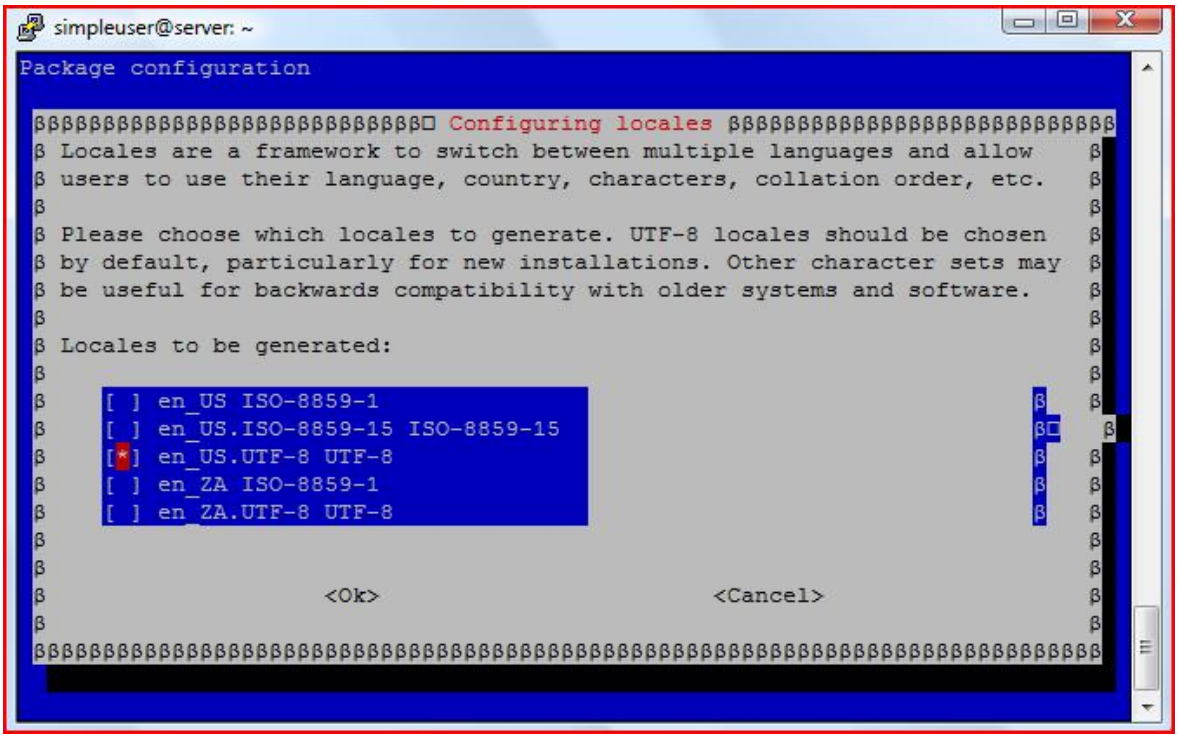
Οδηγία: Εκτελούμε την εντολή επανακαθορισμού των παραμέτρων τοπικοποίησης του συστήματος:

```
dpkg-reconfigure locales
```

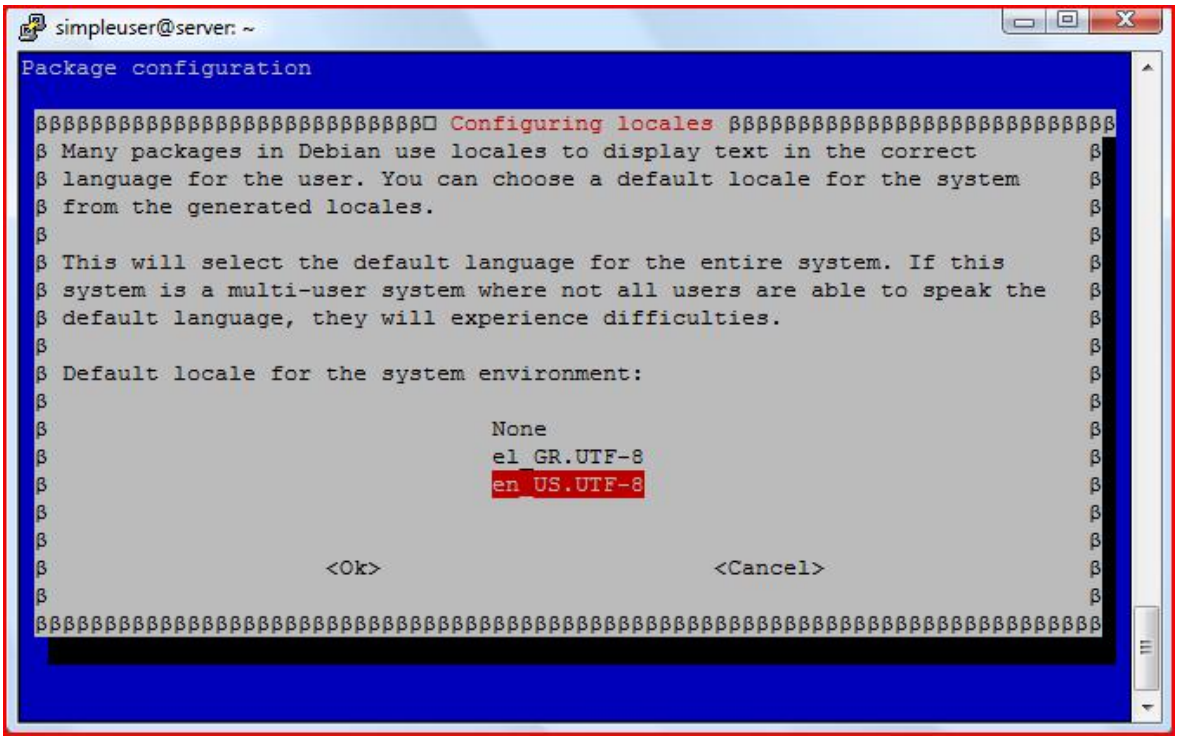
Οδηγία: Επιλέγουμε να γίνει εγκατάσταση της παραμέτρου τοπικοποίησης el_GR.UTF8 UTF8:



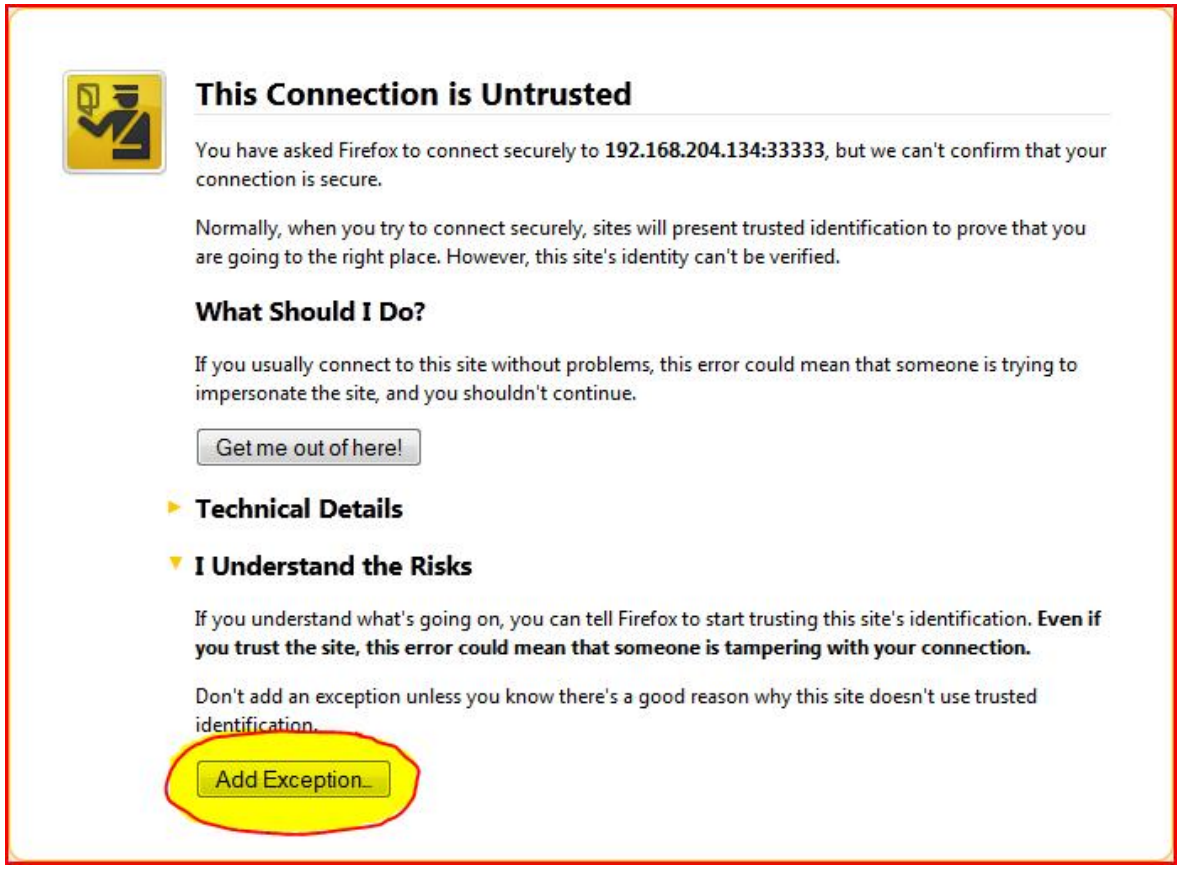
Οδηγία: Επιβεβαιώνουμε ότι είναι ήδη επιλεγμένη και η παράμετρος τοπικοποίησης en_US.UTF8 UTF8 και μετακινούμαστε στο επόμενο βήμα, χρησιμοποιώντας την επιλογή «OK»:

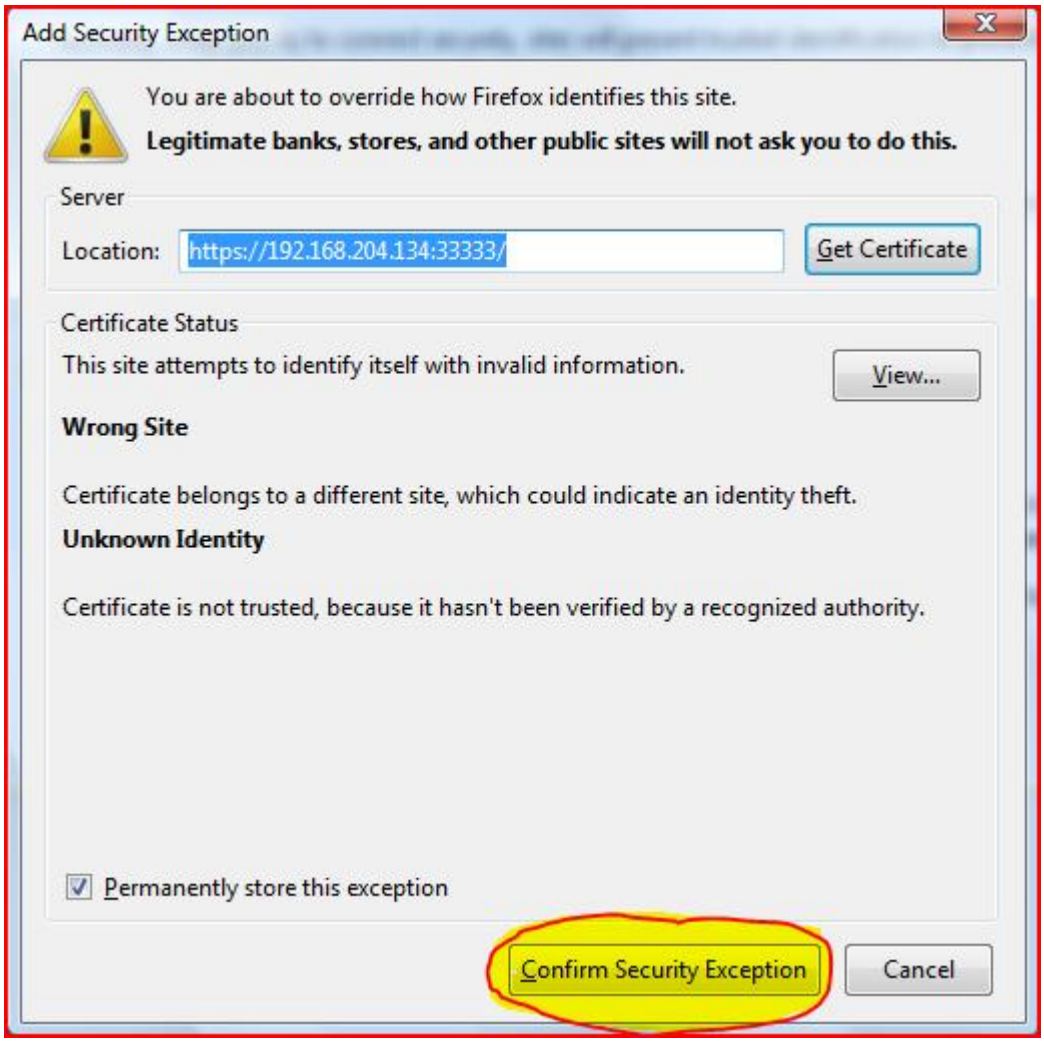


Οδηγία: Καθορίζουμε την παράμετρο τοπικοποίησης en_US.UTF8 UTF8, ως την προεπιλεγμένη παράμετρο για την τοπικοποίηση του συστήματος και επιλέγουμε την ολοκλήρωση της διαδικασίας, χρησιμοποιώντας την επιλογή «OK»:



Εάν κατά τη διαδικασία εγκατάστασης του πίνακα ελέγχου ISPConfig, στην ερώτηση του βοηθού εγκατάστασης «Do you want a secure (SSL) connection to the ISPConfig web interface» έχει δοθεί θετική απάντηση, τότε έχει αυτόματα δημιουργηθεί ένα «self-signed» πιστοποιητικό SSL, το οποίο και χρησιμοποιείται για τις ασφαλείς συνδέσεις των χρηστών με τον εξυπηρετητή. Επειδή το συγκεκριμένο πιστοποιητικό στερείται της υπογραφής κάποιου αναγνωρισμένου φορέα, οι συνδέσεις που επιτυγχάνονται με χρήση του θεωρούνται «μη εμπιστεύσιμες» και ζητείται από το χρήστη η προσθήκη σχετικής εξαίρεσης:





Για να αποφευχθούν οι συγκεκριμένες προειδοποιήσεις ασφαλείας κατά τη χρήση του πιστοποιητικού, θα πρέπει να πραγματοποιηθεί αντικατάστασή του με νέο, το οποίο όμως να είναι υπογεγραμμένο από μια αναγνωρισμένη, ανεξάρτητη πηγή. Η έκδοση ενός τέτοιου, υπογεγραμμένου πιστοποιητικού SSL συνήθως κοστίζει αρκετά, πάραυτα, υπάρχουν περιπτώσεις στις οποίες η διάθεσή του πραγματοποιείται με μικρό ή ακόμη και με μηδενικό κόστος.

Ένα τέτοιο παράδειγμα αποτελεί η περίπτωση του ιστοτόπου www.startssl.com, στον οποίο παρέχεται η δυνατότητα απόκτησης ενός δωρεάν, υπογεγραμμένου, Class 1, Web Server SSL/TLS Certificate (απαιτείται δημιουργία λογαριασμού χρήστη, καθώς και επιβεβαιώσεις της δοθείσας διεύθυνσης ηλεκτρονικού ταχυδρομείου και του ονόματος τομέα του εξυπηρετητή). Στην αυτοματοποιημένη διαδικασία θα ζητηθεί από το χρήστη η αίτηση δημιουργίας του πιστοποιητικού (CSR), η οποία έχει παραχθεί μαζί με το self-signed SSL πιστοποιητικό κατά την εγκατάσταση του ISPConfig και βρίσκεται στο

φάκελο /usr/local/ispconfig/interface/ssl/. Εάν απαιτείται η επαναδημιουργία των σχετικών αρχείων θα πρέπει να εκτελεστεί η εντολή επικαιροποίησης του ISPConfig και ακολούθως να απαντηθεί θετικά η ερώτηση «Create new ISPConfig SSL certificate»:

```
ispconfig_update.sh
```

Όταν θα έχει με τον ένα ή τον άλλο τρόπο αποκτηθεί το νέο, υπογεγραμμένο πιστοποιητικό, θα πρέπει να πραγματοποιηθούν οι ενέργειες εγκατάστασής του, ώστε μπορεί να γίνει η επιχειρησιακή εκμετάλλευσή του. Εάν το εν λόγω, νέο πιστοποιητικό είναι τύπου class1 (όπως στην περίπτωση του παραπάνω δωρεάν πιστοποιητικού) η διαδικασία εγκατάστασης έχει ως ακολούθως. Εύλογα, σε διαφορετική περίπτωση , όπως για παράδειγμα πιστοποιητικού τύπου class2, θα πρέπει να γίνουν οι απαραίτητες διορθώσεις στις εντολές.

Οδηγία: Διατηρούμε το υπάρχον αρχείο ispserver.srt ως αντίγραφο ασφαλείας, μετονομάζοντάς το σε ispserver.srt_bak:

```
mv /usr/local/ispconfig/interface/ssl/ispserver.crt
/usr/local/ispconfig/interface/ssl/ispserver.crt_bak
```

Οδηγία: Δημιουργούμε ένα νέο αρχείο ispserver.srt:

```
touch /usr/local/ispconfig/interface/ssl/ispserver.crt
```

Οδηγία: Ανοίγουμε για επεξεργασία το νέο αρχείο ispserver.srt:

```
vi /usr/local/ispconfig/interface/ssl/ispserver.crt
```

Οδηγία: Αντιγράφουμε και επικολλούμε σε αυτό τα περιεχόμενα του νέου, υπογεγραμμένου πιστοποιητικού:

```
-----BEGIN CERTIFICATE-----
MIIHMTCCBhmgAwIBAgIDxxxxx0GCSqGSIb3DQEBBQUAMIGMMQswCQYDVQQGEwJJ
[...]
c2x1wonVRVmKovt2OuM1ZqZw0Ynk
-----END CERTIFICATE-----
```

Οδηγία: Από σχετικό σύνδεσμο της εκδούσας αρχής του νέου, υπογεγραμμένου πιστοποιητικού μεταφορτώνουμε στον τοπικό φάκελο /usr/local/ispconfig/interface/ssl του εξυπηρετητή, τα απαραίτητα πιστοποιητικά root και intermediate (οι ακόλουθες εντολές αφορούν στην περίπτωση των Root CA και Class1 Intermediate Server CA του παραδείγματος της StartSSL):

```
  cd /usr/local/ispconfig/interface/ssl
  wget https://www.startssl.com/certs/ca.pem
  wget
https://www.startssl.com/certs/sub.class1.server.ca.pem
```

Οδηγία: Μετονομάζουμε τα δύο αρχεία των πιστοποιητικών root και intermediate:

```
  mv ca.pem startssl.ca.crt
  mv sub.class1.server.ca.pem
startssl.sub.class1.server.ca.crt
```

Οδηγία: Επειδή μερικές από τις υπηρεσίες του εξυπηρετητή απαιτούν την ύπαρξη του αρχείου ispserver.pem, δημιουργούμε το εν λόγω αρχείο με τις παρακάτω εντολές:

```
  cat startssl.sub.class1.server.ca.crt startssl.ca.crt >
startssl.chain.class1.server.crt
  cat ispserver.{key,crt} startssl.chain.class1.server.crt >
ispserver.pem
  chmod 600 ispserver.pem
```

Οδηγία: Θα πρέπει να ενημερώσουμε την επιφάνεια διεπαφής του πίνακα ελέγχου ISPConfig για την ύπαρξη του νέου πιστοποιητικού. Στην περίπτωση που έχει επιλεγεί να χρησιμοποιηθεί ως εξυπηρετητής Παγκοσμίου Ιστού του συστήματος ο Apache, ανοίγουμε για επεξεργασία το σχετικό αρχείο ρυθμίσεων ispconfig.vhost:

```
  vi /etc/apache2/sites-available/ispconfig.vhost
```

Οδηγία: Στον τομέα « # SSL Configuration » προσθέτουμε τη γραμμή SLCertificateChainFile /usr/local/ispconfig/interface/ssl/startssl.sub.class1.server.ca.crt (ΠΡΟΣΟΧΗ: *το συγκεκριμένο βήμα θα πρέπει να επαναληφθεί εάν μελλοντικά επικαιροποιηθεί η εφαρμογή ISPConfig*):

```
  [...]
    # SSL Configuration
    SSLEngine On
    SSLCertificateFile /usr/local/ispconfig/interface/ssl/ispserver.crt
    SSLCertificateKeyFile
/usr/local/ispconfig/interface/ssl/ispserver.key
    ## must be re-added after an ISPConfig update!!!
    SSLCertificateChainFile
/usr/local/ispconfig/interface/ssl/startssl.sub.class1.server.ca.crt
  [...]
```

Οδηγία: Για να ισχύσουν άμεσα οι αλλαγές, επανεκκινούμε τον Apache:

```
  /etc/init.d/apache2 restart
```

Οδηγία: Στην περίπτωση που αντί για τον Apache έχει επιλεγεί να χρησιμοποιηθεί ο nginx ως εξυπηρετητής Παγκοσμίου Ιστού στον εξυπηρετητή, θα πρέπει αντί για τα παραπάνω βήματα να εκτελεστούν οι ακόλουθες εντολές:

```
  cat
/usr/local/ispconfig/interface/ssl/startssl.sub.class1.server
.ca.crt >> /usr/local/ispconfig/interface/ssl/ispserver.crt
  /etc/init.d/nginx reload
```

Εκτός από τον πίνακα ελέγχου ISPConfig, θα πρέπει να πραγματοποιηθούν ενέργειες ώστε να ενημερωθεί για την ύπαρξη του νέου, υπογεγραμμένου πιστοποιητικού και η εφαρμογή Postfix.

Οδηγία: Διατηρούμε ως αντίγραφα ασφαλείας τα υπάρχοντα αρχεία smtpd.cert και smtpd.key με τα αντίστοιχα ονόματα smtpd.cert_bak και smtpd.key_bak:

```
  mv /etc/postfix/smtpd.cert /etc/postfix/smtpd.cert_bak
  mv /etc/postfix/smtpd.key /etc/postfix/smtpd.key_bak
```

Οδηγία: Δημιουργούμε συμβολικούς δεσμούς με το όνομα smtpd.cert και smtpd.key που θα «δείχνουν» στα αρχεία ispserver.crt και ispserver.key αντίστοιχα:

```
  ln -s /usr/local/ispconfig/interface/ssl/ispserver.crt
/etc/postfix/smtpd.cert
  ln -s /usr/local/ispconfig/interface/ssl/ispserver.key
/etc/postfix/smtpd.key
```

Οδηγία: Ενημερώνουμε σχετικά το αρχείο ρυθμίσεων main.cf της εφαρμογής Postfix με την παράμετρο smtpd_tls_CAfile:

```
  postconf -e 'smtpd_tls_CAfile =
/usr/local/ispconfig/interface/ssl/startssl.chain.class1.serv
er.crt'
```

Οδηγία: Επανεκκινούμε την εφαρμογή Postfix για να ισχύσουν άμεσα οι αλλαγές:

```
  /etc/init.d/postfix restart
```

Παρομοίως, θα πρέπει να γίνουν οι απαιτούμενες ενέργειες, ώστε να ενημερωθεί και η εφαρμογή Courier για την ύπαρξη του νέου, υπογεγραμμένου πιστοποιητικού.

Οδηγία: Διατηρούμε ως αντίγραφα ασφαλείας τα υπάρχοντα αρχεία imapd.pem και pop3d.pem με τα αντίστοιχα ονόματα imapd.pem_bak και pop3d.pem_bak:

```
  mv /etc/courier/imapd.pem /etc/courier/imapd.pem.bak
  mv /etc/courier/pop3d.pem /etc/courier/pop3d.pem.bak
```

Οδηγία: Δημιουργούμε συμβολικούς δεσμούς με το όνομα imapd.pem και pop3d.pem που θα «δείχνουν» στο αρχείο ispserver.pem:

```
  ln -s /usr/local/ispconfig/interface/ssl/ispserver.pem
/etc/courier/imapd.pem
  ln -s /usr/local/ispconfig/interface/ssl/ispserver.pem
/etc/courier/pop3d.pem
```

Οδηγία: Επανεκκινούμε την εφαρμογή Courier για να ισχύσουν άμεσα οι αλλαγές:

```
  /etc/init.d/courier-imap-ssl stop
  /etc/init.d/courier-imap-ssl start
  /etc/init.d/courier-pop-ssl stop
  /etc/init.d/courier-pop-ssl start
```

Εκτός από τις παραπάνω εφαρμογές θα πρέπει να πραγματοποιηθούν οι ενέργειες που απαιτούνται, ώστε να ενημερωθεί και η εφαρμογή PureFTPd για την ύπαρξη του νέου, υπογεγραμμένου πιστοποιητικού.

Οδηγία: Διατηρούμε αντίγραφο του υπάρχοντος αρχείου pure-ftpd.pem με το όνομα pure-ftpd.pem_bak:

```
  mv /etc/ssl/private/pure-ftpd.pem /etc/ssl/private/pure-
ftpd.pem_bak
```

Οδηγία: Δημιουργούμε συμβολικό δεσμό με το όνομα pure-ftpd.pem που θα «δείχνει» στο αρχείο ispserver.pem:

```
  ln -s /usr/local/ispconfig/interface/ssl/ispserver.pem
/etc/ssl/private/pure-ftpd.pem
```

Οδηγία: Επανεκκινούμε την εφαρμογή PureFTPd για να ισχύσουν άμεσα οι αλλαγές:

```
  /etc/init.d/pure-ftpd-mysql restart
```

Με την ολοκλήρωση της παραπάνω διαδικασίας το νέο, υπογεγραμμένο πιστοποιητικό είναι πλήρως εγκατεστημένο στο σύστημα και έτσι, πλέον δεν εμφανίζονται οι προειδοποιήσεις ασφαλείας κατά τις συνδέσεις με τον εξυπηρετητή.

MySQL tuning

Σε κάθε διαδικτυακό εξυπηρετητή που παρέχει τη συγκεκριμένη υπηρεσία, η βελτιστοποίηση του συστήματος διαχείρισης σχεσιακών βάσεων δεδομένων MySQL αποτελεί μια διαδικασία συνεχής επιδίωξης και όχι ενέργεια που πραγματοποιείται άπαξ.

Η εν λόγω διαδικασία αφενός είναι χρονοβόρα και ιδιαίτερα λεπτομερής, αφετέρου απαιτεί εξειδικευμένες γνώσεις του συγκεκριμένου τομέα. Με στόχο την απλοποίησή της έχουν αναπτυχθεί βοηθήματα για τους υπευθύνους των σχετικών πληροφοριακών συστημάτων, με πολύ γνωστά παραδείγματα τα script Tuning-primer.sh και mysqltuner.pl

Τα παραπάνω script αφού μεταφορτωθούν και εκτελεστούν στο πληροφοριακό σύστημα είναι σε θέση να παράσχουν πληροφορίες σχετικά με τις παραμέτρους της MySQL που θα πρέπει να τροποποιηθούν, ώστε να βελτιστοποιηθεί η αντίστοιχη υπηρεσία. Βέβαια, για να είναι αξιόπιστες οι πληροφορίες προαπαιτείται ικανοποιητικός χρόνος τρεξίματος της υπηρεσίας σε πραγματικές, επιχειρησιακές συνθήκες.

Οδηγία: Δημιουργούμε το φάκελο /root/scripts, στον οποίο θα μεταφορτώσουμε τα συγκεκριμένα βοηθήματα:

```
mkdir /root/scripts
```

Οδηγία: Αλλάζουμε τον τρέχων φάκελο εργασίας (working directory) στο φάκελο που μόλις δημιουργήσαμε:

```
cd /root/scripts
```

Οδηγία: Μεταφορτώνουμε τα δύο script:

```
wget http://www.pc-freak.net/files/Tuning-primer.sh
wget http://mysqltuner.com/mysqltuner.pl
```

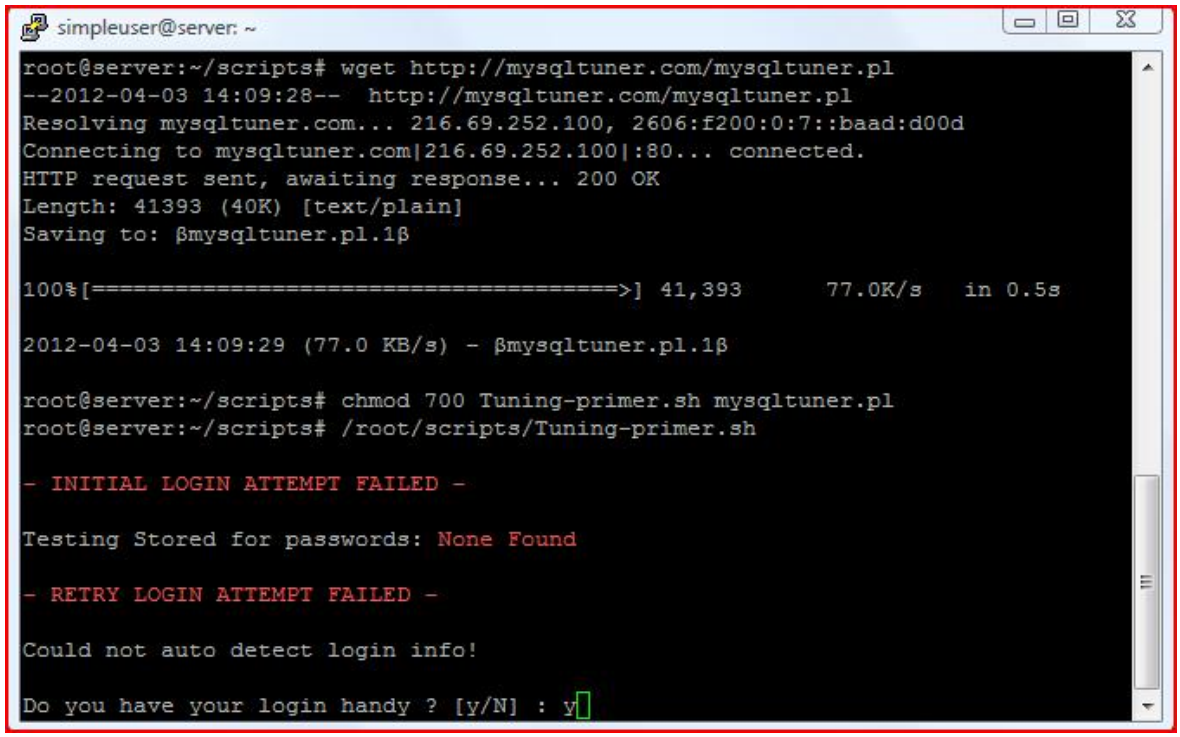
Οδηγία: Τροποποιούμε κατάλληλα τα δικαιώματα των δύο αρχείων που περιέχουν τα script:

```
chmod 700 Tuning-primer.sh mysqltuner.pl
```

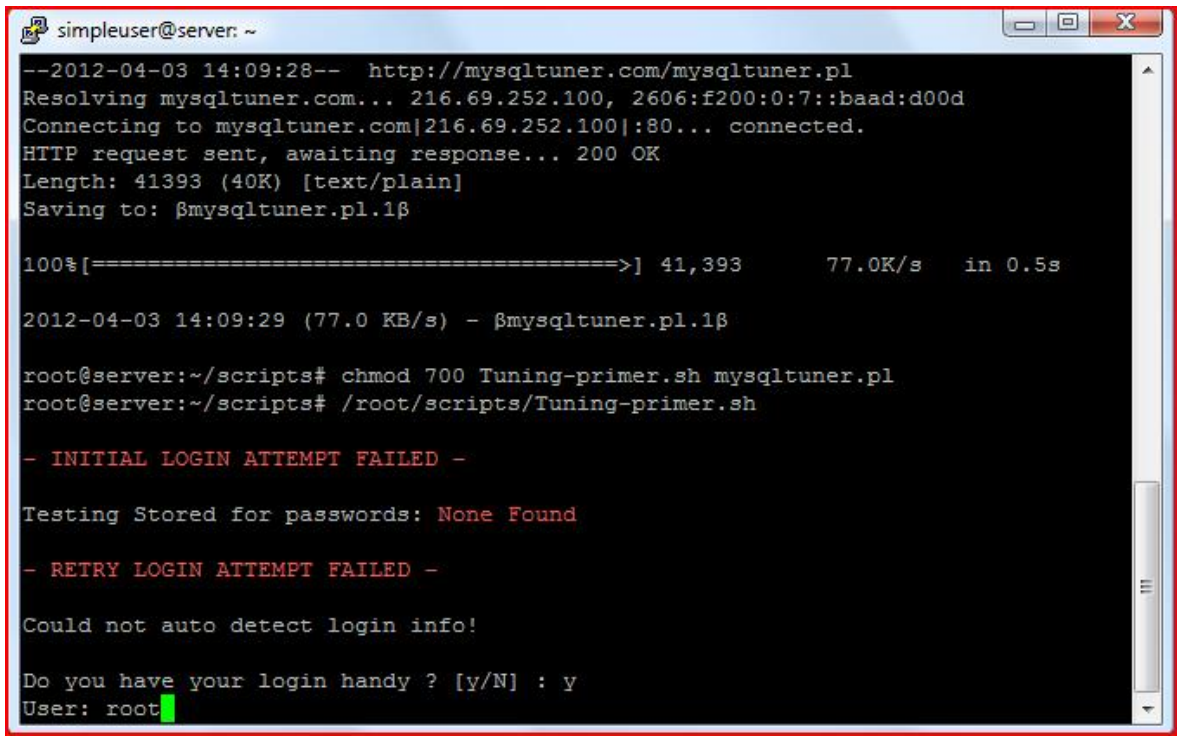
Οδηγία: Εκτελούμε το πρώτο από τα δύο script (Tuning-primer.sh):

```
/root/scripts/Tuning-primer.sh
```

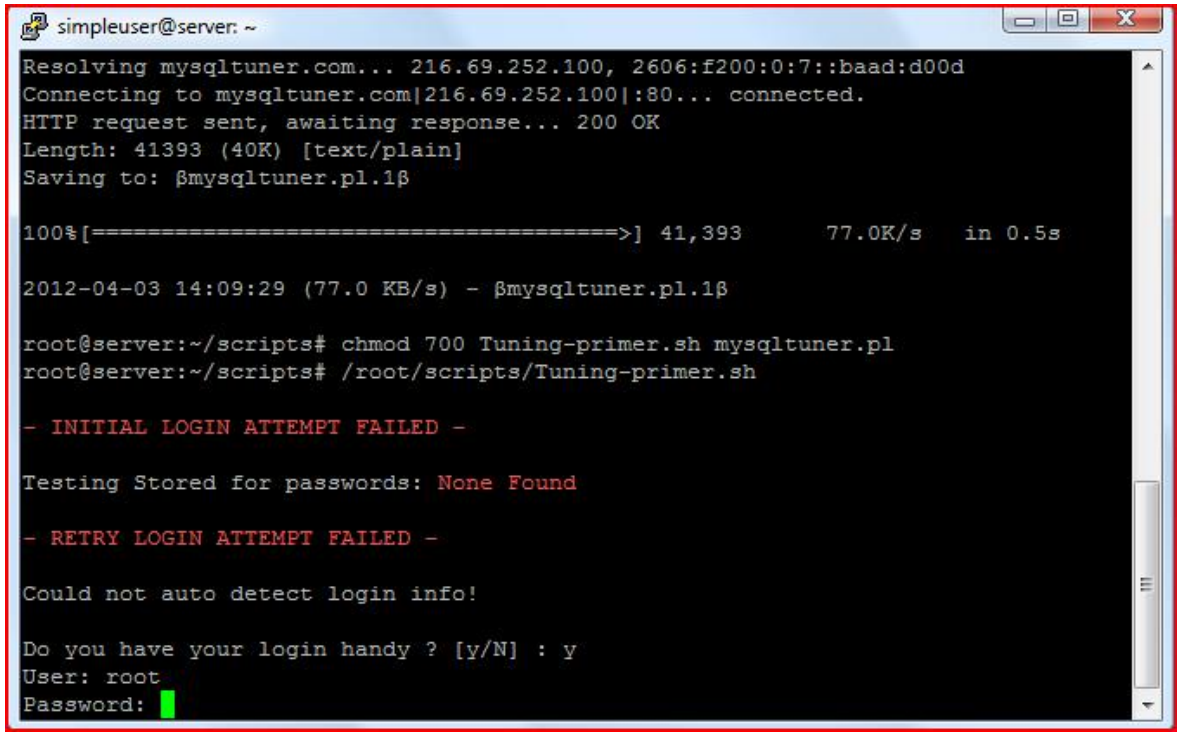
Οδηγία: Επιλέγουμε να ενημερώσουμε το βοήθημα για τα διαπιστευτήρια του διαχειριστή της υπηρεσίας MySQL, εισάγοντας «y»:



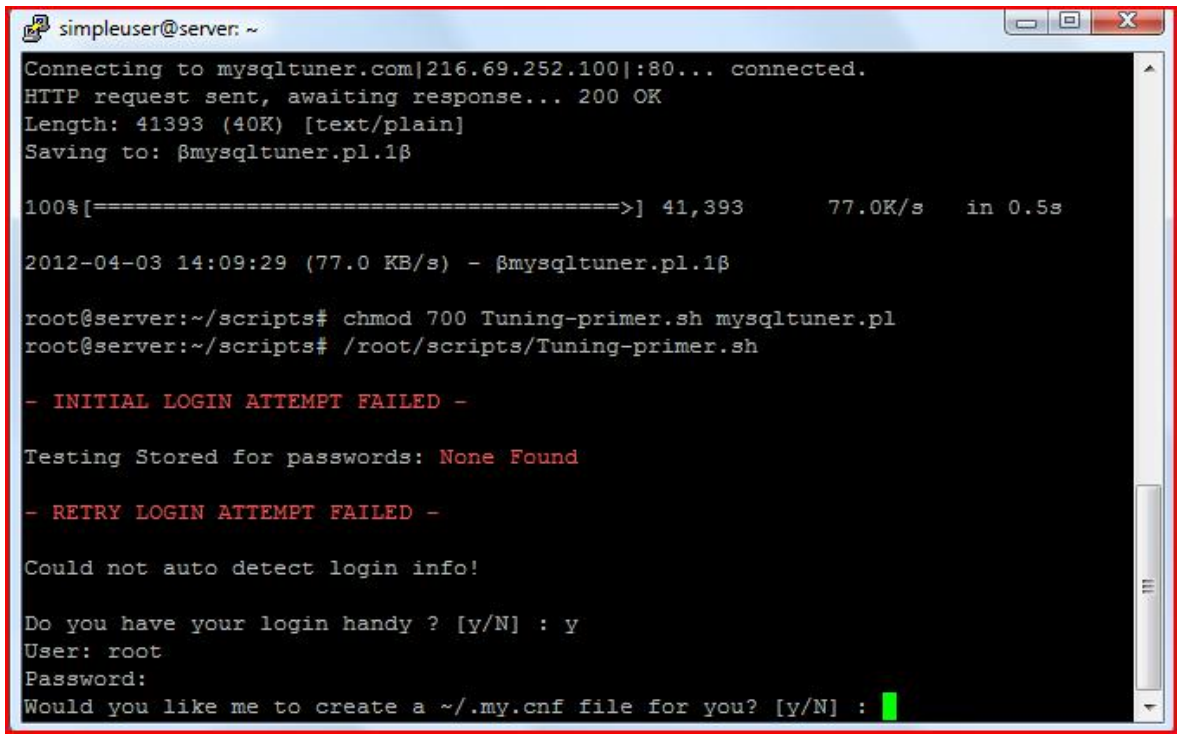
Οδηγία: Εισάγουμε το όνομα χρήστη του διαχειριστή της υπηρεσίας MySQL (root):



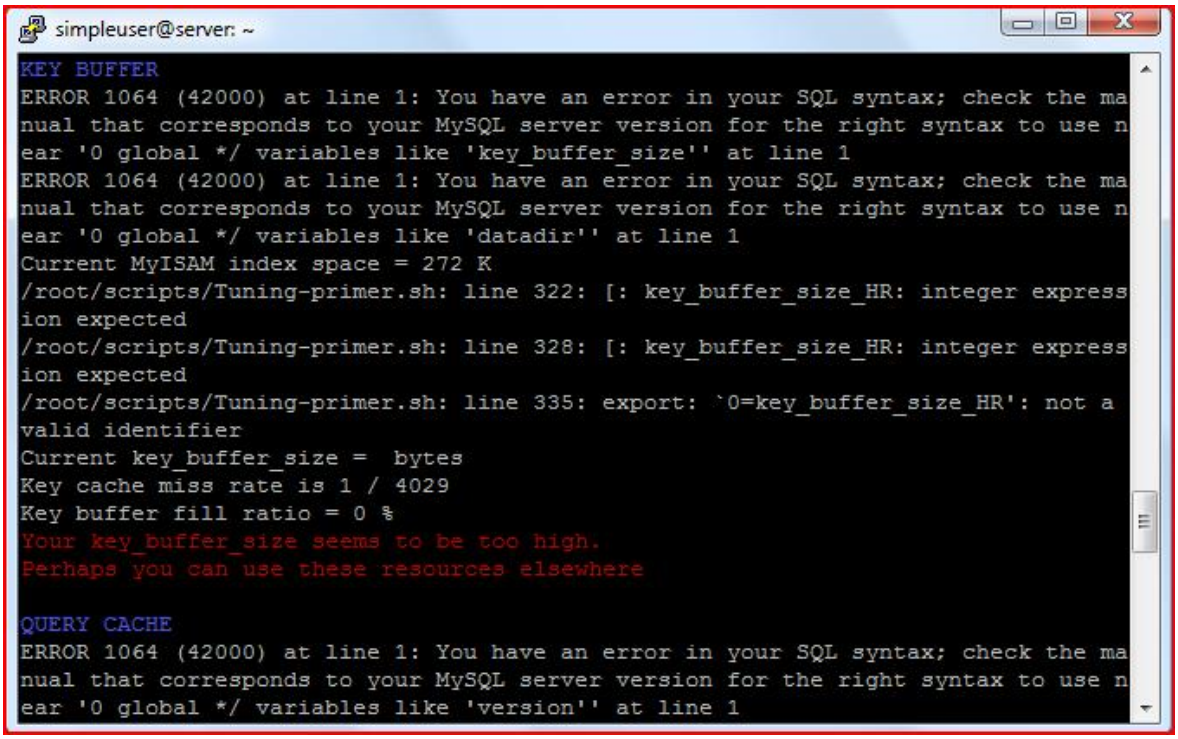
Οδηγία: Εισάγουμε τον κωδικό πρόσβασης του διαχειριστή της υπηρεσίας MySQL:



Οδηγία: Εισάγοντας enter, επιλέγουμε να μη δημιουργηθεί από το βοήθημα αρχείο ρυθμίσεων .my.cnf:



Οδηγία: Το script θα παράγει μια ακολουθία από αποτελέσματα των ελέγχων που έχει πραγματοποιήσει, τονίζοντας με κόκκινου χρώματος κείμενο τα προβλήματα που έχουν εντοπιστεί, καθώς και τις προτεινόμενες λύσεις αυτών:

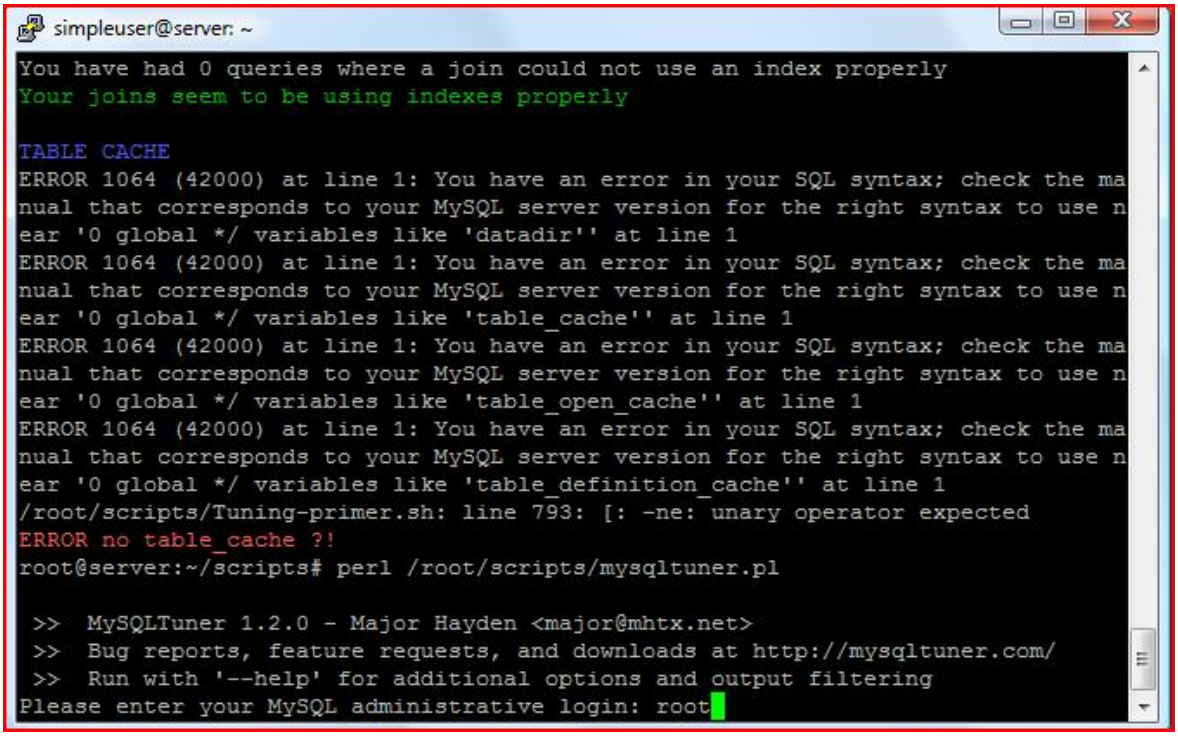


Σημείωση: Αφού διορθώσουμε τα προβλήματα που εντόπισε το script Tuning-primer.sh, επαναλαμβάνουμε τη διαδικασία για δεύτερη φορά, ώστε να επιβεβαιώσουμε την καλή λειτουργία της υπηρεσίας MySQL.

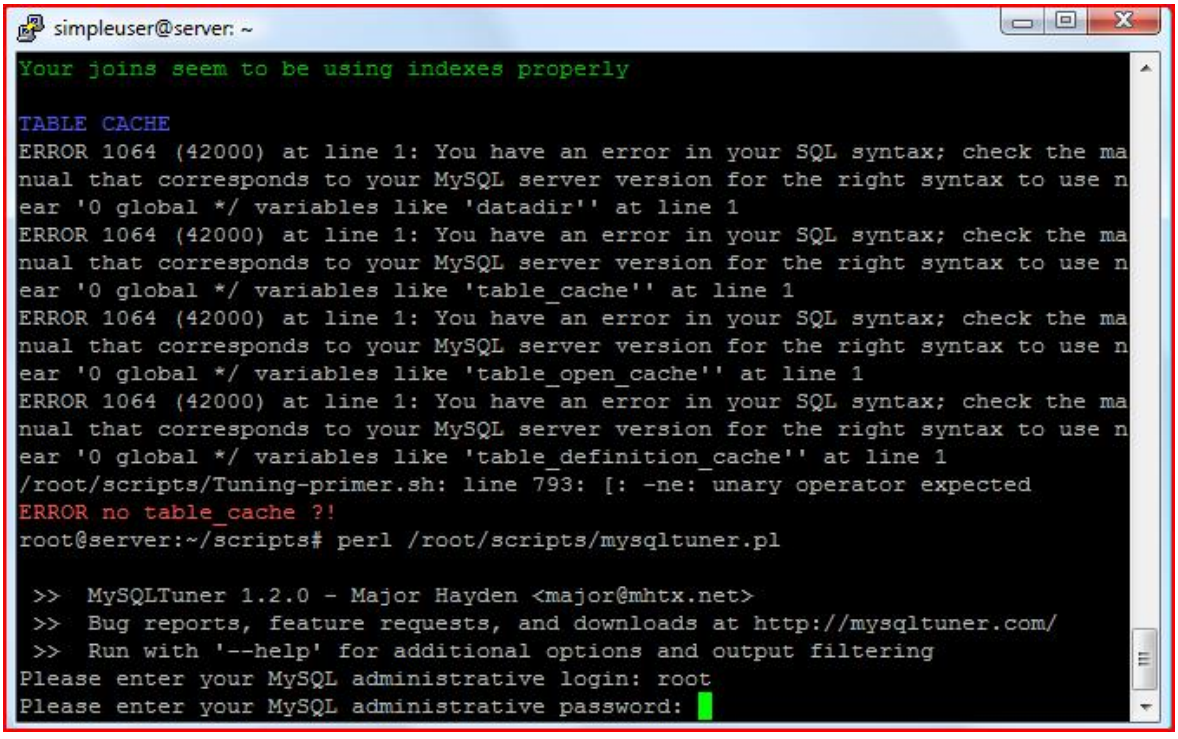
Οδηγία: Ακολύθως, εκτελούμε το δεύτερο από τα script (mysqltuner.pl):

```
perl /root/scripts/mysqltuner.pl
```

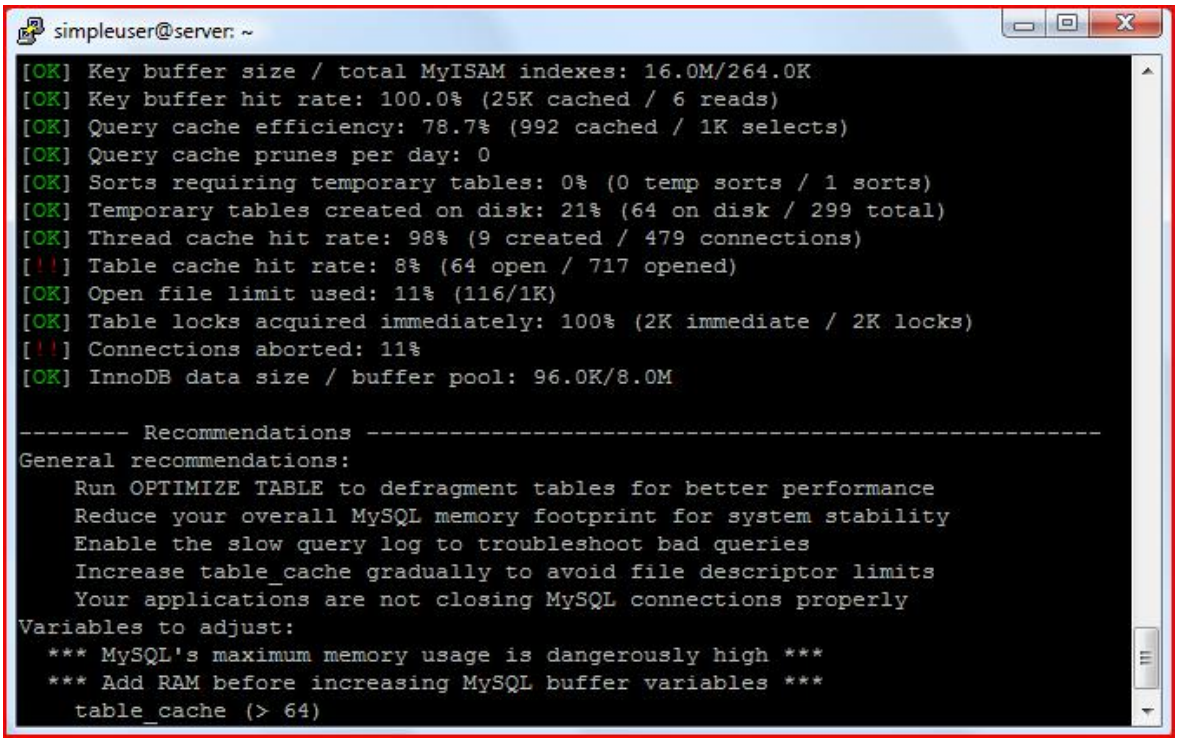
Οδηγία: Εισάγουμε το όνομα χρήστη του διαχειριστή της υπηρεσίας MySQL (root):



Οδηγία: Εισάγουμε τον κωδικό πρόσβασης του διαχειριστή της υπηρεσίας MySQL:



Οδηγία: Το script θα παράγει μια ακολουθία από αποτελέσματα των ελέγχων που έχει πραγματοποιήσει, στα οποία περιλαμβάνονται τυχόν προβλήματα, καθώς και οι προτεινόμενες λύσεις αυτών:



Σημείωση: Αφού διορθώσουμε τα προβλήματα που εντόπισε το συγκεκριμένο script, επαναλαμβάνουμε τη διαδικασία για μια ακόμη φορά, ώστε να επιβεβαιώσουμε τη βέλτιστη λειτουργία της υπηρεσίας MySQL.

Είναι προφανές ότι για την επίλυση των προβλημάτων που είναι πιθανό να εντοπιστούν από τα παραπάνω βοηθήματα, απαιτείται εξειδικευμένη εμβάθυνση στη συγκεκριμένη υπηρεσία διαχείρισης σχεσιακών βάσεων δεδομένων. Φυσικά, αυτό ξεφεύγει από τα όρια της παρούσας πτυχιακής εργασίας και για το λόγο αυτό παραλείπεται.

Δημιουργία αντιγράφου ασφαλείας εγκατάστασης

Έχοντας ολοκληρώσει την πραγματοποίηση όλων των απαιτούμενων ενεργειών που αποσκοπούν στη θωράκιση, αλλά και τη βελτιστοποίηση του συστήματος, αυτό είναι απολύτως έτοιμο για επιχειρησιακή χρήση. Το μόνο που σε αυτό το σημείο απομένει για την ολοκλήρωση του οδηγού της παρούσας πτυχιακής εργασίας είναι το να

δημιουργηθούν τα αντίγραφα ασφαλείας που θα επιτρέπουν αφενός τη σχετικά άμεση επαναλειτουργία του συστήματος σε περίπτωση προβλήματος του υλικού ή και λογισμικού, αφετέρου, την επαναφορά των δεδομένων των χρηστών σε περίπτωση που για κάποιο λόγο αυτά αλλοιωθούν ή διαγραφούν.

Για τη δημιουργία του πρώτου από τα δύο αντίγραφα ασφαλείας θα πρέπει αρχικά να παραχθεί ένα «διπλοτύπο» της εγκατάστασης του λογισμικού από την κατάτμηση με σημείο προσάρτησης το ριζικό φάκελο (/) στην ελεύθερη κατάτμηση του δίσκου (χωρίς σημείο προσάρτησης). Ακολούθως θα πρέπει να εκτελεσθούν οι ενέργειες που αφορούν στις σχετικές τροποποιήσεις του λογισμικού εκκίνησης, ώστε σε περίπτωση κάποιου προβλήματος, ο εξυπηρετητής να είναι σε θέση να λειτουργήσει ξανά, μετά από μια απλή επανεκκίνηση του συστήματος και επιλογή χρήσης της εγκατάστασης ασφαλείας.

Αποθήκευση χαρακτηριστικών κατατμήσεων

Πριν την έναρξη της διαδικασίας λήψης του συγκεκριμένου αντιγράφου ασφαλείας, θα πρέπει να δημιουργηθεί ένας πίνακας με τα χαρακτηριστικά των κατατμήσεων του δίσκου, ώστε να είναι δυνατός ο ακριβής προσδιορισμός τους, στην περίπτωση που κατά τη διάρκεια της διαδικασίας δεν είμαστε σίγουροι για τις κατατμήσεις πηγής και προορισμού. Ο πίνακας χαρακτηριστικών των κατατμήσεων θα πρέπει να περιέχει τα παρακάτω δεδομένα και φυσικά, να δημιουργηθεί εκτός του συστήματος, με «χαρτί και μολύβι»:

device	Mount point	UUID
/dev/sda1	/	39c95aa1-63a7-4e7d-b075-67c017152314
/dev/sda2	/home	b149ca0a-b9e0-42de-a184-146d45d85c1b
/dev/sda3	swap	fa1fd355-95fe-4151-935d-f3c73e5e6ae4
/dev/sda4	-	172342a4-267b-4ec3-addf-1af423de70e1

Σημείωση: Εντολές κονσόλας, που μπορούν να βοηθήσουν στη συμπλήρωση του παραπάνω πίνακα είναι οι ακόλουθες:

```
blkid
df –h
cat /etc/fstab
```

```
cat /proc/mounts
```

Αφού ολοκληρωθεί η καταγραφή των χαρακτηριστικών των κατατμήσεων του δίσκου του συστήματος, ο εξυπηρετητής θα πρέπει να επανεκκινηθεί με χρήση ενός Live CD [99], ώστε το εμπλεκόμενο λογισμικό να μη χρησιμοποιείται στη διαδικασία δημιουργίας του αντιγράφου του. Χωρίς αυτό να είναι απαραίτητο, το Live CD που θα χρησιμοποιηθεί μπορεί να περιέχει το ίδιο λειτουργικό σύστημα που έχει εγκατασταθεί στον εξυπηρετητή (στον παρών οδηγό θα χρησιμοποιηθεί το Live CD του Debian GNU/Linux [100]). Σε κάθε περίπτωση, εκκινούμε το σύστημα χρησιμοποιώντας το Live CD και στη συνέχεια ανοίγουμε ένα παράθυρο τερματικού (στο παράδειγμα του οδηγού επιλέγοντας Applications => Accessories => Terminal), όπου και θα λάβει χώρα η διαδικασία λήψης του αντιγράφου ασφαλείας.

Δημιουργία αντιγράφου εγκατάστασης

Αρχικά θα πρέπει να επιβεβαιώσουμε ότι οι κατατμήσεις πηγής και προορισμού του αντιγράφου ασφαλείας είναι αυτές σωστές. Για να το πραγματοποιήσουμε αυτό, χρησιμοποιούμε τις εντολές του προηγούμενου βήματος και επαληθεύουμε ότι η πρώτη και τελευταία κατάτμηση (sda1 και sda4) έχουν ακριβώς τα ίδια χαρακτηριστικά με τις αντίστοιχες κατατμήσεις στον πίνακα χαρακτηριστικών των κατατμήσεων που δημιουργήσαμε παραπάνω.

Στη συνέχεια εκκινούμε τη διαδικασία, η οποία απαιτεί ειδικά δικαιώματα διαχείρισης του συστήματος.

Οδηγία: Αιτούμαστε την εκχώρηση «ανεβασμένων» δικαιωμάτων:

```
sudo -i
```

Οδηγία: Δημιουργούμε το φάκελο που θα χρησιμοποιηθεί για την προσάρτηση της κατάτμησης πηγής (sda1):

```
mkdir /media/sda1
```

Οδηγία: Προσαρτούμε την κατάτμηση πηγής (sda1) στο φάκελο που μόλις δημιουργήσαμε:

```
mount /dev/sda1 /media/sda1
```

Οδηγία: Δημιουργούμε το φάκελο που θα χρησιμοποιηθεί για την προσάρτηση της κατάτμησης προορισμού (sda4):

```
mkdir /media/sda4
```

Οδηγία: Προσαρτούμε την κατάτμηση προορισμού (sda4) στο φάκελο που μόλις δημιουργήσαμε:

```
mount /dev/sda4 /media/sda4
```

Οδηγία: Αντιγράφουμε την κατάτμηση πηγής (sda1) στην κατάτμηση προορισμού (sda4):

```
rsync -a /media/sda1/ /media/sda4/
```

Οδηγία: Επιβεβαιώνουμε ότι η δημιουργία του αντιγράφου ολοκληρώθηκε με επιτυχία (δε θα πρέπει να υπάρχουν διαφορές μεταξύ των αντίστοιχων αρχείων στις δύο κατατμήσεις):

```
diff -r /media/sda1/ /media/sda4/
```

Σημείωση: Μετά τη δημιουργία του αντιγράφου ασφαλείας το χρησιμοποιούμενο τμήμα της κατάτμησης προορισμού μπορεί να παρουσιάζει διαφορετικό μέγεθος από το αντίστοιχο της κατάτμησης πηγής. Αυτό δε θα πρέπει να μας ανησυχήσει! Το σύστημα δεσμεύει ένα **ποσοστό** (%) της εκάστοτε κατάτμησης για το διαχειριστή αυτού (root), συνεπώς σε μεγαλύτερες κατατμήσεις ο συγκεκριμένος χώρος είναι μεγαλύτερος.

File System TABle (fstab) προορισμού

Εάν το σύστημα απαιτηθεί να εκκινηθεί με χρήση του αντιγράφου ασφαλείας, η κατάτμηση που σε κανονικές συνθήκες δεν έχει σημείο προσάρτησης, απαιτείται να προσαρτηθεί στο ριζικό φάκελο, ώστε να λειτουργήσει στη θέση της αρχικής εγκατάστασης, διατηρώντας με την τελευταία κοινόχρηστο το φάκελο χρηστών (/home),

στην κατάτμηση sda2. Ο πίνακας του συστήματος αρχείων (fstab) του αντιγράφου ασφαλείας λοιπόν θα πρέπει να ενημερωθεί σχετικά, με μια απλή αντικατάσταση του UUID της κατάτμησης sda1 με το αντίστοιχο UUID της κατάτμησης sda4.

Οδηγία: Δημιουργούμε αντίγραφο ασφαλείας του υπάρχοντος πίνακα του συστήματος αρχείων της κατάτμησης sda4:

```
cp /media/sda4/etc/fstab /media/sda4/etc/fstab.backup
```

Οδηγία: Εάν το επιθυμούμε, επιβεβαιώνουμε τη χωρίς σφάλματα ολοκλήρωση της διαδικασίας λήψης του αντιγράφου ασφαλείας:

```
cmp /media/sda4/etc/fstab /media/sda4/etc/fstab.backup
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο fstab της κατάτμησης sda4:

```
vi /media/sda4/etc/fstab
```

Οδηγία: Αντικαθιστούμε το UUID της κατάτμησης sda1 με το αντίστοιχο UUID της κατάτμησης sda4, το οποίο μπορούμε να αντλήσουμε από τον πίνακα χαρακτηριστικών των κατατμήσεων που δημιουργήσαμε σε προηγούμενο βήμα:

```
  [...]
  # / was on /dev/sda1 during installation
  UUID=172342a4-267b-4ec3-addf-1af423de70e1 /               ext4
errors=remount-ro 0       1
  [...]
```

Αφαιρούμε τον οπτικό δίσκο με το Live CD και επανεκκινούμε το σύστημα, ώστε αυτό να λειτουργήσει όπως και αρχικά, από την πρωτότυπη εγκατάσταση του λογισμικού στην κατάτμηση sda1.

Ενημέρωση λογισμικού εκκίνησης

Μετά τα ανωτέρω βήματα, θα πρέπει να ενημερωθεί το λογισμικό εκκίνησης του συστήματος για την ύπαρξη του λειτουργικού συστήματος του αντιγράφου ασφαλείας στην κατάτμηση sda4.

Οδηγία: Εκτελούμε την εντολή αυτόματης ενημέρωσης του λογισμικού εκκίνησης:

```
update-grub
```

Οδηγία: Επειδή το αρχείο ρυθμίσεων του λογισμικού εκκίνησης του συστήματος είναι μόνο για ανάγνωση, τροποποιούμε κατάλληλα το δικαίωμα εγγραφής αυτού, ώστε να μπορέσουμε να το επεξεργαστούμε:

```
chmod o+w /boot/grub/grub.cfg
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο grub.cfg:

```
vi /boot/grub/grub.cfg
```

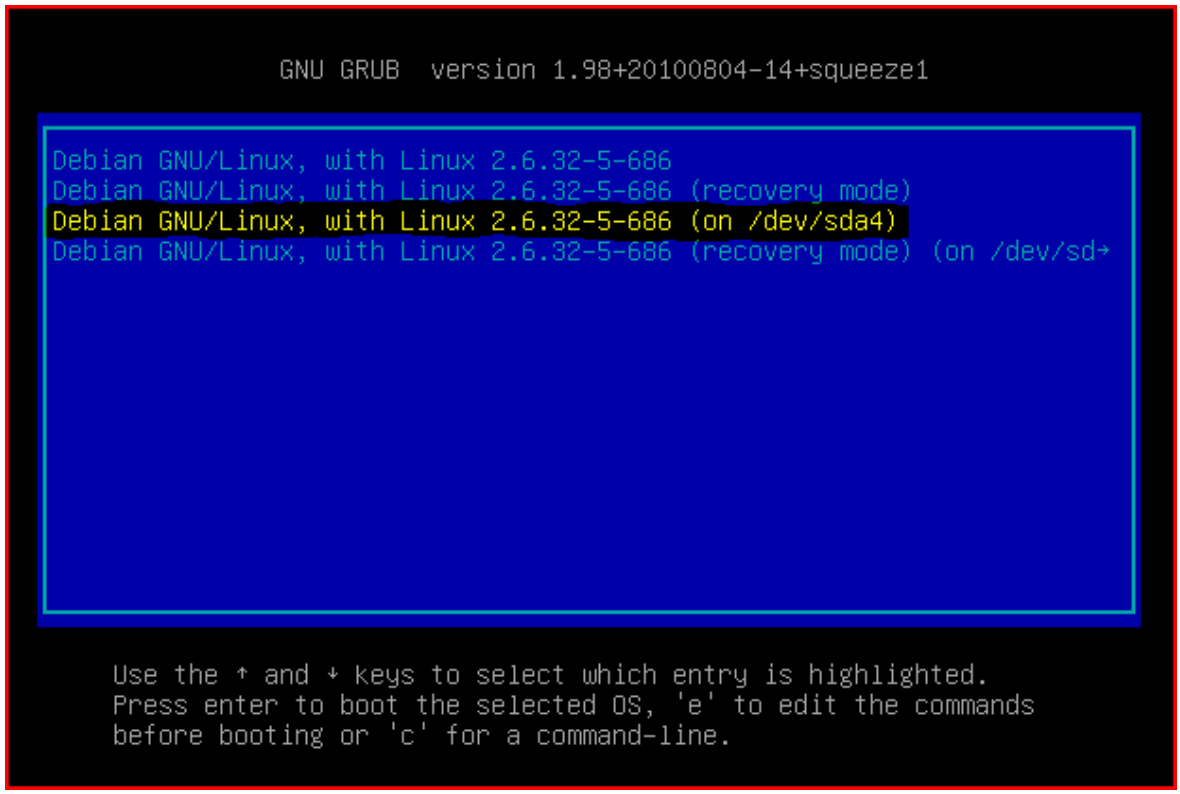
Οδηγία: Εντοπίζουμε την εγγραφή "Debian GNU/Linux, with Linux 2.6.32-5-686 (**on /dev/sda4**)" και μερικές γραμμές παρακάτω αντικαθιστούμε το UUID της κατάτμησης sda1, με αυτό της κατάτμησης sda4 (οι υπόλοιπες σχετικές εγγραφές που απαιτείται να ενημερωθούν, θα ενημερωθούν αυτόματα σε επόμενο βήμα του οδηγού):

```
  [...]
  menuentry "Debian GNU/Linux, with Linux 2.6.32-5-686 (on /dev/sda4)" {
          insmod part_msdos
          insmod ext2
          set root='(hd0,msdos4)'
          search --no-floppy --fs-uuid --set 172342a4-267b-4ec3-addf-
1af423de70e1
          linux /boot/vmlinuz-2.6.32-5-686 root=UUID=172342a4-267b-4ec3-
addf-1af423de70e1 ro quiet
          initrd /boot/initrd.img-2.6.32-5-686
  [...]
```

Οδηγία: Αφαιρούμε το δικαίωμα για τροποποίηση του αρχείου ρυθμίσεων του λογισμικού εκκίνησης του συστήματος:

```
chmod o-w /boot/grub/grub.cfg
```

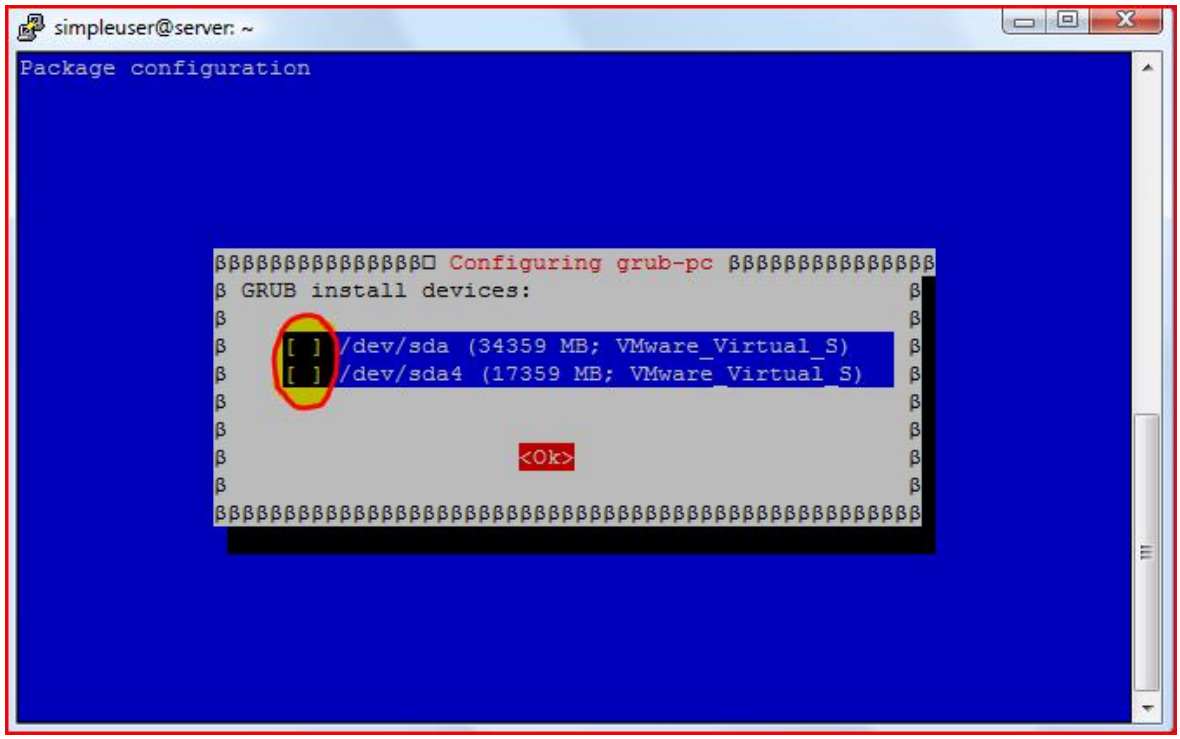
Οδηγία: Επανεκκινούμε το σύστημα και στο μενού επιλογών του λογισμικού εκκίνησης επιλέγουμε να χρησιμοποιήσουμε για την εκκίνηση του συστήματος, την κατάτμηση με το αντίγραφο ασφαλείας:



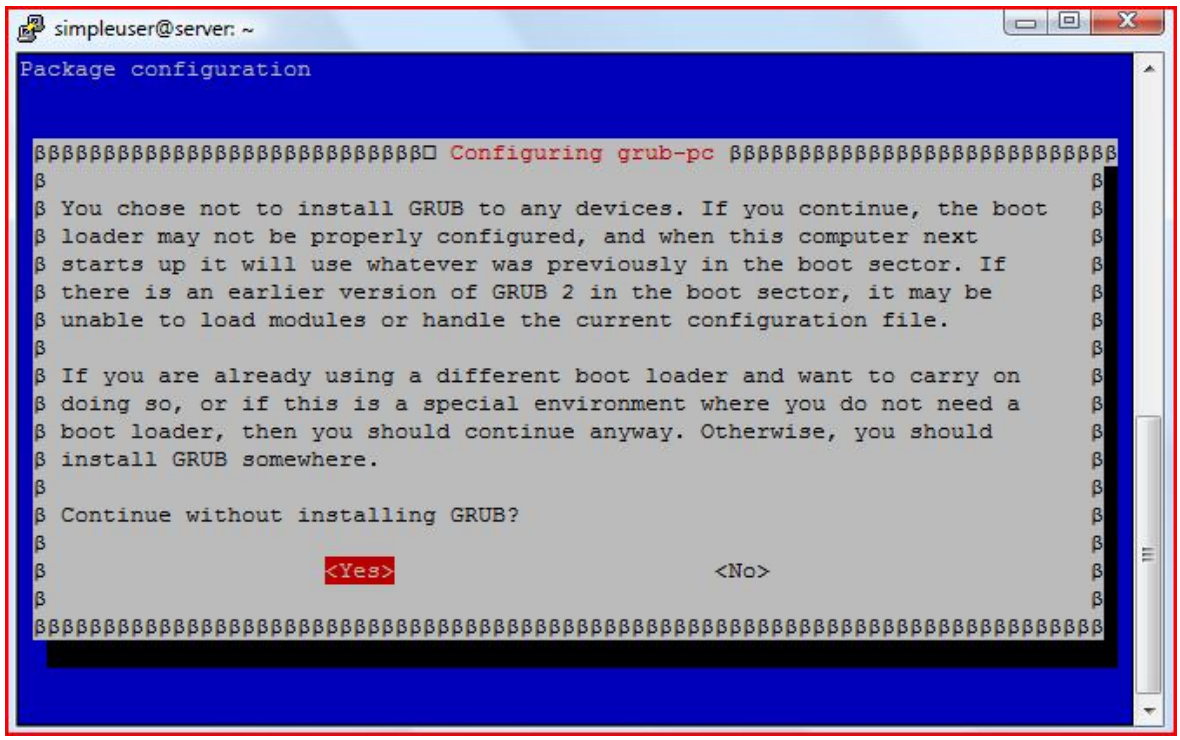
Οδηγία: Εκτελούμε την εντολή επαναρύθμισης του λογισμικού εκκίνησης:

```
dpkg-reconfigure grub-pc
```

Οδηγία: Αφήνουμε αμετάβλητες τις προεπιλεγμένες τιμές και μόνο στο τελευταίο παράθυρο ρυθμίσεων επιλέγουμε να ΜΗΝ εγκατασταθεί το λογισμικό εκκίνησης:



Οδηγία: Επιβεβαιώνουμε την πρόθεσή μας για μη εγκατάσταση του λογισμικού εκκίνησης, απαντώντας θετικά στη σχετική προειδοποίηση:



Οδηγία: Επανεκκινούμε το σύστημα και στο παράθυρο του λογισμικού εκκίνησης επιλέγουμε να χρησιμοποιήσουμε την αρχική εγκατάσταση στην κατάτμηση sda1 για την εκκίνηση του συστήματος. Στη συνέχεια εκτελούμε για μία ακόμη φορά την εντολή αυτόματης ενημέρωσης του λογισμικού εκκίνησης, ώστε να διορθωθούν αυτόματα τα εσφαλμένα UUID των δίσκων:

```
update-grub
```

Η διαδικασία δημιουργίας του αντιγράφου ασφαλείας των περιεχομένων της κατάτμησης που έχει ως σημείο προσάρτησης το ριζικό φάκελο (/) του συστήματος έχει πλέον ολοκληρωθεί και έτσι εξασφαλίζεται η ακεραιότητα του αρχειακού περιβάλλοντος του λειτουργικού συστήματος, καθώς και των εφαρμογών που έχουν χρησιμοποιηθεί από πιθανή δυσλειτουργία του υλικού ή του λογισμικού του εξυπηρετητή. Ο εξυπηρετητής έχει πλήρως ενημερωθεί για την ύπαρξη του συγκεκριμένου αντιγράφου ασφαλείας και έτσι, κατά την επιχειρησιακή χρήση του εξυπηρετητή η κατάτμηση που θα πρέπει να χρησιμοποιείται είναι η «πρωτότυπη» κατάτμηση sda1 και μόνο στην περίπτωση προβλήματος θα πρέπει να επιλέγεται το αντίγραφο ασφαλείας στην κατάτμηση sda4.

Είναι αυτονόητο, ότι η παραπάνω διαδικασία λήψης του αντιγράφου ασφαλείας θα πρέπει να επαναλαμβάνεται μετά από σημαντικές αλλαγές που τυχόν λάβουν χώρα στο λογισμικό του εξυπηρετητή, ώστε να διατηρείται ενημερωμένο σε σχέση με αυτό, το αντίγραφο ασφαλείας του συστήματος. Βέβαια, πριν από την εκάστοτε λήψη του αντιγράφου ασφαλείας θα πρέπει να πιστοποιείται η καλή λειτουργία του εξυπηρετητή μετά την οποιαδήποτε τροποποίησή του.

Δημιουργία αντιγράφου ασφαλείας φακέλου χρηστών

Στο παραπάνω αντίγραφο ασφαλείας δεν έχουν συμπεριληφθεί τα περιεχόμενα του φακέλου χρηστών (/home), ο οποίος έχει επιλεγεί να χρησιμοποιείται ως σημείο προσάρτησης ξεχωριστής κατάτμησης, ώστε να μπορεί να είναι κοινόχρηστος μεταξύ της πρωτότυπης εγκατάστασης του «βασικού» λογισμικού του συστήματος και του παραπάνω αντιγράφου ασφαλείας αυτής. Ο φάκελος αυτός είναι αναμενόμενο ότι θα υπόκειται σε συχνότερες τροποποιήσεις σε σχέση με το υπόλοιπο λογισμικό του εξυπηρετητή, συνεπώς

η λήψη αντιγράφων ασφαλείας του είναι επιβεβλημένο να γίνεται αφενός σε συχνότερα χρονικά διαστήματα, αφετέρου πλήρως αυτοματοποιημένα.

Καθορισμός πολιτικής

Πριν από την έναρξη λήψης αντιγράφων ασφαλείας του φακέλου χρηστών, θα πρέπει να καθοριστούν όλες οι παράμετροι που αφορούν στη συγκεκριμένη διαδικασία και που συνολικά αποτελούν την πολιτική λήψης αντιγράφων ασφαλείας του εν λόγω φάκελου. Στις πολιτικές λήψης τέτοιων αντιγράφων ασφαλείας συνήθως περιλαμβάνονται περισσότεροι από έναν τύποι αντιγράφων, οι οποίοι μπορεί να λαμβάνονται ημερησίως, εβδομαδιαίως, μηνιαίως ή ακόμη και ετησίως. Τα αντίγραφα αυτά μπορεί να είναι πλήρη/γενικά και να λαμβάνονται επί του συνόλου του περιεχομένου του φακέλου χρηστών (full backups), ή μερικά/ειδικά και να λαμβάνονται με βάση τις διαφοροποιήσεις των προς αντιγραφή αρχείων από το τελευταίο ειδικό ή γενικό αντίγραφο ασφαλείας (incremental ή differential backups αντίστοιχα) [101, 102]. Τα αντίγραφα ασφαλείας, ανεξαρτήτως του τύπου ή της συχνότητας λήψης τους, μπορούν να λαμβάνονται σε αποθηκευτικό μέσο του ίδιου ή διαφορετικού πληροφοριακού συστήματος (ακόμη και απομακρυσμένου, μέσω του διαδικτύου). Τέλος, για εξοικονόμηση αποθηκευτικού χώρου, τα αντίγραφα συνηθίζεται να λαμβάνονται «κυκλικά», με το πλέον νεότερο να αντικαθιστά περιστροφικά το πλέον παλαιότερο.

Με βάση τη διαμέριση του σκληρού δίσκου του εξυπηρετητή του παρόντος οδηγού, καθώς και του μεγέθους αλλά και της χρήσης των κατατμήσεων αυτού, έχουν επιλεγεί για το φάκελο χρηστών του συστήματος να δημιουργούνται ημερήσια incremental αντίγραφα ασφαλείας με διάστημα περιστροφής ένα μήνα, καθώς και μηνιαία πλήρη αντίγραφα ασφαλείας με διάστημα περιστροφής ένα χρόνο. Κάθε πρώτη του μήνα θα δημιουργείται ένα πλήρες αντίγραφο, το οποίο και θα περιλαμβάνει όλα τα περιεχόμενα του φακέλου χρηστών. Το κάθε μηνιαίο αντίγραφο θα διατηρείται για ένα χρόνο και θα διαγράφεται αυτόματα κατά τη διαδικασία δημιουργίας του αντιγράφου ασφαλείας του ίδιου μήνα του επομένου έτους. Παρομοίως, κάθε ημέρα (εξαιρουμένης της πρώτης ημέρας εκάστοτε μηνός κατά την οποία θα λαμβάνεται το πλήρες αντίγραφο ασφαλείας) θα δημιουργείται ένα ειδικό αντίγραφο ασφαλείας, το οποίο και θα περιλαμβάνει μόνο τα περιεχόμενα του φακέλου χρηστών που έχουν τροποποιηθεί από τη λήψη του πλέον πρόσφατου αντιγράφου ασφαλείας. Το κάθε ημερήσιο αντίγραφο θα διατηρείται για ένα μήνα και θα διαγράφεται

αυτόματα κατά τη διαδικασία δημιουργίας του αντιγράφου ασφαλείας της ίδιας ημέρας του επομένου μήνα.

Με τη συγκεκριμένη πολιτική λήψης αντιγράφων ασφαλείας περιορίζεται σημαντικά ο συνολικός αποθηκευτικός χώρος που απαιτείται για την εν λόγω υλοποίηση, αυξάνεται όμως (πιθανώς) ο χρόνος που θα απαιτηθεί για την ανάκτηση των δεδομένων. Η αύξηση του χρονικού διαστήματος ανάκτησης των δεδομένων εξαρτάται από την ημέρα του μήνα κατά την οποία θα προκύψει η απαίτηση, μιας και για την επανάκτηση του περιεχομένου του φακέλου χρηστών είναι απαραίτητος ο συνδυασμός του τελευταίου πλήρους αντιγράφου ασφαλείας, καθώς και όλων των ειδικών από το τελευταίο πλήρες έως την ημερομηνία που προκύπτει η απαίτηση. Συνεπώς, εάν απαιτηθεί η επανάκτηση του περιεχομένου του φακέλου χρηστών την πρώτη του μήνα, θα χρειαστεί μόνο το τελευταίο πλήρες αντίγραφο ασφαλείας. Εάν η ίδια απαίτηση προκύψει την τέταρτη ημέρα του μήνα, θα χρειαστεί το τελευταίο πλήρες αντίγραφο ασφαλείας, καθώς και τα ειδικά αντίγραφα της δεύτερης και τρίτης ημέρας. Αντίστοιχα, για την τελευταία ημέρα του μήνα θα απαιτηθεί το τελευταίο πλήρες, καθώς και όλα τα ειδικά αντίγραφα ασφαλείας που έχουν ληφθεί για το συγκεκριμένο μήνα.

Σημείωση: Η πολιτική λήψης αντιγράφων ασφαλείας που έχει επιλεγεί να χρησιμοποιηθεί στο παράδειγμα του οδηγού δε θα πρέπει να παίξει καθοριστικό ρόλο στον προσδιορισμό της πολιτικής της εκάστοτε υλοποίησης, μιας και η τελευταία θα πρέπει να είναι εστιασμένη καθαρά στις ανάγκες της εκάστοτε περίστασης.

Δημιουργία δέσμης ενεργειών κελύφους - προγραμματισμός εργασίας

Η διαδικασία που απαιτείται για την υλοποίηση της πολιτικής λήψης αντιγράφων ασφαλείας του φακέλου χρηστών που περιγράφηκε παραπάνω περιλαμβάνει τη δημιουργία ενός προσωρινού φακέλου, την προσάρτηση της κατάτμησης προορισμού του αντιγράφου ασφαλείας στον προσωρινό φάκελο (στο παράδειγμα του οδηγού η κατάτμηση sda4), τη λήψη του κατάλληλου αντιγράφου ανάλογα με την τρέχουσα μέρα του μήνα, την αποπροσάρτηση της κατάτμησης προορισμού και τέλος, τη διαγραφή του προσωρινού φακέλου. Όλες οι σχετικές ενέργειες είναι δυνατό να πραγματοποιηθούν με απλές εντολές τερματικού και έτσι, η όλη διαδικασία δύναται να συμπεριληφθεί σε ένα εκτελέσιμο αρχείο δέσμης ενεργειών κελύφους.

Το συγκεκριμένο αρχείο δέσμης ενεργειών κελύφους είναι δυνατό να ενεργοποιείται μέσα από μια ημερήσια προγραμματισμένη εργασία (cron job) [103], απλοποιώντας σε μεγάλο βαθμό την αυτοματοποίηση της διαδικασίας. Οι προγραμματισμένες εργασίες στο λειτουργικό σύστημα Debian GNU/Linux καθορίζονται στο αρχείο crontab (CRON TABle file), το οποίο βρίσκεται στο φάκελο /etc/ και εξ' ορισμού περιέχει τέσσερις προγραμματισμένες εργασίες:

- **ü** μια ωριαία, που έχει προγραμματιστεί να εκτελείται κάθε ώρα στις HH:17
- **ü** μια ημερήσια, που έχει προγραμματιστεί να εκτελείται κάθε μέρα στις 06:25
- **ü** μια εβδομαδιαία, που έχει προγραμματιστεί να εκτελείται κάθε έβδομη ημέρα της εβδομάδος στις 06:47
- **ü** μια μηνιαία, που έχει προγραμματιστεί να εκτελείται κάθε πρώτη ημέρα του μήνα στις 06:52.

Οι εργασίες αυτές είναι στην πραγματικότητα φάκελοι, μέσα στους οποίους ο χρήστης μπορεί να προσθέσει τα δικά του αρχεία με τις ενέργειες που επιθυμεί να συμπεριλάβει στην εκάστοτε προγραμματισμένη εργασία.

Έτσι, για τη λήψη των αντιγράφων ασφαλείας του φακέλου χρηστών στον οδηγό της παρούσας εργασίας θα χρησιμοποιηθεί ο φάκελος ημερησίων προγραμματισμένων εργασιών, όπου θα προστεθεί ένα νέο αρχείο με το όνομα homefolderbackup.cron, το οποίο και θα περιέχει τη δέσμη ενεργειών κελύφους που απαιτείται για την ολοκλήρωση της σχετικής διαδικασίας.

Οδηγία: Δημιουργούμε ένα νέο αρχείο με το όνομα homefolderbackup.cron στο φάκελο ημερήσιων προγραμματισμένων εργασιών /etc/cron.daily:

```
touch /etc/cron.daily/homefolderbackup.cron
```

Οδηγία: Ανοίγουμε για επεξεργασία το αρχείο που μόλις δημιουργήσαμε:

```
vi /etc/cron.daily/homefolderbackup.cron
```

Οδηγία: Προσθέτουμε στο αρχείο τις παρακάτω γραμμές, φροντίζοντας (εάν αυτό απαιτείται) να τροποποιήσουμε κατάλληλα τις παραμέτρους που αφορούν:

- στη διαδρομή της «συσκευής» της κατάτμησης, στην οποία θα τηρούνται τα αντίγραφα ασφαλείας (/dev/sda4 στο παράδειγμα του οδηγού)
- στο όνομα του φακέλου μέσα στον οποίο θα τηρούνται τα αρχεία με τα αντίγραφα ασφαλείας
- στο πρόθεμα των ονομάτων αρχείων για τα ημερήσια και τα μηνιαία αντίγραφα ασφαλείας:

```
  #!/bin/sh
  set –e
  MountDev="/dev/sda4"
  MountDir=$(mktemp -d)
  BackUpThisDir="/home"
  BackUpDir="$MountDir/backups"
  DayOfMonth=$(date "+%d")
  MonthOfYear=$(date "+%m")
  DailyBackUpFileName="$BackUpDir/daily-$DayOfMonth.tar.xz"
  MonthlyBackUpFileName="$BackUpDir/monthly-$MonthOfYear.tar.xz"
  mount "$MountDev" "$MountDir"
  if [ ! -d "$BackUpDir" ]
  then
      mkdir "$BackUpDir"
  fi
  if [ -f "$BackUpDir/DateOfLastBackUp" ]
  then
      DateOfLastBackUp=$(cat "$BackUpDir/DateOfLastBackUp")
      if [ "${DateOfLastBackUp%-*}"  = "$(date "+%Y-%m")" ]
      then
            PerformDaily=true
      fi
  fi
  if [ -n "$PerformDaily" ]
  then
    echo "Daily backup started on $(date "+%F %T")." >>
"$BackUpDir/LogOfLastBackUp"
    tar --one-file-system --newer "$DateOfLastBackUp" -cJf
"$DailyBackUpFileName" -C "$BackUpThisDir" .
```

```
  else
    echo "Monthly backup started on $(date "+%F %T")." >>
"$BackUpDir/LogOfLastBackUp"
    tar --one-file-system -cJf "$MonthlyBackUpFileName" -C
"$BackUpThisDir" .
  fi
  echo "$(date "+%F")" > "$BackUpDir/DateOfLastBackUp"
  echo "Succesfully finished backup process on $(date "+%F %T")." >>
"$BackUpDir/LogOfLastBackUp"
  umount "$MountDir"
  rmdir "$MountDir"
```

Οδηγία: Τροποποιούμε τα δικαιώματα του αρχείου, ώστε αυτό να είναι εκτελέσιμο:

```
  chmod 755 /etc/cron.daily/homefolderbackup.cron
```

Μετά τις παραπάνω ενέργειες, στις 06:25 καθημερινά θα δημιουργείται ένας προσωρινός φάκελος με τυχαίο όνομα της μορφής tmp.xs4Po6LuM3, στη διαδρομή /tmp/, ο οποίος αμέσως μετά τη δημιουργία του θα χρησιμοποιείται ως σημείο για να προσαρτηθεί η κατάτμηση, στην οποία θα αποθηκεύονται τα αντίγραφα ασφαλείας. Στη συνέχεια, θα ελέγχεται η ύπαρξη του φακέλου όπου έχει καθοριστεί να τοποθετούνται τα αντίγραφα ασφαλείας και σε περίπτωση μη ύπαρξής του, αυτός θα δημιουργείται αυτόματα. Ακολούθως, θα ελέγχεται (εάν αυτή υπάρχει) η ημερομηνία πραγματοποίησης του τελευταίου αντιγράφου ασφαλείας από το αρχείο καταγραφής της συγκεκριμένης πληροφορίας (DateOfLastBackUp) και ανάλογα θα λαμβάνεται είτε μηνιαίο είτε ημερήσιο αντίγραφο ασφαλείας (την πρώτη φορά που θα εκτελεστεί η δέσμη ενεργειών, καθώς και την πρώτη ημέρα κάθε μήνα θα ληφθεί μόνο μηνιαίο και όχι ημερήσιο αντίγραφο). Για την ημερομηνία και ώρα έναρξης και πέρατος της διαδικασίας, θα ενημερώνεται το αρχείο LogOfLastBackUp στο φάκελο όπου έχουν οριστεί να τοποθετούνται τα αντίγραφα ασφαλείας. Μετά την ολοκλήρωση της λήψης του αντιγράφου ασφαλείας, θα ενημερώνεται το αρχείο DateOfLastBackUp για την ημερομηνία εκτέλεσης της διαδικασίας και θα αποπροσαρτάται η κατάτμηση προορισμού των αντιγράφων. Τέλος, θα διαγράφεται ο προσωρινός φάκελος που χρησιμοποιήθηκε ως σημείο προσάρτησης της κατάτμησης των αντιγράφων ασφαλείας.

Επίλογος

Με την ολοκλήρωση των αμέσως προηγούμενων ενεργειών που απαιτούνται για την αυτοματοποιημένη δημιουργία του αντιγράφου ασφαλείας του φακέλου χρηστών έχει ολοκληρωθεί και ο οδηγός της παρούσας πτυχιακής εργασίας. Η διαδικασία εγκατάστασης και παραμετροποίησης ενός Linux Server για την υποστήριξη και παροχή με ασφάλεια υπηρεσιών WEB έχει καλυφθεί πλήρως, ενώ σε όλα τα βήματα του οδηγού έχουν αδιάλειπτα παρατεθεί παραπομπές στη σχετική (κατά κύριο λόγο διαδικτυακή) βιβλιογραφία και έτσι εύκολα μπορεί κανείς να αναζητήσει επιπλέον αναφορές σε σχετικά σημεία ενδιαφέροντος.

Παρά τη σχετικά μεγάλη έκταση της παρούσας πτυχιακής εργασίας, υπάρχουν περιοχές στις οποίες μελλοντικά θα μπορούσε να γίνει επιπρόσθετη εμβάθυνση. Επιγραμματικά αναφέρονται οι περιπτώσεις:

- υλοποίησης με χρήση περισσοτέρων του ενός εξυπηρετητή, για την οποία θα πρέπει να εξεταστούν παράμετροι όπως ο διαμοιρασμός των υπηρεσιών, καθώς και ο καταμερισμός του φόρτου εργασίας μεταξύ των εμπλεκομένων πληροφοριακών συστημάτων

- σύγκρισης αποδοτικότητας των περιπτώσεων υλοποίησης με χρήση διαφορετικού, καθ' όλα συμβατού λογισμικού, για την παροχή των ίδιων υπηρεσιών (πχ σύγκριση των εξυπηρετητών Παγκοσμίου Ιστού Apache και nginx με βοήθεια του ιστοτόπου http://www.loadimpact.com)

- περαιτέρω επόπτευσης του εξυπηρετητή, μέσα από λογισμικό που να υποστηρίζει την αυτόματη επανεκκίνηση των υπηρεσιών που παρουσιάζουν πρόβλημα, ή που λόγω προβλήματος έχουν ήδη τερματιστεί (πχ munin και monit)

- περαιτέρω επόπτευσης του εξυπηρετητή, μέσα από λογισμικό που να υποστηρίζεται από υπερφορητές συσκευές, όπως για παράδειγμα τα κινητά τηλέφωνα με λειτουργικό σύστημα Android και η σχετική εφαρμογή ISPConfig Monitor App For Android

- περιγραφής, ανάλυσης και σύγκρισης διαφορετικών πολιτικών διαμέρισης και προσάρτησης των αποθηκευτικών μέσων του εξυπηρετητή, με στόχο τη βέλτιστη λειτουργικότητα, αποδοτικότητα αλλά και μέγιστη ασφάλεια του συστήματος

- περιγραφής και ανάλυσης της διαδικασίας λεπτομερούς εξέτασης του επιπέδου ασφαλείας του συστήματος, με χρήση λογισμικού εξομοίωσης κακόβουλης χρήσης [104]

- επέκτασης των παρεχομένων υπηρεσιών σε επιπρόσθετους διαδικτυακούς τομείς (πχ ροής δεδομένων, εξυπηρέτησης εφαρμογών κτλ)

Κλείνοντας την παρούσα πτυχιακή εργασία θα ήθελα να θυμίσω στον αναγνώστη ότι ο διαδικτυακός εξυπηρετητής, όπως και κάθε άλλο πληροφοριακό σύστημα που είναι προσβάσιμο, είτε φυσικά, είτε διαδικτυακά, δε θα πρέπει να θεωρείται ασφαλής. Οι κακόβουλοι χρήστες θα επιδιώκουν σε συνεχή βάση να εκμεταλλευτούν σχετικές αδυναμίες, συνεπώς, η διατήρηση ενός συστήματος πλήρως επικαιροποιημένου, αλλά και βέλτιστα παραμετροποιημένου, θα πρέπει να αποτελεί για τον υπεύθυνό του αδιάκοπη επιδίωξη. Σε κάθε περίπτωση, εύχομαι ολόψυχα «καλή επιτυχία»!

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΠΑΡΑΠΟΜΠΕΣ

[1] http://portal.kathimerini.gr/4dcgi/_w_articles_kathextra_100008_14/04/2008_229340 (24-11-2011, 10:41)

[2] http://www.observatory.gr/files/meletes/A100526_Προφίλ χρηστών internet 2010.pdf (24-11-2011, 10:30)

[3] http://el.wikipedia.org/wiki/Μοντέλο_πελάτη-διακομιστή (22-02-2012, 10:05)

[4] http://en.wikipedia.org/wiki/Web_server (22-02-2012, 10:19)

[5] http://el.wikipedia.org/wiki/Ελεύθερο_λογισμικό (22-02-2012, 11:25)

[6] http://foss.ntua.gr/wiki/index.php/Ελεύθερο_Λογισμικό-Λογισμικό_Ανοικτού_Κώδικα (22-02-2012, 12:52)

[7] http://members.apex-internet.com/sa/windowslinux/04-cost.html (22-02-2012, 16:38)

[8] http://open-source.gbdirect.co.uk/migration/benefit.html#cost (22-02-2012, 17:51)

[9] von Engelhardt, S (2008), “Intellectual property rights and ex-post transaction costs: the case of open and closed source software”.

[10] http://www.biznix.org/whylinux/windows/zdnet.htm (23-02-2012, 08:10)

[11] http://www.slideshare.net/madhugr/productivity-gains-using-open-source-products (23-02-2012, 09:22)

[12] ACM Transactions on Software Engineering and Methodology (2002) Volume: 11, Issue: 3, Publisher: ACM, Pages: 309-346

[13] http://ifipwg213.org/system/files/mockusapache.pdf (23-02-2012, 11:05)

[14] https://www.virtualbox.org (23-02-2012, 18:13)

[15] http://en.wikipedia.org/wiki/Web_hosting_control_panel (29-02-2012, 15:12)

[16] http://en.wikipedia.org/wiki/Comparison_of_web_hosting_control_panels (25-11-2011, 09:29)

[17] http://www.howtoforge.com/forums/showpost.php?p=16207&postcount=2 (29-02-2012, 17:32)

[18] http://www.howtoforge.com/forums/archive/index.php/t-2680.html (29-02-2012, 17:49)

[19] http://www.ispconfig.org/releases/ispconfig-3-0-4-released (29-02-2012, 18:56)

[20] http://www.ispconfig.org/ispconfig-3 (29-02-2012, 19:29)

[21] http://www.debian.org/News/2012/20120128 (01-03-2012, 09:02)

[22] http://www.debian.org/CD/netinst (01-03-2012, 12:17)

[23] http://ftp.acc.umu.se/debian-cd/6.0.4/i386/iso-cd/debian-6.0.4-i386-netinst.iso (01-03-2012, 16:11)
[24] http://d-i.alioth.debian.org/manual/el.i386/install.el.txt (02-03-2012, 08:06)
[25] http://d-i.alioth.debian.org/manual/el.i386/index.html (02-03-2012, 08:07)
[26] http://www.debian.org/releases/stable/debian-installer/#errata (02-03-2012, 09:42)
[27] http://wiki.debian.org/Locale (04-12-2011, 13:52)
[28] http://lists.debian.org/debian-boot/2007/11/msg00312.html (04-12-2011, 14:06)
[29] http://en.wikipedia.org/wiki/Ext4 (07-12-2011, 20:36)
[30] http://d-i.alioth.debian.org/manual/el.i386/install.el.txt (07-12-2011, 15:57)
[31] http://www.debian.org/doc/manuals/apt-howto/ch-basico.en.html (12-12-2011, 12:23)
[32] http://www.debian.org/mirror/mirrors_full (12-12-2011, 12:18)
[33] http://comments.gmane.org/gmane.linux.debian.user/390797 (13-12-2011, 09:11)
[34] http://www.debian-administration.org/articles/254 (13-12-2011, 09:44)
[35] http://princessleia.com/plug/2008-JP_bash_vs_dash.pdf (13-12-2011, 17:57)
[36] http://www.debian.org/doc/manuals/system-administrator/ch-sysadmin-time.html (16-12-2011, 07:21)
[37] http://wiki.debian.org/DateTime [16-12-2011/08:40]
[38] http://articles.slicehost.com/2010/11/8/using-ntp-to-sync-time-on-debian (16-12-2011, 09:33)
[39] http://www.postfix.org/start.html (19-12-2011, 09:32)
[40] http://www.courier-mta.org/ (19-12-2011, 07:12)
[41] http://packages.debian.org/testing/mail/getmail4 (19-12-2011, 10:22)
[42] http://packages.debian.org/squeeze/libsasl2-2 (18-12-2011, 19:05)
[43] http://packages.debian.org/squeeze/mysql-server (18-12-2011, 12:08)
[44] http://packages.debian.org/squeeze/mysql-client (18-12-2011, 12:09)
[45] http://rkhunter.cvs.sourceforge.net/viewvc/rkhunter/rkhunter/files/FAQ (17-12-2011, 11:48)
[46] http://en.wikipedia.org/wiki/GNU_Binutils (17-12-2011, 11:35)
[47] http://packages.debian.org/squeeze/binutils (17-12-2011, 10:43)
[48] http://www.amavis.org (20-12-2011, 09:52)
[49] http://spamassassin.apache.org (20-12-2011, 08:30)
[50] http://en.wikipedia.org/wiki/SpamAssassin (20-12-2011, 09:20)
[51] http://www.clamav.net/lang/en (20-12-2011, 10:23)
[52] http://en.wikipedia.org/wiki/Clam_AntiVirus (20-12-2011, 10:51)

[53] http://httpd.apache.org (20-12-2011, 13:18)

[54] http://www.php.net (20-12-2011, 13:32)

[55] http://el.wikipedia.org/wiki/PHP (20-12-2011, 13:59)

[56] http://www.phpmyadmin.net/home_page/index.php (20-12-2011, 14:11)

[57] http://en.wikipedia.org/wiki/PhpMyAdmin (20-12-2011, 14:28)

[58] http://www.fastcgi.com (20-12-2011, 14:49)

[59] http://en.wikipedia.org/wiki/FastCGI (20-12-2011, 15:13)

[60] http://httpd.apache.org/docs/2.0/suexec.html (20-12-2011, 15:22)

[61] http://en.wikipedia.org/wiki/SuEXEC (20-12-2011, 15:40)

[62] http://pear.php.net (21-12-2011, 10:21)

[63] http://mcrypt.sourceforge.net (21-12-2011, 11:37)

[64] http://en.wikipedia.org/wiki/Mcrypt (21-12-2011, 12:25)

[65] http://www.pureftpd.org/project/pure-ftpd (21-12-2011, 17:21)

[66] http://en.wikipedia.org/wiki/Pure-FTPd (21-12-2011, 17:36)

[67] http://en.wikipedia.org/wiki/Disk_quota (21-12-2011, 19:02)

[68] http://www.isc.org/software/bind (22-12-2011, 09:10)

[69] http://en.wikipedia.org/wiki/BIND (22-12-2011, 09:45)

[70] http://packages.debian.org/squeeze/dnsutils (22-12-2011, 09:52)

[71] http://n0rp.chemlab.org/vlogger (10-01-2012, 09:15)

[72] http://www.webalizer.org (10-01-2012, 09:38)

[73] http://en.wikipedia.org/wiki/Webalizer (10-01-2012, 09:52)

[74] http://awstats.sourceforge.net (10-01-2012, 10:13)

[75] http://en.wikipedia.org/wiki/AWStats (10-01-2012, 10:29)

[76] http://packages.debian.org/sid/geoip-database (10-01-2012, 10:42)

[77] http://www.fail2ban.org/wiki/index.php/Main_Page (12-01-2012, 10:09)

[78] http://en.wikipedia.org/wiki/Fail2ban (12-01-2012, 11:23)

[79] http://en.wikipedia.org/wiki/Regular_expression (12-01-2012, 15:51)

[80] http://www.regular-expressions.info (12-01-2012, 16:10)

[81] http://roundcube.net (13-01-2012, 10:04)

[82] http://en.wikipedia.org/wiki/Roundcube (13-01-2012, 10:09)

[83] http://people.debian.org/~seanius/policy/dbconfig-common-using.html (13-01-2012, 12:31)

[84] http://en.wikipedia.org/wiki/Secure_Shell (14-03-2012, 09:01)

[85] http://el.wikipedia.org/wiki/Telnet (14-03-2012, 09:26)

[86] http://www.unix.com/man-page/Linux/1/ssh (15-03-2012, 11:19)
[87] http://en.wikipedia.org/wiki/Comparison_of_SSH_clients (15-03-2012, 12:44)
[88] http://www.employees.org/~satch/ssh/faq/ssh-faq-1.html (15-03-2012, 13:27)
[89] http://en.wikipedia.org/wiki/Hardening_%28computing%29 (15-03-2012, 18:58)
[90] http://www.openspf.org/Introduction (17-03-2012, 08:28)
[91] http://el.wikipedia.org/wiki/Επιθέσεις_άρνησης_υπηρεσιών (26-03-2012, 10:41)
[92] http://el.wikipedia.org/wiki/Firewall (26-03-2012, 11:53)
[93] http://nmap.org (26-03-2012, 12:06)
[94] http://packages.debian.org/sid/bastille (26-03-2012, 13:17)
[95] http://wiki.debian.org/iptables (26-03-2012, 13:18)
[96] http://en.wikipedia.org/wiki/Reverse_DNS_lookup (27-03-2012, 08:38)
[97] http://el.wikipedia.org/wiki/SMTP (30-03-2012, 09:43)
[98] http://www.postfix.org/uce.html (30-03-2012, 11:01)
[99] http://en.wikipedia.org/wiki/Live_CD (05-04-2012, 11:25)
[100] http://wiki.debian.org/LiveCD (05-04-2012, 11:32)
[101] http://www.backup.info/difference-between-full-differential-and-incremental-backup (08-04-2012, 11:04)
[102] http://support.microsoft.com/kb/136621 (08-04-2012, 11:05)
[103] http://en.wikipedia.org/wiki/Cron (09-04-2012, 13:19)
[104] http://www.softwareqatest.com/qatweb1.html#SECURITY (29-04-2012, 11:34)