



**Πανεπιστήμιο Πειραιώς**

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ “Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων”

Κατεύθυνση “Ασφάλεια Ψηφιακών Συστημάτων”

*Μεταπτυχιακή Διπλωματική Εργασία*

***Ανάπτυξη Ασφαλούς Πλατφόρμας Ηλεκτρονικής Μάθησης - Moodle, για Αξιολόγηση Στελεχών του Στρατού Ξηράς***

***Μαρίνος Ν. Ευστράτιος, ΜΤΕ 14015***

***Επιβλέπων: κ. Λαμπρινουδάκης Κωνσταντίνος, Αναπληρωτής Καθηγητής***

***Πειραιάς, Μάρτιος 2015***

*...στην οικογένεια μου, και σε όσους έκαναν υπομονή 1,5 χρόνο.*



*Ευχαριστίες...*

*Θα ήθελα να ευχαριστήσω τον επιβλέποντα αναπληρωτή καθηγητή κ.Κ Λαμπρινουδάκη για τις πολύτιμες συμβουλές που μου παρείχε στην ολοκλήρωση της εργασίας μου.*

*Ιδιαίτερες ευχαριστίες στον Ανχη (ΕΠ) Σιάνα Παναγιώτη, για την καθοδήγηση, τη βοήθεια και την άμεση απόκρισή του καθ' όλη τη διάρκεια, της συνεργασίας μας.*

*Τέλος εκφράζω την ευγνωμοσύνη μου στην σύζυγο μου Μαρία, στους φίλους και τους συνάδελφους μου, για την υποστήριξή τους σε όλη την διάρκεια των μεταπτυχιακών μου σπουδών.*



## Πίνακας Περιεχομένων

Περίληψη .....	7
Abstract .....	8
1. Εισαγωγή.....	9
1.1 Σκοπός.....	9
1.2 Δομή.....	9
1.3 Ηλεκτρονική μάθηση .....	10
2. Εγχειρίδιο Εγκατάστασης .....	13
2.1 Προετοιμασία Συστήματος.....	13
2.1.1 Λειτουργικό Σύστημα.....	14
2.1.2 Βοηθητικά Προγράμματα .....	14
2.1.3 Εγκατάσταση του LAMP server.....	15
2.1.4 Εγκατάσταση του FTP Server .....	17
2.2 Πλατφόρμα Moodle.....	18
2.2.1 Δημιουργία Βάσης .....	18
2.2.2 Δημιουργία Data Directory.....	19
2.2.3 Εγκατάσταση Moodle .....	19
2.2.4 Δημιουργία Λογαριασμού Admin.....	26
2.2.5 Τελικές Ρυθμίσεις .....	27
2.3 Ασφαλίζοντας το Περιεχόμενο .....	29
2.3.1 IP Blocker.....	29
2.3.2 Site Policies .....	29
2.3.3 HTTP Security .....	31
2.3.4 Notification .....	32
2.3.5 Antivirus .....	32
2.3.6 Firewall.....	33
3. Δημιουργία μαθήματων .....	34
3.1 Εισαγωγή.....	34
3.2 Ενότητες Μαθήματος: Ασφάλεια Δικτύων Ηλεκτρονικών Υπολογιστών .....	35
3.2.1 Ενότητα: Δικτυακές επιθέσεις .....	35
3.2.2 Ενότητα: Πρωτόκολλα Διαχείρισης .....	35
3.2.3 Ενότητα: VPNs.....	36
3.2.4 Ενότητα: Κρυπτογραφία για διαχειριστές δικτύου .....	36



3.2.5	Ενότητα: Μοντέλο του OSI και επιθέσεις στο TCP .....	36
3.2.6	Ενότητα: Ενότητα Switching Security .....	36
3.2.7	Ενότητα: Επιθέσεις στο επίπεδο 2 του OSI .....	36
3.2.8	Ενότητα: Firewalls .....	37
3.2.9	Ενότητα: IPS/IDS.....	37
3.2.10	Ενότητα: Subnetting, NAT, ACLs .....	37
3.2.11	Test.....	37
4.	Επίλογος.....	38
4.1	Σύνοψη.....	38
4.2	Προτάσεις Βελτίωσης .....	38
4.2.1	Κρυπτογράφηση της βάσης .....	38
4.2.2	Επανασχεδιασμός με βάση το Three Tier Architecture .....	38
4.2.3	Επιπλέον μέτρα ασφαλείας .....	40
	Βιβλιογραφία .....	41



## Πίνακας Εικόνων

Εικόνα 1 - Απαιτήσεις Εγκατάστασης Virtual Machine .....	13
Εικόνα 2 - Taskset.....	15
Εικόνα 3 - LAMP Server Installation.....	16
Εικόνα 4 - Apache Server .....	16
Εικόνα 5 – File vsft.conf .....	17
Εικόνα 6 - Moodledata file.....	19
Εικόνα 7 - Εγκατάσταση Moodle .....	20
Εικόνα 8 - Αρχικές ρυθμίσεις.....	20
Εικόνα 9 - Επιλογή database.....	21
Εικόνα 10 - Ρυθμίσεις της database .....	22
Εικόνα 11 - Τελικές ρυθμίσεις database.....	23
Εικόνα 12 - File config.php.....	24
Εικόνα 13 - Αποδοχή όρων .....	24
Εικόνα 14 - Τελική εγκατάσταση .....	25
Εικόνα 15 - Δημιουργία admin .....	26
Εικόνα 16 - Πρώτη σελίδα moodle .....	27
Εικόνα 17 - Ρυθμίσεις για τις διαδρομές συστήματος.....	27
Εικόνα 18 - Location settings .....	28
Εικόνα 19 - Πολιτική κωδικών πρόσβασης.....	31
Εικόνα 20 - Quarantine file .....	32
Εικόνα 21 - Antivirus .....	33
Εικόνα 22 – Δείγμα Μαθήματος.....	34



## Περίληψη

Η παρούσα μεταπτυχιακή εργασία εκπονήθηκε στα πλαίσια της συνεργασίας του τμήματος **Ασφάλειας Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς** και των **Ελληνικών Ενόπλων Δυνάμεων**.

Επικεντρώνεται στην εγκατάσταση και ανάπτυξη της ασφαλούς πλατφόρμας ηλεκτρονικής μάθησης και αξιολόγησης Moodle (Modular Object Oriented Developmental Learning Environment). Είναι ένα πακέτο ελεύθερου λογισμικού - **ανοιχτού κώδικα σύστημα εικονικής μάθησης**. Με αυτή τη πλατφόρμα αναπτύχθηκε σειρά μαθημάτων, συμπεριλαμβανομένης της διαδικασίας αξιολόγησης των εκπαιδευόμενων. Ειδικότερα, περιγράφεται ο πλήρης οδηγός – εγχειρίδιο εγκατάστασης της ηλεκτρονικής πλατφόρμας **Moodle v.2.9.2**.

Στην συνέχεια αναπτύσσεται σειρά μαθημάτων, σε μορφή ενοτήτων, με αντικείμενο την **ασφάλεια των δικτύων των ηλεκτρονικών υπολογιστών**. Παρουσιάζεται ο σκοπός και το αντικείμενο του κάθε μαθήματος ενώ περιγράφονται οι διαδικασίες αυτοαξιολόγησης και τελικής αξιολόγησης των εκπαιδευόμενων αλλά και της εκπαιδευτικής διαδικασίας.

Η εργασία αυτή αποτελεί τμήμα μιας συνολικότερης εργασίας με κύριο στόχο την ανάπτυξη μαθημάτων για την **εξ αποστάσεως εκπαίδευση** και την **αξιολόγηση** των στελεχών του **Στρατού Ξηράς** σε θέματα ασφάλειας ηλεκτρονικών υπολογιστών. Επιπρόσθετα, στόχο έχει την **εξοικονόμηση οικονομικών πόρων** μέσω της μείωσης του κόστους εκπαίδευσής τους.

**Λέξεις-κλειδιά:** δικτυακές επιθέσεις, συστήματα διαχείρισης μάθησης-αξιολόγησης, σύστημα εικονικής μάθησης, ηλεκτρονική μάθηση, ασύγχρονη μάθηση, εκπαίδευση από απόσταση, Moodle, πολυμέσα, ασφάλεια δικτύων, ασφάλεια πληροφοριών, συνεργατική μάθηση, αξιολόγηση, μείωση κόστους, διάδραση, ελεύθερο λογισμικό, κινητής/φορητή εκπαίδευσης, ΤΠΕ, ψηφιακός αλφαριθμητισμός, δια βίου μάθηση, εικονικό δίκτυο, σύστημα ανίχνευσης εισβολής



## Abstract

This postgraduate thesis created under the cooperation of the department of **Digital Security Systems University of Piraeus** and the **Greek Armed Forces**.

It focuses on the establishment and development of a secure electronic virtual learning and evaluation platform. The platform is the Moodle (Modular Object Oriented Developmental Learning Environment). It is a free software package – an **open source Virtual Learning Environment (VLE)**. Using this platform a Course Management System (CMS) was developed and a series of courses including trainees' assessment process was added. In particular, it describes the complete Guide - Installation Manual of e-learning platform **Moodle v.2.9.2**.

Then, a series of courses were developed in form of modules, with subject the **Network Security**. The purpose and the subject of each course is presented while it is described the self-evaluation process and final evaluation of learners but also of the educational process.

The current document is part of a more comprehensive work with main objective the development of **distance learning** courses and **evaluation** of the **Army Staff** on issues regarding computer security. In addition, the aim is **financial savings** by reducing the training cost.

**Keywords:** network attacks, learning-assessment management systems (LMS), course management system (CMS), asynchronous learning, Virtual Learning Environment (VLE), distance learning-education, Moodle, multimedia, network security, information security, cooperative learning, evaluation, cost reduction, Web2.0, online, interaction, social constructivism, MOOC, training assistant, m-learning, open source, OSI model, VPN, IDS, Firewall, Switching





## 1. Εισαγωγή

### 1.1 Σκοπός

Σκοπός της παρούσας διπλωματικής εργασίας είναι η εγκατάσταση και ανάπτυξη της ηλεκτρονικής πλατφόρμας Moodle με παράλληλη δημιουργία μαθημάτων με αντικείμενο την ασφάλεια δικτύων και η εκπαίδευση και αξιολόγηση των στελεχών των ενόπλων δυνάμεων στο εν λόγω αντικείμενο μέσω της πλατφόρμας αυτής.

### 1.2 Δομή

Στο πρώτο κεφάλαιο γίνεται συνοπτική παρουσίαση του σκοπού, και της δομής της εργασίας ενώ παράλληλα γίνεται σύντομη αναφορά του περιβάλλοντος και της αναγκαιότητας ανάπτυξης συστημάτων εξ αποστάσεως εκπαίδευσης ως αποτέλεσμα της επέκτασης και χρήσης περιβαλλόντων online μετεκπαίδευσης/επιμόρφωσης/κατάρτισης αλλά και αξιολόγησης.

Στο δεύτερο κεφάλαιο παρουσιάζεται βήμα προς βήμα η εγκατάσταση της πλατφόρμας Moodle. Με την χρήση των εικόνων και την περιγραφή κύριος στόχος είναι η δημιουργία ενός εγχειριδίου εγκατάστασης σε ένα virtual machine. Ιδιαίτερη αναφορά γίνεται στα θέματα ασφάλειας των δεδομένων της πλατφόρμας Moodle.

Στο επόμενο κεφάλαιο, παρουσιάζονται οι ενότητες μαθημάτων που θα φιλοξενηθούν στην πλατφόρμα. Το μάθημα “Ασφάλεια Δικτύων Ηλεκτρονικών Υπολογιστών”, αναπτύσσεται μέσα από 10 αυτόνομες θεματικές ενότητες, που περιλαμβάνουν θεμελιώδεις γνώσεις σχετικά με το αντικείμενο. Η ύλη περιλαμβάνει δικτυακές επιθέσεις, πρωτόκολλα ασφάλειας δικτύου, διαχείριση VPN, βασικές μεθόδους κρυπτογραφίας. Επίσης, αναπτύσσεται το OSI μοντέλο και πως μπορούμε να αποφύγουμε επιθέσεις στο TCP, γίνεται αναφορά στο Switching Security και σε προηγμένες τεχνολογίες Firewall, IDS και Natting που χρησιμοποιούνται από την πλειονότητα των σύγχρονων επιχειρήσεων και οργανισμών για την ασφάλεια των δικτύων τους. Τα μαθήματα ολοκληρώνονται, με την ανάπτυξη της διαδικασίας αυτοαξιολόγησης και τελικής αξιολόγησης των εκπαιδευόμενων και της εκπαιδευτικής διαδικασίας μέσω της εκτέλεσης αντίστοιχων test. Τέλος, εκτυπώνονται πιστοποιητικά στους επιτυχόντες διδασκόμενους και παρέχονται στατιστικά στοιχεία για περαιτέρω ανάλυση των επιδόσεών τους.

Τελειώνοντας, στο τέταρτο κεφάλαιο αναφέρονται συνοπτικά συμπεράσματα, ενώ γίνονται και κάποιες προτάσεις για την βελτίωση της ασφάλειας του περιεχομένου της πλατφόρμας. Επίσης, γίνονται προτάσεις τρόπων πιστοποίησης της ποιότητάς της.



### 1.3 Ηλεκτρονική μάθηση

Σίγουρα ζούμε στην εποχή που η διείσδυση του Internet στην ζωή μας, επηρεάζει την καθημερινότητα μας σε βαθμό που κι εμείς οι ίδιοι πριν από λίγα χρόνια δεν θα μπορούσαμε ούτε να φανταστούμε. Ιατρική, υπηρεσίες προς πολίτες, OnLine αγορές, εκλογές είναι μονάχα κάποιοι από τους τομείς που έχουν επηρεαστεί από την ανάπτυξη των τεχνολογιών πληροφορικής και τηλεπικοινωνιών. Η γνώση εξελίσσεται με ραγδαίους ρυθμούς. Στη συνεχώς εξελισσόμενη «κοινωνία της πληροφορίας»-όρος εύστοχος για τη σύγχρονη κοινωνία ραγδαίας ανάπτυξης της τεχνολογίας και, κατ' επέκταση, της πληροφόρησης και της ενημέρωσης-ο τομέας της εκπαίδευσης έχει αποκτήσει και βιωματικό χαρακτήρα. Η εκπαιδευτική διαδικασία προϋποθέτει διάδραση. Ως διάδραση ορίζουμε το είδος δράσης που συντελείται όταν δύο ή περισσότερα άτομα δρουν, επηρεάζοντας το ένα το άλλο ή διαφορετικά όταν ένα άτομο αλληλοεπιδρά με ένα τεχνολογικό μέσο που επιτρέπει αμφίδρομη επικοινωνία.

Πλέον κάνουμε λόγο για ηλεκτρονική μάθηση (e-learning) καθώς και για distance learning. Δεν είναι λίγα τα πανεπιστήμια που ανά την υφήλιο παρέχουν πτυχίο και μεταπτυχιακούς τίτλους σπουδών με μαθήματα μέσω υπολογιστή (MOOC-Massive Open Online Course). Τα μαθήματα αυτά δεν αφορούν μόνο μαθητές, φοιτητές αλλά και στελέχη επιχειρήσεων και οργανισμών. Η ανάπτυξη του λεγόμενου Web2.0, έχει ευνοήσει την ανάπτυξη διαδικασιών κοινωνικού χαρακτήρα στην εκπαιδευτική διαδικασία και στην αξιολόγησή της. Μεγάλες πολυεθνικές επιχειρήσεις αλλά και μικρότερες εταιρείες και οργανισμοί εκπαιδεύουν τους εργαζόμενους τους σε νέες τεχνολογίες και επιδεξιότητες μέσα από e-learning training μειώνοντας με αυτό τον τρόπο εργατώρες και κόστη. Παράλληλα, υπάρχουν εταιρίες που εξειδικεύονται στην ανάπτυξη λογισμικού για συστήματα ηλεκτρονικής μάθησης.

Με τον όρο ηλεκτρονική μάθηση αναφερόμαστε στην εκπαιδευτική διαδικασία που πραγματοποιείται αποκλειστικά με ηλεκτρονικά μέσα, τόσο για την ανάπτυξη των μαθημάτων όσο και του εκπαιδευτικού υλικού καθώς και στο λογισμικό που χρησιμοποιούν εκπαιδευτής και εκπαιδευμένος που δεν είναι στον ίδιο φυσικό χώρο για να επικοινωνήσουν. Η ηλεκτρονική μάθηση δεν περιορίζεται στην απόκτηση ψηφιακού αλφαριθμητισμού, δηλαδή στην απόκτηση δεξιοτήτων ΤΠΕ (τεχνολογίες πληροφορίας και επικοινωνίας) αλλά μπορεί να περιλαμβάνει διαφορετικά αντικείμενα. Περιλαμβάνει επίσης ποικιλία από μεθοδολογίες και μέσα εκμάθησης όπως τη χρήση λογισμικού, πολυμέσων (multimedia learning), δικτύων Internet/Intranet, διαδραστικών πινάκων και οποιεσδήποτε άλλες μορφές ηλεκτρονικών ή διαδραστικών μέσων. Ακόμα και οι εκπαιδευόμενοι μπορούν να επικοινωνήσουν μεταξύ τους μέσω chat, forum, email (ηλεκτρονικό ταχυδρομείο) και να ανταλλάξουν άμεσα ή ετεροχρονισμένα απόψεις, απορίες, έγγραφα, προβληματισμούς και πληροφορίες πάνω στο αντικείμενο μάθησης. Η ηλεκτρονική μάθηση μπορεί να διεξάγεται εκτός τάξης αλλά και εντός. Για βέλτιστα αποτελέσματα προϋποθέτει διαδραστικές, εποικοδομητικές εκπαιδευτικές πλατφόρμες, λογισμικά και ηλεκτρονικά εποπτικά μέσα, αξιοποίηση του Web2.0 και τεχνολογιών δικτύων γρήγορων ταχυτήτων. Ακόμα και η χρήση κινητών τηλεφωνικών συσκευών δύναται να χρησιμοποιηθεί αποτελεσματικά στη μάθηση με ηλεκτρονικούς τρόπους.

Οι λόγοι που κάνουν την όλη διαδικασία να κερδίζει έδαφος έχουν να κάνουν με την δραστική μείωση των εξόδων αλλά και με το γεγονός ότι πλέον ζούμε σε μια διεθνή αγορά. Έτσι λοιπόν μειώνονται αισθητά τα κόστη σχετικά με μετακινήσεις, αίθουσες διδασκαλίας, εποπτικού υλικού, διαμονής, σημειώσεων κ.α. Οι τεχνολογίες μάθησης Web2.0 έχουν βασιστεί σε πακέτα λογισμικού όπως το Moodle που ως επί το πλείστον παρέχονται δωρεάν λόγω της ύπαρξης μιας οικονομίας κλίμακας



προκαλούμενη από το πλήθος των ατόμων που τα χρησιμοποιούν (Krogh 2012). Επίσης, οι μεγαλύτερες ταχύτητες δικτύου που απαιτούνται, στην εποχή μας παρέχονται και με πολύ μικρότερο κόστος και πολύ μεγαλύτερη αξιοπιστία και ποιότητα. Αυτό έχει σαν αποτέλεσμα και την ανάπτυξη της κινητής/φορητής εκπαίδευσης (m-learning), δηλαδή εκπαίδευσης μέσω φορητών συσκευών δίνοντας έμφαση στην έννοια της φορητότητας της μάθησης.

Ο εκπαιδευόμενος μπορεί να παρακολουθήσει τα μαθήματα με το δικό του ρυθμό, στο δικό του χώρο, σε άμεση συνεργασία όμως με τους υπόλοιπους εκπαιδευόμενους και φυσικά τον εκπαιδευτή του. Η μάθηση γίνεται περισσότερο διαδραστική, ενδιαφέρουσα, πολύπλευρη και εξειδικευμένη. Τα μαθήματα ανταποκρίνονται στην κατά φύσει κοινωνική προδιάθεση του ανθρώπου και στους ρυθμούς της καθημερινότητάς του που δεν αφήνουν πολύ χρόνο και διάθεση για την εκμάθηση δύσκολων αντικειμένων. Τέλος, η ηλεκτρονική μάθηση προάγει τον όρο της δια βίου μάθησης σύμφωνα με την οποία η εκπαίδευση θεωρείται ως μια μακροχρόνια διαδικασία που ξεκινάει από την γέννηση του ανθρώπου και συνεχίζει σε όλη τη διάρκεια της ζωής του.

Επιπλέον, η ποιότητα της εξ αποστάσεως εκπαίδευσης έχει φτάσει σήμερα σε υψηλά επίπεδα τα οποία είναι ήδη αναγνωρίσιμα. Τα μαθήματα αυτά είναι περισσότερο ανοικτά στο δημόσιο έλεγχο από ότι της παραδοσιακής διδασκαλίας, αφού είναι ευκολότερα προσβάσιμα από οποιονδήποτε. Αυτό οδηγεί αφ' ενός σε βελτίωση της ποιότητας και αφ' ετέρου σε μια συνεχή υποχρέωση λογοδοσίας, καθιστώντας έτσι την εξ αποστάσεως εκπαίδευση ολοένα και περισσότερο ανταγωνιστική έναντι των συμβατικών μεθόδων.

Θα μπορούσαμε να συνοψίσουμε τα οφέλη στα εξής σημεία:

- Δεν απαιτείται φυσική παρουσία του εκπαιδευόμενου/εκπαιδευτή
- Απευθύνεται σε πολύ μεγάλο φάσμα θεμάτων
- Ο εκπαιδευόμενος επιλέγει το χρόνο, τον τόπο και τον ρυθμό μελέτης
- Αξιοποιούνται οι νέες τεχνολογίες και το διαδίκτυο.
- Το αντικείμενο της μάθησης γίνεται περισσότερο διαδραστικό και ενδιαφέρον
- Αξιοποιείται η έννοια της συνεργατικότητας
- Το εκπαιδευτικό υλικό μπορεί να είναι περισσότερο επίκαιρο, ανανεώνεται συνεχώς και άμεσα (μέσω Internet ή Intranet)
- Το κόστος της διαδικασίας είναι μικρό
- Ανταποκρίνεται πλήρως στην ανάγκη κατάρτισης και επιμόρφωσης ενηλίκων, δια βίου μάθηση
- Εξειδίκευση ανάλογα με τις απαιτήσεις της εργασίας κάθε εκπαιδευόμενου
- Αξιοκρατία, συνεχής έλεγχος και βελτίωση ποιότητας

Σε σχέση με την παραδοσιακή εκπαίδευση ο ρόλος του εκπαιδευτή διαφοροποιείται ενώ αναβαθμίζεται κατά πολύ η ποιότητα και το είδος του εκπαιδευτικού υλικού. Ο εκπαιδευτής δεν είναι υποχρεωτικό να είναι παρών, ούτε κατέχει την ολότητα της γνώσης. Είναι απλώς καθοδηγητής και διευκολύνει τον εκπαιδευόμενο στην ανακάλυψη της γνώσης (training assistant) παρέχοντάς του πηγές και επιλύοντας απορίες παρεμβαίνοντας σε κρίσιμα σημεία. Επίσης, συμβάλει στην τελική αξιολόγηση και στην αναβάθμιση της εκπαιδευτικής διαδικασίας προς περαιτέρω και καλύτερη αξιοποίησή της.



Όσον αφορά στα είδη της ηλεκτρονικής μάθησης, αυτά διακρίνονται σε δύο μορφές στην σύγχρονη και στην ασύγχρονη. Με τον όρο σύγχρονη εννοούμε όλες εκείνες τις μορφές μάθησης και διδασκαλίας που πραγματοποιούνται την ίδια χρονική στιγμή αλλά εκπαιδευτής και εκπαιδευόμενος βρίσκονται σε διαφορετικά γεωγραφικά σημεία. Είναι απαραίτητη λοιπόν η παρουσία και των δύο για να έχουμε αλληλεπίδραση σε πραγματικό χρόνο. Η αλληλεπίδραση έχει να κάνει με την ανταλλαγή απόψεων επί του υλικού, επίλυση αποριών, ανταλλαγή πηγών γνώσης κ.τ.λ. Παραδείγματα σύγχρονης ηλεκτρονικής μάθησης αποτελούν οι τηλεδιασκέψεις μέσω video camera ή ακόμα και οι συνομιλίες σε ένα ειδικά για το μάθημα διαμορφωμένο chat room.

Με τον όρο ασύγχρονη μάθηση περιγράφουμε την εκπαιδευτική διαδικασία η οποία πραγματοποιείται σε διαφορετικό χρόνο και τόπο. Δεν είναι λοιπόν απαραίτητη η ταυτόχρονη συμμετοχή του εκπαιδευτή και του εκπαιδευόμενου. Ενώ ο εκπαιδευόμενος επιλέγει το προσωπικό του εκπαιδευτικό χρονικό πλαίσιο για την ολοκλήρωση των μαθημάτων του. Επιπρόσθετα, μπορεί να ολοκληρώνει ένα κομμάτι της ύλης σε όσο χρόνο χρειάζεται για να την κατανοήσει, κάτι που συμβάλει και στον να μην διαταράσσεται η καθημερινότητά του αλλά και η εκπλήρωση των υπόλοιπων επαγγελματικών καθηκόντων του από την εκάστοτε αναγκαία εκπαίδευση. Το ηλεκτρονικό ταχυδρομείο (email), οι βιντεοδιασκέψεις, τα podcasts, τα φόρουμ κ.α. αποτελούν μορφές ασύγχρονης μάθησης. Η ασύγχρονη εκπαίδευση είναι περισσότερο ευέλικτη από την σύγχρονη. Στο είδος αυτό της εκπαίδευσης ανήκει η Αυτοδιδασκαλία, η Ημιαυτόνομη Εκπαίδευση και η Συνεργαζόμενη Εκπαίδευση.

Στα πλαίσια αυτά και προκειμένου να εκμεταλλευτεί τις δυνατότητες της ασύγχρονης διδασκαλίας, ζητήθηκε από τις υπηρεσίες των ενόπλων δυνάμεων να γίνει αξιοποίηση της πλατφόρμας Moodle για δημιουργία μαθημάτων, σχετικά με την ασφάλεια των δικτύων των ηλεκτρονικών υπολογιστών. Όλα τα πλεονεκτήματα της ασύγχρονης μάθησης σε συνδυασμό με την εξ' αποστάσεως διδασκαλία καλύπτονται πλήρως από την πλατφόρμα Moodle.

Άλλες παρόμοιες πλατφόρμες είναι τα Blackboard και open e-Class. Το Blackboard είναι ένα εμπορικό προϊόν ενώ το Moodle λογισμικό ανοιχτού κώδικα, άρα το δεύτερο ανταποκρίνεται καλύτερα στον στόχο για μείωση του κόστους. Το e-Class αναπτύχθηκε και χρησιμοποιείται κυρίως από ελληνικά ακαδημαϊκά ιδρύματα. Γι' αυτή την εργασία επιλέχθηκε το Moodle για τη δημιουργία και διεξαγωγή των μαθημάτων ως το περισσότερο διαδεδομένο LMS (Learning Management System) από το 1999 (έτος δημιουργίας του). Επιπλέον, είναι σταθερό, ασφαλές, εύκολα διαχειρίσιμο και διαλειτουργικό αφού επιτρέπει την επικοινωνία με άλλα συστήματα. Τέλος, το Moodle βασίζεται στη θεωρία του κοινωνικού εποικοδομισμού (social constuctivism), η οποία υπογραμμίζει τη σημασία του πολιτισμού και της θεωρίας του πλαισίου της μάθησης του στη συλλογική κατασκευή της γνώσης. Αυτή η προοπτική συνδέεται με θεωρίες μάθησης σύγχρονες όπως η αναπτυξιακή των Vygotsky και Bruner και η κοινωνιογνωστική θεωρία του Bandura. (Ράπτη Α.-Ράπτη Α., Μάθηση και Διδασκαλία στην Εποχή της Πληροφορίας. Ολιστική Προσέγγιση. Αθήνα 2007).

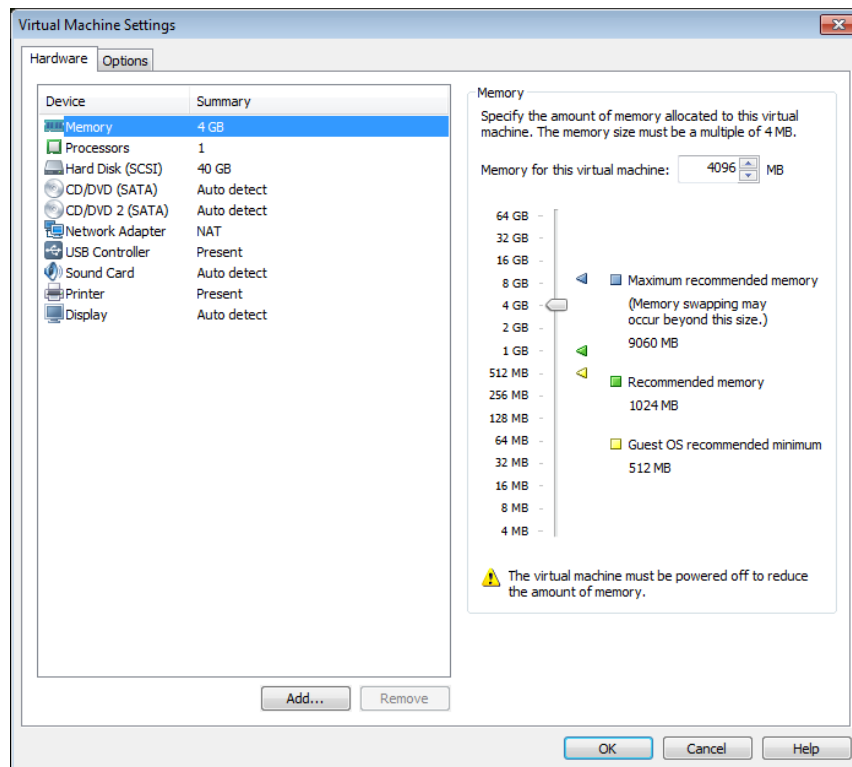
Στις σελίδες που ακολουθούν γίνεται λεπτομερής καταγραφή - εν είδη εγχειριδίου των βημάτων που κάποιος πρέπει να ακολουθήσει για να εγκαταστήσει την έκδοση Moodle 2,9 σε ένα virtual περιβάλλον ενώ ακολουθούν τα μαθήματα.



## 2. Εγχειρίδιο Εγκατάστασης

### 2.1 Προετοιμασία Συστήματος

Για την εγκατάσταση της πλατφόρμας του Moodle επιλέχθηκε η εγκατάσταση σε λειτουργικό σύστημα Ubuntu Linux και πιο συγκεκριμένα στην έκδοση Ubuntu 14.04.3 LTS. Για το σκοπό αυτό δημιουργήθηκε ένα virtual machine με τα εξής χαρακτηριστικά:



Εικόνα 1 - Απαιτήσεις Εγκατάστασης Virtual Machine

<b>CPU</b>	<b>1</b>
<b>Μνήμη</b>	<b>4096 MB</b>
<b>Σκληρός δίσκος</b>	<b>40 GB</b>
<b>NIC</b>	<b>NAT</b>

Οι επιλογές των παραπάνω τιμών έγιναν με βάση της προδιαγραφές που ορίζει η ίδια η Moodle, προκειμένου ο τελικός χρήστης να έχει στη διάθεσή του ένα γρήγορο και αξιόπιστο σύστημα.



### 2.1.1 Λειτουργικό Σύστημα

Αρχικά μέσω του iso έγινε η εγκατάσταση του λειτουργικού, και στην συνέχεια update και upgrade, προκειμένου να εγκατασταθούν τα καινούργια patches (ενημερώσεις ασφάλειας) και οι βιβλιοθήκες με σκοπό να παραδοθεί προς χρήση, ένα ασφαλές και ενημερωμένο σύστημα. Οι εντολές για το update και το upgrade εκτελέστηκαν μέσω cli (command line interface) με δικαιώματα root και είναι αντίστοιχα οι εξής:

```
sudo apt-get update
sudo apt-get upgrade
```

### 2.1.2 Βοηθητικά Προγράμματα

Η πλατφόρμα του Moodle χρησιμοποιεί μια σειρά βοηθητικών προγραμμάτων για τις διάφορες λειτουργίες της. Έτσι, με δικαιώματα root πραγματοποιείται εγκατάσταση των παρακάτω προγραμμάτων:

```
sudo apt-get install graphviz aspell php5-pspell php5-curl php5-gd php5-intl
php5-mysql php5-xmllrpc php5-ldap clamav
```

- **graphviz** (Graph Visualization Software), πακέτο με την χρήση του οποίου γίνεται οπτική απεικόνιση σε μορφή διαγραμμάτων. Είναι γραμμένο σε γλώσσα DOT και χρησιμοποιείται εκτενώς σε εφαρμογές που έχουν σχέση με τομείς όπως networking, bioinformatics, software engineering, database and web design, machine learning
- **Aspell** ένας spell checker (διορθωτής κειμένου) που ήρθε για να αντικαταστήσει τον Ispell, και περιλαμβάνει πάνω από 70 λεξικά
- **php5-pspell** αποτελεί module για τις pspell functions (συναρτήσεις) στην PHP
- **php5-curl** ένα ακόμα module της PHP. Η curl είναι βιβλιοθήκη με την χρήση της οποίας γίνεται ανταλλαγή αρχείων μέσω FTP (File Transfer Protocol), HTTP server (webservice).
- **php5-gd** module για τα γραφικά το οποίο υποστηρίζει τύπους αρχείων PNG, JPEG, XPM καθώς και Freetype/ttf γραμματοσειρές
- **php5-intl** το πακέτο αυτό είναι ένα module που διευκολύνει την διεθνοποίηση των PHP scripts.
- **php5-mysql** module για την MySQL
- **php5-xmllrpc** αποτελεί module για της xmllrpc functions στην PHP
- **php5-ldap** αποτελεί module για της ldap functions στην PHP
- **clamav** open source antivirus

Εκτός από τα παραπάνω προγράμματα απαραίτητη είναι και η εγκατάσταση:

- ενός LAMP server με χαρακτηριστικά: λειτουργικό O/S **Linux**, Webserver **Apache**, βάση (Database) **MySQL**, (γλώσσα εφαρμογής) Application Programming Language **PHP** και
- ενός FTP server για μεταφορά αρχείων.



### 2.1.3 Εγκατάσταση του LAMP server

Η εγκατάσταση του LAMP server έγινε με χρήση του προγράμματος `tasksel` που είναι ένα εργαλείο των Debian/Ubuntu το οποίο κάνει εγκαταστάσεις πολλαπλών πακέτων με συντονισμένο τρόπο- σαν ένα task στο σύστημα μας.

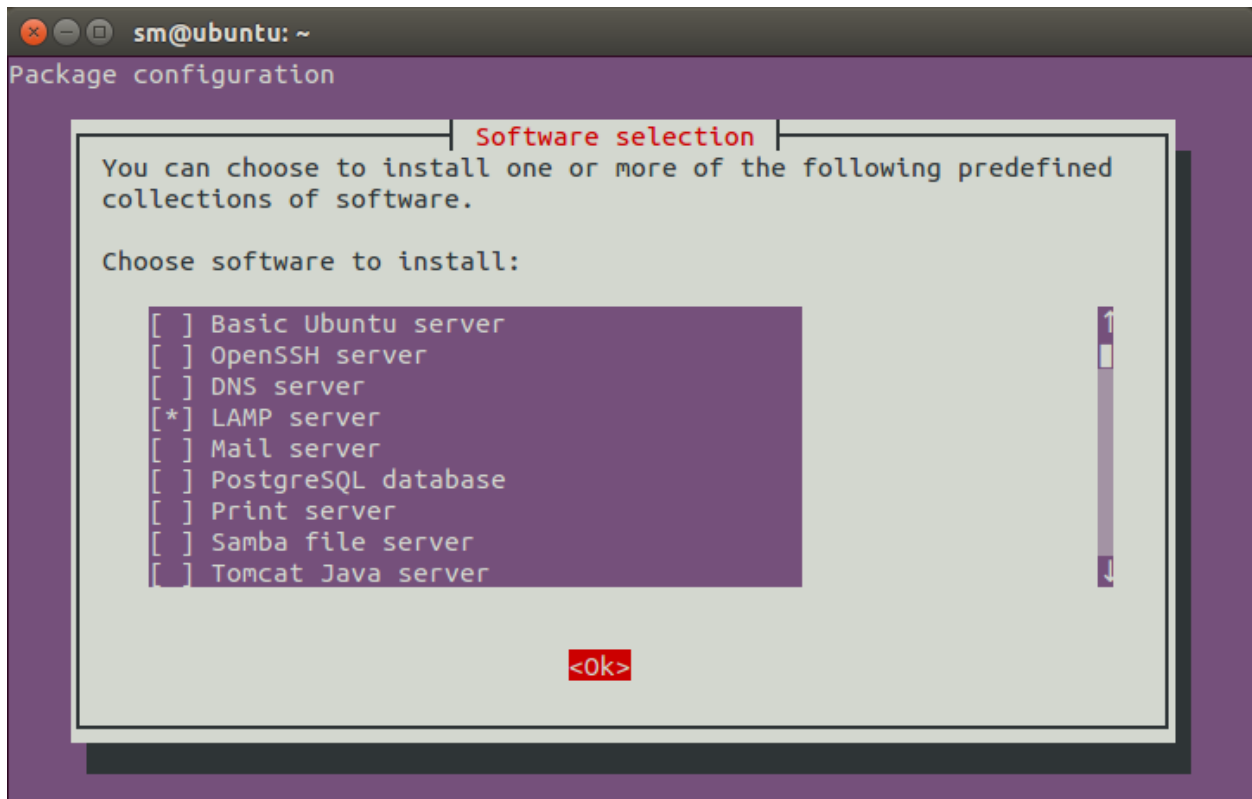
Για την εγκατάσταση με δικαιώματα `root`, δόθηκε η παρακάτω εντολή για το κατέβασμα του αρχείου:

```
sudo apt-get install tasksel
```

Στην συνέχεια για την εκτέλεση του δόθηκε η παρακάτω εντολή:

```
sudo tasksel
```

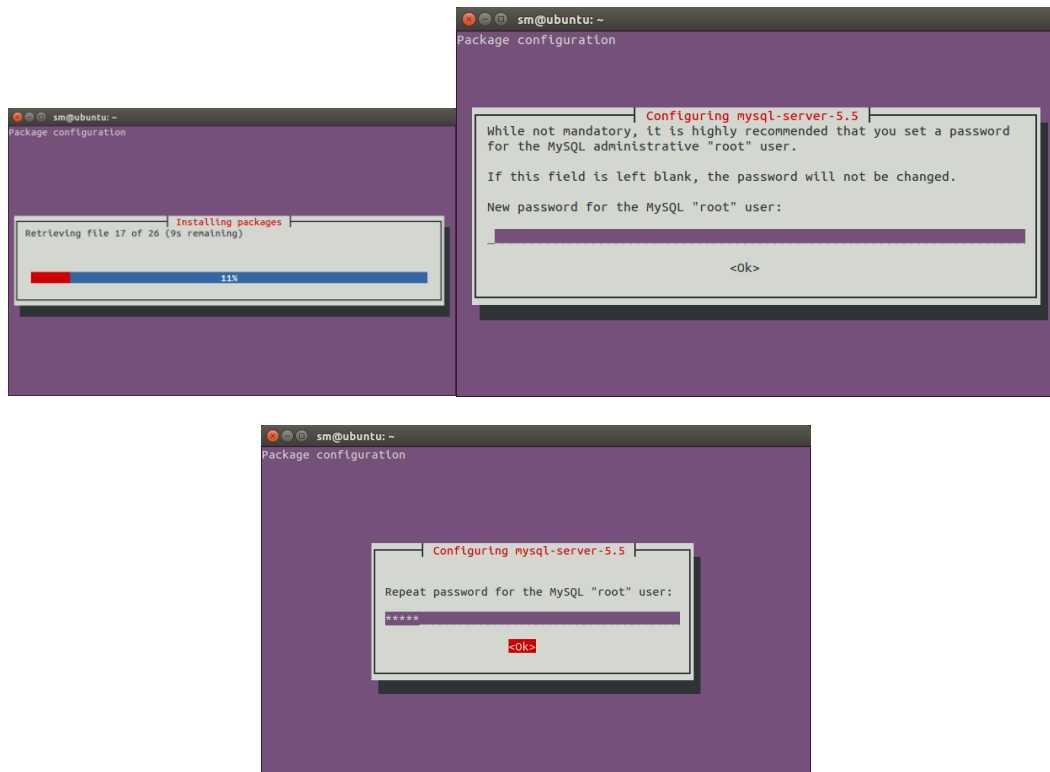
Στο μενού που εμφανίστηκε έγινε η επιλογή της εγκατάστασης του LAMP server.



Εικόνα 2 - Tasksel

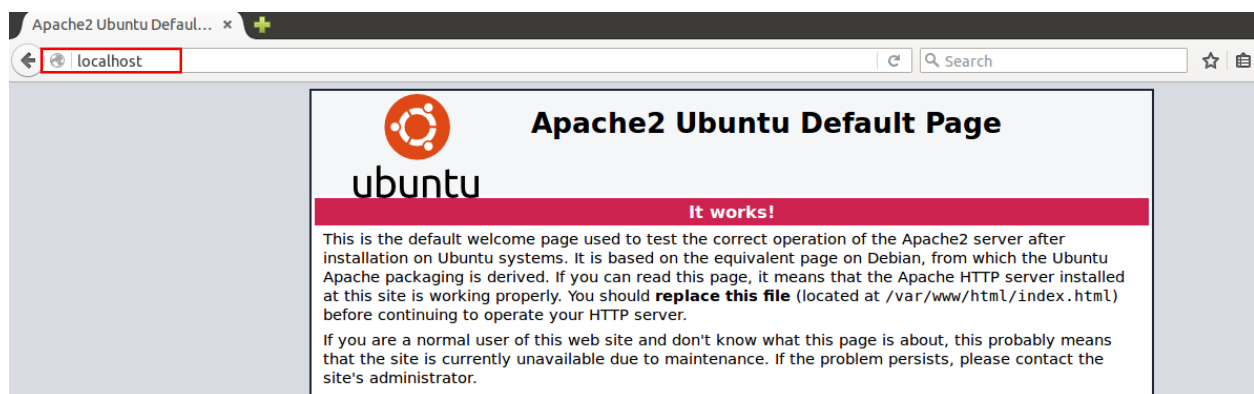


Στην συνέχεια της εγκατάστασης δόθηκε και επιβεβαιώθηκε με καινούργια εισαγωγή το password για τον root χρήστη της MySQL.



Εικόνα 3 - LAMP Server Installation

Τέλος, έγινε επιβεβαίωση της ορθής εγκατάστασης του Apache Server, με κλίση μέσω του προγράμματος πλοήγησης Firefox του localhost.



Εικόνα 4 - Apache Server



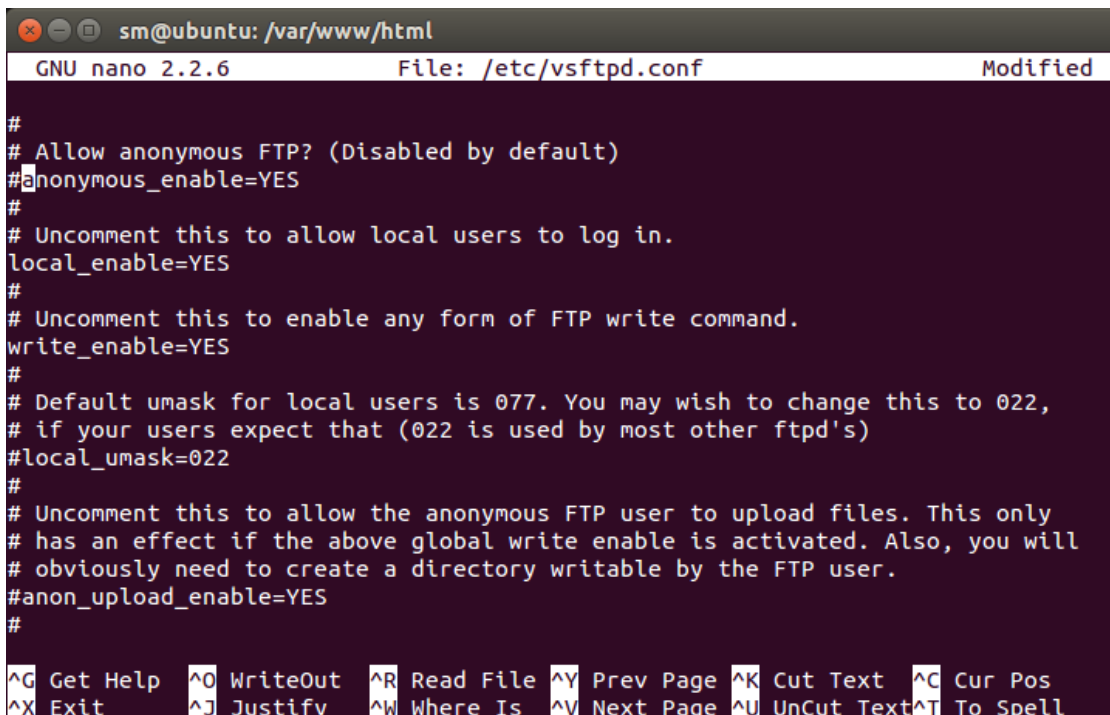
### 2.1.4 Εγκατάσταση του FTP Server

Για την ευκολότερη και ασφαλή μεταφορά αρχείων από και προς τον server εγκαταστάθηκε ένας FTP (File Transfer) server.

Συγκεκριμένα εγκαταστάθηκε ο vsftpd server (very secure ftp), ο οποίος παρέχει ασφάλεια και σταθερότητα. Η εγκατάσταση έγινε με δικαιώματα root μέσω της εντολής:

```
sudo apt-get install vsftpd
```

Για την απόκτηση δικαιωμάτων της εντολής write στον FTP server έγινε αποσχολιάστηκε (uncomment) η γραμμή write\_enable=YES στο αρχείο vsftpd.conf



```

sm@ubuntu: /var/www/html
GNU nano 2.2.6      File: /etc/vsftpd.conf      Modified
#
# Allow anonymous FTP? (Disabled by default)
#anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell

```

Εικόνα 5 – File vsft.conf

Τέλος, για να δοθούν δικαιώματα πρόσβασης και εκτέλεσης εντολών για εναπόθεση αρχείων από κάποιο απομακρυσμένο χρήστη, αλλάχτηκαν και τα δικαιώματα στον φάκελο html με τις εντολές:

```
sudo chown -R sm:www-data /var/www/html/
sudo chmod 775 /var/www/html/
```

sm είναι ο χρήστης τον οποίο ορίσαμε στο λειτουργικό και θα μπορεί να εναποθέσει αρχεία στον συγκεκριμένο φάκελο.

## 2.2 Πλατφόρμα Moodle

Για την εγκατάσταση της πλατφόρμας έγινε περιήγηση στην σελίδα

<https://download.moodle.org/>

και στην συνέχεια κατέβασμα και τοπική αποθήκευση της συμπιεσμένης έκδοσης του προγράμματος στο home directory.

Αφού έγινε αποσυμπίεση του αρχείου, μεταφέρθηκε στον φάκελο του webserver (/var/www/html), ενώ με τις παρακάτω εντολές για λόγους ασφαλείας λήφθηκε μέριμνα ώστε στο φάκελο moodle να έχει δικαιώματα μονάχα ο χρήστης root

```
sudo chown -R root /var/www/html/moodle/
sudo chmod -R 0755 /var/www/html/moodle/
sudo find /var/www/html/moodle -type f -exec chmod 0644 {} \;
```

```
drwxr-xr-x 45 root sm          4096 Jan 15 00:11 moodle
```

### 2.2.1 Δημιουργία Βάσης

Για τη δημιουργία της MySQL βάσης έγιναν οι τα εξής ενέργειες:

- Login στην MySQL:

```
mysql -u root -p
```

Καταχωρήσαμε σαν password, αυτό που βάλουμε κατά την εγκατάσταση του LAMP server

- Δημιουργία κενής βάσης με όνομα moodle

```
mysql> CREATE DATABASE moodle DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;
```

- Δημιουργία του χρήστη moodleuser με password 'yourpassword' με τα ελάχιστα δικαιώματα (select, insert, delete κ.τ.λ) στη βάση moodle

```
mysql> GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,CREATE TEMPORARY TABLES,DROP,INDEX,ALTER ON moodle.* TO moodleuser@localhost IDENTIFIED BY 'yourpassword';
```



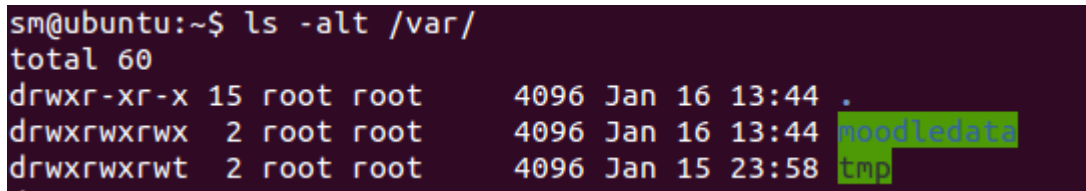
### 2.2.2 Δημιουργία Data Directory

Η πλατφόρμα moodle χρειάζεται ένα φάκελο moodledata για την αποθήκευση των αρχείων (π.χ. τα ανεβασμένα αρχεία, τα temporary data, cache, session data κ.τ.λ).

Θα πρέπει ο web server να έχει δικαιώματα εγγραφής σε αυτό το directory.

Επιπλέον, ο φάκελος αυτός δεν θα πρέπει να είναι προσβάσιμος απευθείας από το web για λόγους ασφαλείας. Επίσης, πρέπει μην είναι στο φάκελο της εγκατάστασης /var/www/html/moodle. Έχοντας τα προηγούμενα υπόψιν δημιουργήθηκε ο φάκελος στη διαδρομή /var και έγινε αλλαγή των δικαιωμάτων χρήσης για όλους τους χρήστες με τις εξής εντολές

```
sudo mkdir /var/moodledata
sudo chmod 0777 /var/moodledata
```



```
sm@ubuntu:~$ ls -alt /var/
total 60
drwxr-xr-x 15 root root 4096 Jan 16 13:44 .
drwxrwxrwx 2 root root 4096 Jan 16 13:44 moodledata
drwxrwxrwt 2 root root 4096 Jan 15 23:58 tmp
```

Εικόνα 6 - Moodledata file

Αυτός ο φάκελος και τα δεδομένα του θα πρέπει κατά τακτά χρονικά διαστήματα να αντιγράφεται και αποθηκεύεται σε διαφορετικό μηχάνημα ή tape (backup) ώστε σε περίπτωση απώλειας δεδομένων ή καταστροφής να μπορούν να ανακτηθούν.

### 2.2.3 Εγκατάσταση Moodle

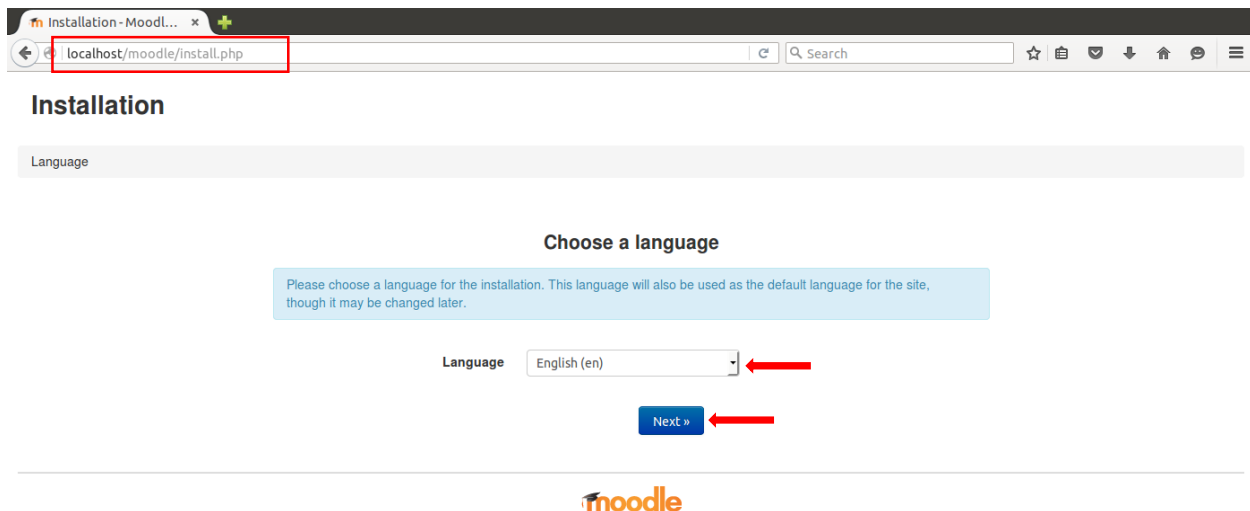
Για την συνέχιση της εγκατάστασης της πλατφόρμας υπάρχουν δυο επιλογές:

- Εγκατάσταση μέσω CLI (Command Line Interface)
- Εγκατάσταση μέσω WEB

Ακολουθήθηκε η δεύτερη μέθοδος, αφού αυτή η διαδικασία μπορεί να λειτουργήσει και σε συστήματα με λειτουργικό σύστημα Windows με το οποίο ο μέσος χρήστης είναι εξοικειωμένος.

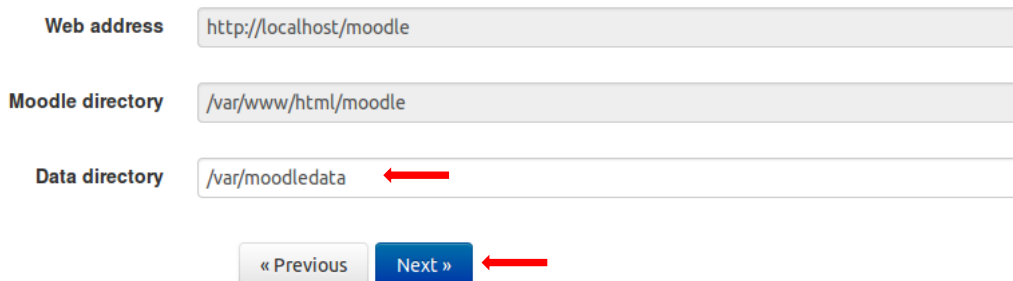
Μέσω ενός browser καλέσαμε το <http://localhost/moodle> και στη σελίδα επιλέχθηκε η γλώσσα εγκατάστασης. Το κουμπί επόμενο μεταβιβάζει τον χρήστη στο επόμενο βήμα της εγκατάστασης.





Εικόνα 7 - Εγκατάσταση Moodle

Στην επόμενη σελίδα γίνεται αναφορά στο path της ιστοσελίδας, στην διαδρομή του φακέλου της εγκατάστασης και στον φάκελο των δεδομένων. Έτσι, έγινε αλλαγή της διαδρομής από την `/var/www/moodledata` σε αυτή που δημιουργήθηκε στο προηγούμενο βήμα `/var/moodledata`



Εικόνα 8 - Αρχικές ρυθμίσεις

Εδώ πρέπει να σημειωθεί ότι ορθογραφικό ή άλλο λάθος καταχώρησης της διεύθυνσης του φακέλου δεδομένων δημιουργεί πρόβλημα στη λειτουργία της Moodle εφαρμογής, αφού αυτή ψάχνει σε λάθος φάκελο για τα δεδομένα.




Στην επόμενη σελίδα ζητήθηκε η επιβεβαίωση του τύπου του server που χρησιμοποιούμε για την βάση δεδομένων .

### Choose database driver

Moodle supports several types of database servers. Please contact server administrator if you do not know which type to use.

Type

---



Εικόνα 9 - Επιλογή database

Μετά, έγινε εισαγωγή του username (modleuser) και του password (yourpassword) της βάσης δεδομένων που είχε δημιουργηθεί στο 1.2.1 Δημιουργία Βάσης.



## Database settings

### Improved MySQL (native/mysqli)

The database is where most of the Moodle settings and data are stored and must be configured here.

The database name, username, and password are required fields; table prefix is optional.

If the database currently does not exist, and the user you specify has permission, Moodle will attempt to create a new database with the correct permissions and settings.

Database host	<input type="text" value="localhost"/>
Database name	<input type="text" value="moodle"/>
Database user	<input type="text" value="moodleuser"/> ←
Database password	<input type="text" value="yourpassword"/> ←
Tables prefix	<input type="text" value="mdl_"/>
Database port	<input type="text"/>
Unix socket	<input type="text"/>
	<input type="button" value="« Previous"/> <input type="button" value="Next »"/> ←

Εικόνα 10 - Ρυθμίσεις της database

Το γεγονός ότι για λόγους ασφάλειας των δεδομένων έγινε αλλαγή διαδρομής εγκατάστασης του data directory έχει σαν αποτέλεσμα να μην μπορεί να ολοκληρωθεί πλήρως αυτόματα η εγκατάσταση. Στην παρακάτω απεικόνιση παρουσιάζετε η αποτυχία της προσπάθειας εγκατάστασης, αφού ο installer δεν μπόρεσε να δημιουργήσει το αρχείο config.php.



## Configuration completed

Moodle made an attempt to save your configuration in a file in the root of your Moodle installation. The installer script was not able to automatically create a config.php file containing your chosen settings, probably because the Moodle directory is not writeable. You can manually copy the following code into a file named config.php within the root directory of Moodle.

```
<?php // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype      = 'mysqli';
$CFG->dblibrary   = 'native';
$CFG->dbhost      = 'localhost';
$CFG->dbname      = 'moodle';
$CFG->dbuser      = 'moodleuser';
$CFG->dbpass      = 'cisco';
$CFG->prefix      = 'mdl_';
$CFG->dboptions  = array (
    'dbpersist' => 0,
    'dbport'    => '',
    'dbsocket'  => '',
);

$CFG->wwwroot    = 'http://localhost/moodle';
$CFG->dataroot   = '/var/moodledata';
$CFG->admin      = 'admin';

$CFG->directorypermissions = 0777;

require_once(dirname(__FILE__) . '/lib/setup.php');

// There is no php closing tag in this file,
// it is intentional because it prevents trailing whitespace problems!
```

Εικόνα 11 - Τελικές ρυθμίσεις database

Το αρχείο αυτό το δημιουργήθηκε από τον διαχειριστή ως εξής:

Με δικαιώματα root δημιουργήθηκε το αρχείο config.php

```
sudo nano /var/www/html/moodle/config.php
```

ενώ το περιεχόμενό του είναι το κείμενο του πλαισίου.



```

sm@ubuntu: ~
GNU nano 2.2.6 File: /var/www/html/moodle/config.php Modified
$CFG->dbuser = 'moodleuser';
$CFG->dbpass = 'cisco';
$CFG->prefix = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => '',
  'dbsocket' => '',
);
$CFG->wwwroot = 'http://localhost/moodle';
$CFG->dataroot = '/var/moodledata';
$CFG->admin = 'admin';
$CFG->directorypermissions = 0777;
require_once(dirname(__FILE__) . '/lib/setup.php');

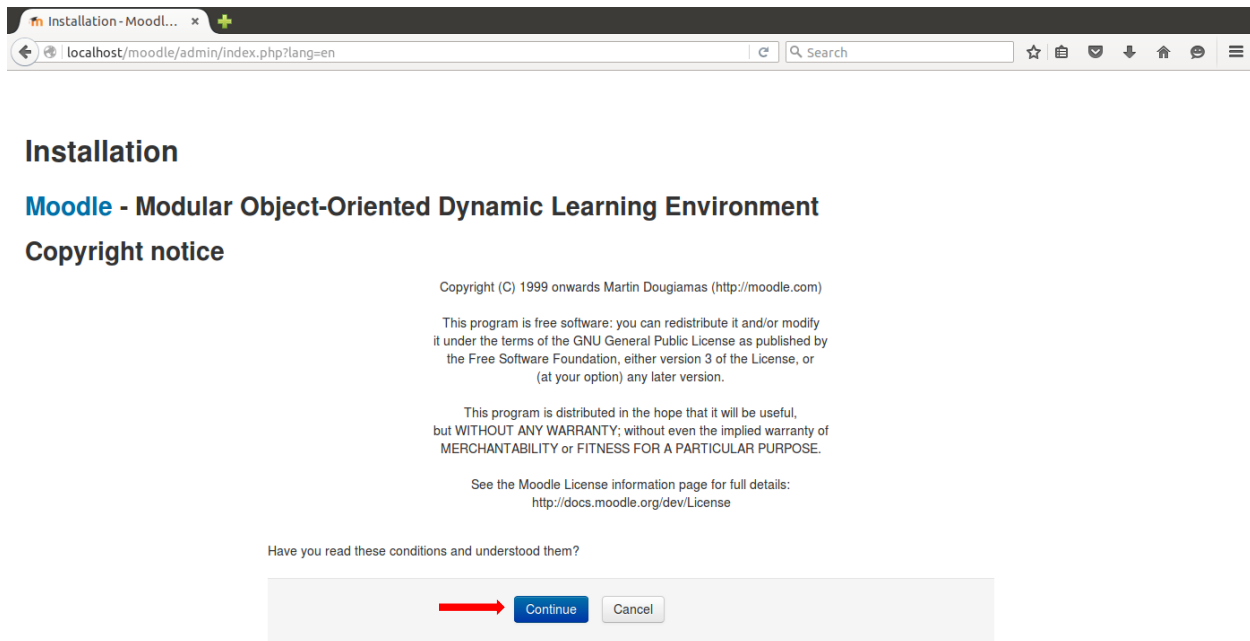
// There is no php closing tag in this file,
// it is intentional because it prevents trailing whitespace problems!

^G Get Help      ^O WriteOut     ^R Read File    ^V Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit         ^J Justify     ^W Where Is    ^N Next Page    ^U UnCut Text   ^T To Spell

```

Εικόνα 12 - File config.php

Μετά το refresh της σελίδας επιλέχθηκε 'continue' για την αποδοχή του copyright.



Εικόνα 13 - Αποδοχή όρων

Στην επόμενη σελίδα το ίδιο το πρόγραμμα εκτέλεσε σειρά ελέγχων για την ύπαρξη διαφόρων υποσυστημάτων που είναι αναγκαία για την λειτουργία του. Αφού διαπιστώθηκε η εγκατάσταση όλων των απαιτούμενων επιλέχτηκε το continue ώστε να συνεχιστεί η εγκατάσταση.



Installation - Moodle 3.0.2+ (Build: 20160114)

Moodle 3.0.2+ (Build: 20160114)

For information about this version of Moodle, please see the online [Release Notes](#)

### Server checks

Name	Information	Report	Plugin	Status
unicode		① must be installed and enabled		OK
database	mysql (5.5.46-0ubuntu0.14.04.2)	① version 5.5.31 is required and you are running 5.5.46.0.0.14.04.2		OK
php		① version 5.4.4 is required and you are running 5.5.9.1.4.14		OK
pcreunicode		① should be installed and enabled for best results		OK
php_extension	iconv	① must be installed and enabled		OK
php_extension	mbstring	① should be installed and enabled for best results		OK
php_extension	curl	① must be installed and enabled		OK
php_extension	openssl	① should be installed and enabled for best results		OK
php_extension	tokenizer	① should be installed and enabled for best results		OK
php_extension	xmlrpc	① should be installed and enabled for best results		OK
php_extension	soap	① should be installed and enabled for best results		OK
php_extension	ctype	① must be installed and enabled		OK
php_extension	zip	① must be installed and enabled		OK
php_extension	zlib	① must be installed and enabled		OK
php_extension	gd	① must be installed and enabled		OK
php_extension	simplexml	① must be installed and enabled		OK
php_extension	spl	① must be installed and enabled		OK
php_extension	pcre	① must be installed and enabled		OK
php_extension	dom	① must be installed and enabled		OK
php_extension	xml	① must be installed and enabled		OK
php_extension	intl	① should be installed and enabled for best results		OK
php_extension	json	① must be installed and enabled		OK
php_extension	hash	① must be installed and enabled		OK
php_setting	memory_limit	① recommended setting detected		OK
php_setting	file_uploads	① recommended setting detected		OK
php_setting	opcache.enable	① recommended setting detected		OK

Your server environment meets all minimum requirements.

Continue

Εικόνα 14 - Τελική εγκατάσταση

Στο σημείο αυτό ολοκληρώθηκε η εγκατάσταση της βάσης και η δημιουργία των πινάκων της.

## 2.2.4 Δημιουργία Λογαριασμού Admin

Στη συνέχεια της εγκατάστασης δημιουργήθηκε το admin account, δίνοντας το password & μία διεύθυνση ηλεκτρονικού ταχυδρομείου (email address).

Η επιλογή update profile, προχώρησε την εγκατάσταση στη σελίδα όπου δόθηκαν το όνομα της σελίδας -Diplomatiki, αφήνοντας όλες τις υπόλοιπες ρυθμίσεις στις αρχικές.

Installation

On this page you should configure your main administrator account which will have complete control over the site. Make sure you give it a secure username and password as well as a valid email address. You can create more admin accounts later on.

Expand all

General

Username\* admin

Choose an authentication method Manual accounts

The password must have at least 8 characters, at least 1 digit(s), at least 1 lower case letter(s), at least 1 upper case letter(s), at least 1 non-alphanumeric character(s)

New password\* \*\*\*\*\*  Unmask

Force password change

First name\* Admin

Surname\* User

Email address\* stmarinos@gmail.com

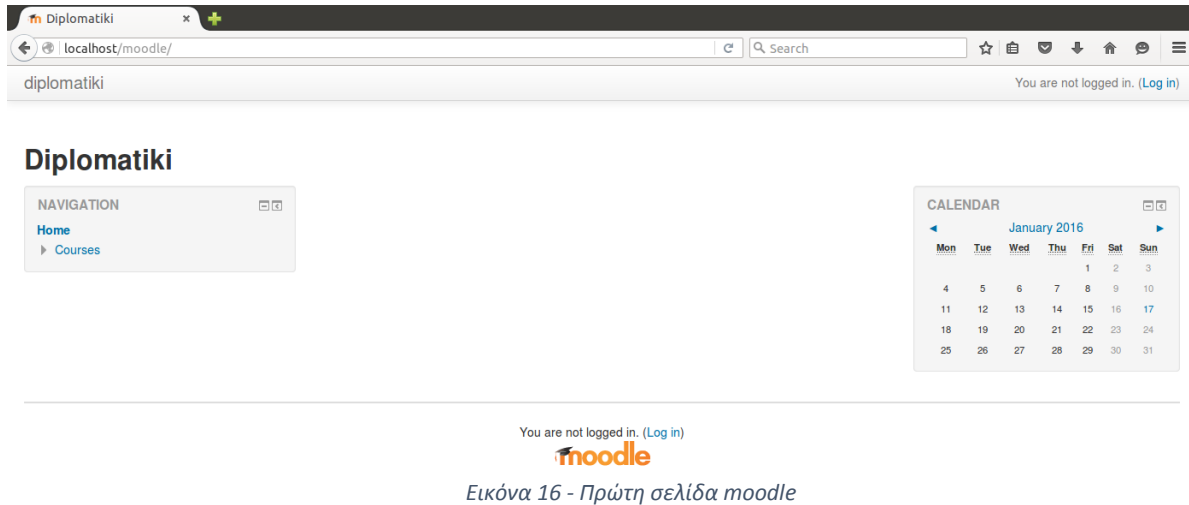
Email display Allow everyone to see my email address

City/town

Εικόνα 15 - Δημιουργία admin

Ολοκληρώνοντας την εγκατάσταση έγινε κλίση του Home page της ιστοσελίδας που μόλις δημιουργήθηκε:

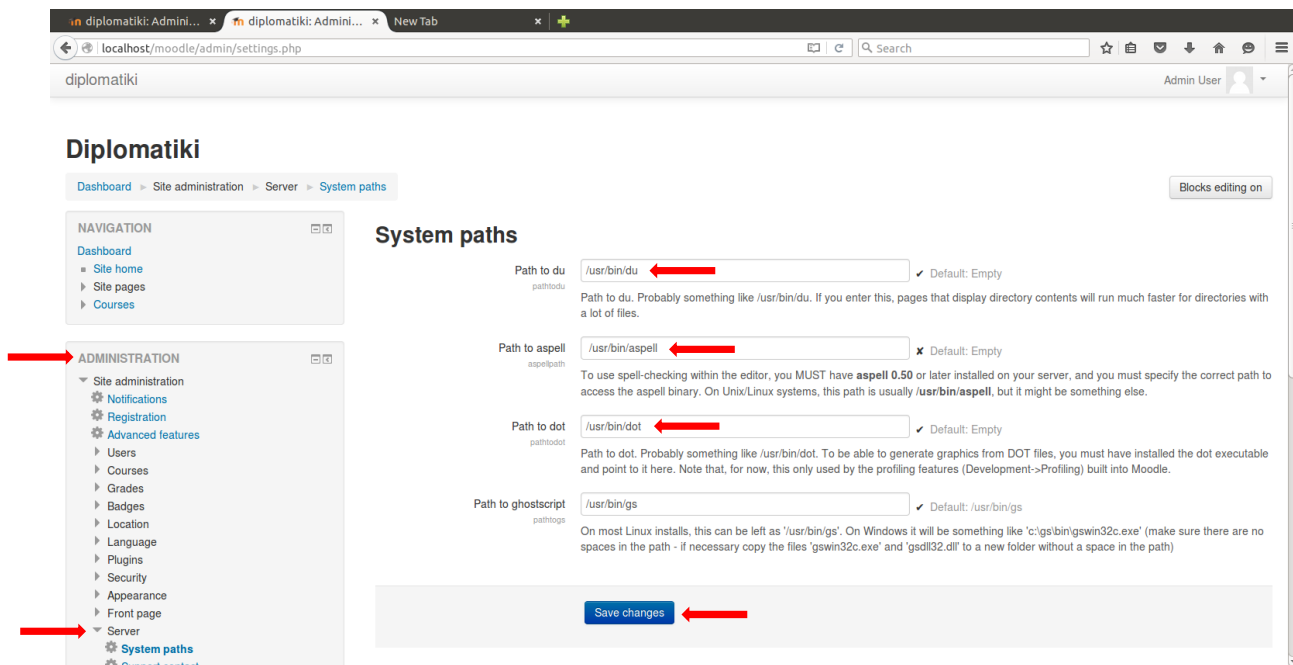




Εικόνα 16 - Πρώτη σελίδα moodle

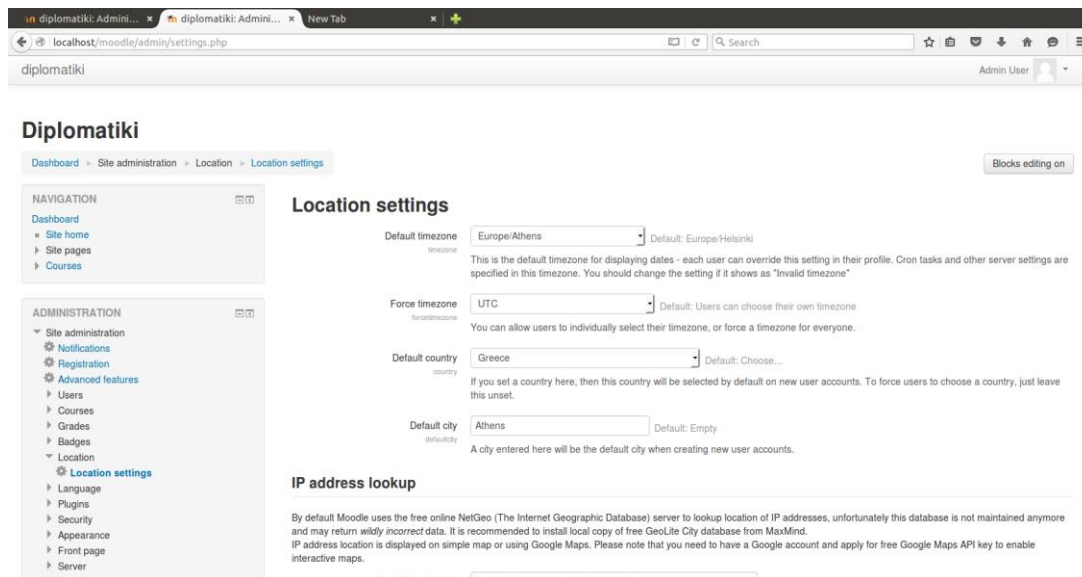
## 2.2.5 Τελικές Ρυθμίσεις

Τελειώνοντας την εγκατάσταση θα πρέπει να γίνουν κάποιες επιπλέον ρυθμίσεις, όπως προτείνει ο οργανισμός της Moodle. Πιο συγκεκριμένα, μετά το login με admin rights, ακολουθήθηκε η διαδρομή Administration → Site administration → Server → System paths και τέθηκαν οι διαδρομές των binaries των du, dot και aspell. Πρόκειται για διαδρομές που αφορούν σε εγκαταστάσεις σε περιβάλλον Linux και σε προγράμματα για λεξικά και αναζήτηση. Με τις προτεινόμενες αλλαγές βελτιώνεται η απόδοσή τους.



Εικόνα 17 - Ρυθμίσεις για τις διαδρομές συστήματος

Μια επιπλέον αλλαγή βρίσκεται στην διαδρομή Administration → Site administration → Location Settings και αφορά στις επιλογές για το time zone κ.τ.λ.



Εικόνα 18 - Location settings

Τέλος, έγινε χρήση του crontab. Το crontab είναι διαδικασία των Linux για την εκτέλεση προγραμμάτων από το σύστημα σε περιοδική βάση ή κάποια στιγμή στην οποία ο διαχειριστής δεν είναι παρών. Στην ουσία ελέγχει τι θα τρέξει, και τότε μειώνοντας έτσι τον φόρτο εργασίας για τους διαχειριστές συστημάτων/εφαρμογών. Σχετικά με το crontab περισσότερες πληροφορίες μπορείτε να βρείτε παρακάτω:

<http://www.linuxinsider.gr/forum/8887/pos-leitoyrgei-crontab#ixzz405BADlmm>

Με εντολή στο crontab η βάση ρυθμίστηκε να παίρνει ανά τακτά χρονικά διαστήματα updates, να στέλνει mail κ.τ.λ. Η διαδικασία μπορεί να γίνει με χρήση cli, ή με χρήση του παραθυρικού περιβάλλοντος ή με το ίδιο το crontab. Η τρίτη μέθοδος είναι αυτή που τελικά υλοποιήθηκ καθώς είναι η συνήθης.

Με δικαιώματα root έγινε κλίση του crontab editor για τον χρήστη www-data του λειτουργικού

```
sudo crontab -u www-data -e (σε περιβάλλον vi)
```

και στο αρχείο προστέθηκε η γραμμή

```
*/15 * * * * /usr/bin/php /var/www/html/moodle/admin/cli/cron.php
```

Η εντολή αυτή θα εκτελείται κάθε 15 λεπτά από τον χρήστη www-data και θα κάνει update τη βάση, τα reports της Moodle και θα ολοκληρώνει οποιεσδήποτε δραστηριότητες πρέπει να εκτελούνται σε τακτά χρονικά διαστήματα.

## 2.3 Ασφαλίζοντας το Περιεχόμενο

Η ίδια η Moodle έχει μια σειρά από ενέργειες που προτείνει προκυμμένους να ασφαλιστεί το περιεχόμενο της βάσης. Για το λόγο αυτό υπάρχει ειδική αναφορά στην διαδρομή Administration → Site administration → Security.

### 2.3.1 IP Blocker

Ακολουθώντας τη διαδρομή

Administration → Site administration → Security → IP Blocker φτάνουμε στο menu που δίνει στον administrator της πλατφόρμας την δυνατότητα να επιτρέπει ή να αποτρέπει σε συγκεκριμένες IP διευθύνσεις ή σε block IP διευθύνσεων την πρόσβαση στο site.

Εξ ορισμού οι διευθύνσεις στις οποίες απαγορεύεται η πρόσβαση είναι εκείνες που επεξεργάζονται και υλοποιούνται κατά προτεραιότητά, εκτός αν επιλεγεί το Allowed list, όπου οι διευθύνσεις αυτές επεξεργάζονται και υλοποιούνται κατά προτεραιότητα.

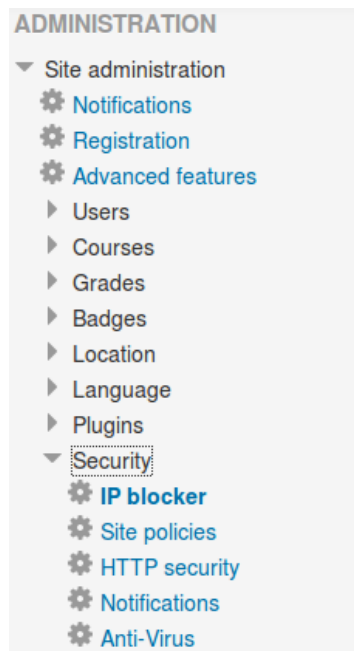
Απαιτείται ιδιαίτερη προσοχή κατά την εφαρμογή τους, γιατί υπάρχει κίνδυνος να απαγορευθεί η πρόσβαση στο site από διευθύνσεις που έρχονται για παράδειγμα μέσω Proxy, ή ακόμα και στον ίδιο τον administrator.

### 2.3.2 Site Policies

Στη διαδρομή Administration → Site administration → Security → Site policies υπάρχει το menu που παρέχει στον διαχειριστή τη δυνατότητα για επιλογές πολιτικής ασφαλείας που εκτός των υπολοίπων επηρεάζουν και θέματα ιδιωτικότητας.

Στο menu υπάρχει μια πληθώρα επιλογών που περιλαμβάνει:

- **Protect usernames**, με την ενεργοποίηση του αποτρέπονται οι κακόβουλοι να καταλάβουν αν κάνουμε χρήση κάποιου username. Στην περίπτωση που κάποιος προσπαθήσει να κάνει reset το password του εμφανίζεται το εξής μήνυμα: *"If you supplied a correct username or email address then an email should have been sent to you."* χωρίς να του δίνονται άλλες πληροφορίες, όπως για παράδειγμα ότι δεν έχει γράψει σωστό email ή username.
- **Force users to login**, θα πρέπει όλοι να κάνουν login για να έχουν πρόσβαση ακόμα και σε βασικές πληροφορίες όπως ο τίτλος του μαθήματος.
- **Force users to login to view profile**, θα πρέπει όλοι οι χρήστες να κάνουν login. Έτσι, οι προσωπικές πληροφορίες των χρηστών είναι προστατευμένες και επιπλέον σε περίπτωση που κάποιος χρήστης ανεβάσει μη επιτρεπτό περιεχόμενο στο profile του, αυτό δεν θα είναι ορατό στους υπόλοιπους επισκέπτες της ιστοσελίδας.



- **Open to Google**, επιτρέπει στους google search spiders να έχουν quest access.
- **Profile visible roles**, κάθε ρόλος που έχει επιλεγεί θα είναι ορατός στους συμμετέχοντες στο μάθημα. Εξ ορισμού οι ρόλοι Teacher, Non-editing teacher και Student είναι επιλεγμένοι.
- **Maximum uploaded file size**, καθορίζει το μέγεθος των αρχείων που μπορεί κάποιος να ανεβάσει. Με αυτή την επιλογή προστατεύεται ο χώρος που έχει κατανεμηθεί για τη βάση και ο οποίος είναι πεπερασμένος. Σε αντίθετη περίπτωση κάποιος κακόβουλος χρήστης μπορεί να ανεβάσει κάποιο αρχείο μεγαλύτερο από τον διαθέσιμο χώρο στη βάση με αποτέλεσμα να προκαλέσει τεχνικό πρόβλημα στον server και μη διαθεσιμότητα της ιστοσελίδας.
- **User quota**, ο μέγιστος αποθηκευτικός χώρος που δίνουμε στον χρήστη (def = 100M)
- **Allow Embed and object tags**, επιτρέπει την χρήση σε embed multimedia π.χ. flash. Θα πρέπει οι διαχειριστές να είναι πολύ προσεκτικοί, γιατί με αυτό τον τρόπο ενδεχομένως να ανοίγουν κενά ασφαλείας καθώς τέτοιου είδους αρχεία είναι πιθανό να εμπεριέχουν κακόβουλα λογισμικά (πχ. Trojans).
- **Enable trusted content**, η πλατφόρμα δέχεται μόνο clear text. Παρολαυτά, για συγκεκριμένους χρήστες –ρόλους μπορεί να παραληφθεί αυτή η πολιτική. Με τον τρόπο αυτό όμως είναι δυνατόν από άγνοια του χρήστη να ανέβει κακόβουλο υλικό τύπου bad scripts, media κ.τ.λ.
- **Maximum time to edit posts**, διαθέσιμο χρόνος για αλλαγές σε κάτι που έχει καταχωρηθεί, πριν ειδοποιηθούν οι χρήστες (def = 30min).
- **Allow extended characters in usernames**, για χρήση ειδικών χαρακτήρων στα usernames.
- **Site policy URL**, εφόσον υπάρχει σελίδα που αναφέρει κανόνες χρήσης, οι χρήστες ανακατευθύνονται εκεί για να τους διαβάσουν και να συμφωνήσουν με αυτούς πριν από τη χρήση της πλατφόρμας.
- **Site policy URL for guests**, όμοια επιλογή με τη παραπάνω για τους επισκέπτες.
- **Keep tag name caching**, αν θέλει ο διαχειριστής να κρατούνται τα tags, όπως τα έβαλαν οι χρήστες (μικρά και κεφαλαία)
- **Profiles for enrolled users only**, ώστε ο διαχειριστής να αποτρέψει τους spammers από την άσκοπη δημιουργία profile.
- **Cron execution via command line only**, αποτρέποντας έτσι την εκτέλεση του Cron από web interface.
- **Cron password for remote access**, στην περίπτωση που επιτρέπεται η εκτέλεση του Cron μέσω web θα πρέπει να καταχωρείται password.
- **Account lockout**, κλείδωμα λογαριασμού σε περίπτωση πολλαπλών αποτυχιών. Ο διαχειριστής ορίζει τον αριθμό τους.
- **Password Policy**, πολιτική σύμφωνα με την οποία ορίζεται το μήκος, η χρήση ειδικών χαρακτήρων αλφαριθμητικών κλπ. κανόνες που απαιτούνται ώστε ο κωδικός πρόσβασης να είναι ισχυρός σε επιθέσεις hacker.



**Password policy**  Default: Yes  
passwordpolicy  
 Turning this on will make Moodle check user passwords against a valid password policy. Use the settings below to specify your policy (they will be ignored if you set this to 'No').

**Password length**  Default: 8  
minpasswordlength  
 Passwords must be at least these many characters long.

**Digits**  Default: 1  
minpassworddigits  
 Passwords must have at least these many digits.

**Lowercase letters**  Default: 1  
minpasswordlower  
 Passwords must have at least these many lower case letters.

**Uppercase letters**  Default: 1  
minpasswordupper  
 Passwords must have at least these many upper case letters.

**Non-alphanumeric characters**  Default: 1  
minpasswordnonalphanumeric  
 Passwords must have at least these many non-alphanumeric characters.

**Consecutive identical characters**  Default: 0  
maxconsecutiveidentchars  
 Passwords must not have more than this number of consecutive identical characters. Use 0 to disable this check.

Εικόνα 19 - Πολιτική κωδικών πρόσβασης

- **Password rotation limit**, ορίζεται ο αριθμός των φορών που πρέπει κάποιος να αλλάξει password προκειμένου να χρησιμοποιήσει κάποιο παλαιότερο.
- **Maximum time to validate password reset request**, χρόνος που μπορεί να περάσει μέχρι να γίνει επικύρωση της αίτησης για password reset (def = 30 min).
- **Log out after password change**, ο χρήστης γίνεται log out από όλα τα ενεργά sessions εκτός αυτού που κάνει την αλλαγή του password.
- **Group enrolment key policy**, με την ενεργοποίηση του, τα κλειδιά που έχουν να κάνουν με groups ακολουθούν την ορισμένη από το Password Policy, πολιτική για τα κλειδιά.
- **Disable user profile images**, οι χρήστες δεν μπορούν να αλλάξουν εικόνα στα profile τους.
- **Email change confirmation**, απαιτεί ένα mail ως επιβεβαίωση για την αλλαγή του mail address.
- **Remember username**, αποθήκευση cookies με username.
- **Strict validation of required fields**, αποτρέπει τους χρήστες να βάζουν κενό ή enter σε όποιες φόρμες δεν επιθυμεί ο διαχειριστής.

### 2.3.3 HTTP Security

Στη διαδρομή Administration → Site administration → Security → HTTP security μπορούν να ενεργοποιηθούν οι επιλογές που έχουν να κάνουν με την χρήση του Https και τον secure cookies. Έτσι, τα δεδομένα που ανταλλάσσονται στην πλατφόρμα θα είναι κρυπτογραφημένα ώστε να αποτραπεί η υποκλοπή τους μέσω sniffer (πρόγραμμα υποκλοπής web πληροφορίας).



### 2.3.4 Notification

Στη διαδρομή Administration → Site administration → Security → Notification ο διαχειριστής μπορεί να ορίσει τις ειδοποιήσεις που αφορούν σε αποτυχημένες προσπάθειες login.

### 2.3.5 Antivirus

Ήδη από την αρχή εγκαταστάθηκε το ClamAV που είναι ένα πρόγραμμα open source antivirus. Θα το ενεργοποιηθεί, έτσι ώστε οτιδήποτε καταχωρήσει στην εφαρμογή κάποιος από τους καθηγητές ή τους μαθητές να σαρώνεται και ότι είναι ύποπτο να πηγαίνει στο φάκελο quarantine. Το φάκελο αυτό θα τον δημιουργήσουμε και θα στην συνέχεια θα δώσουμε την κυριότητα (ownership) στον χρήστη www-data του web server.

```
sudo mkdir /var/quarantine
sudo chown -R www-data /var/quarantine/
```

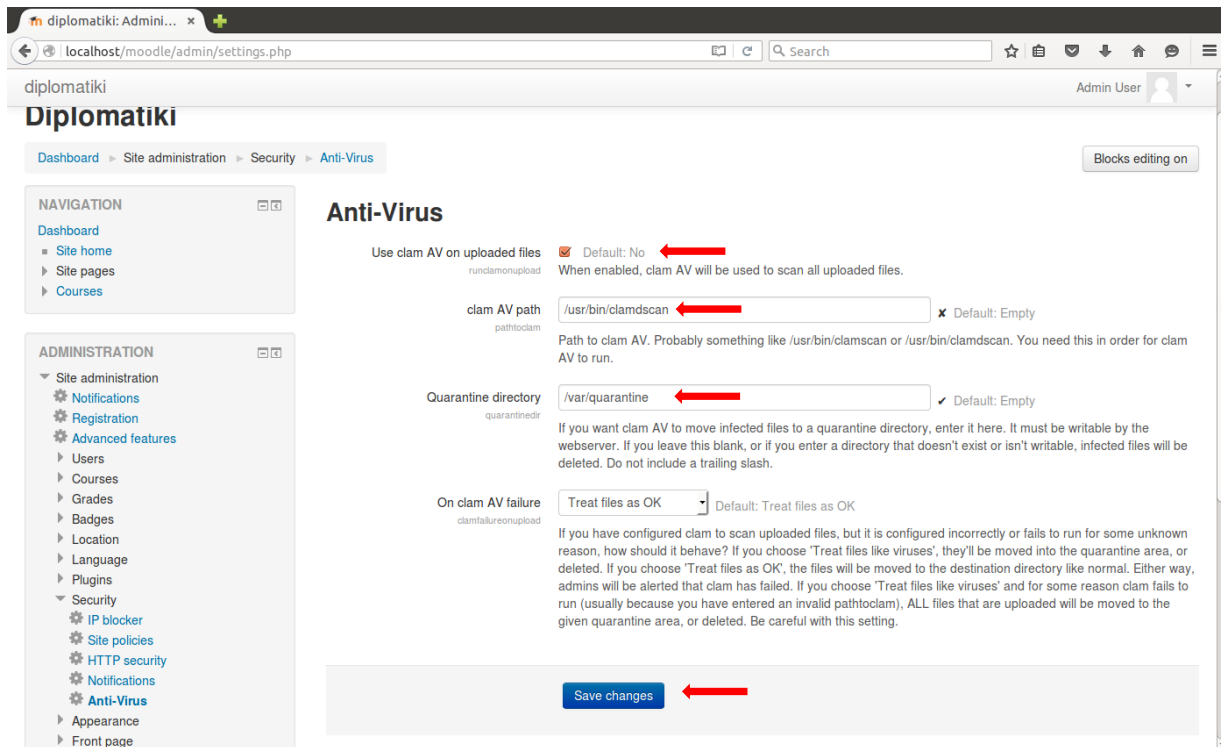
```
sm@ubuntu:/var$ ls -alt
total 64
drwxr-xr-x 16 root    root    4096 Jan 18 11:27 .
drwxr-xr-x  2 www-data root    4096 Jan 18 11:27 quarantine
drwxrwxrwx 11 root    root    4096 Jan 18 11:15 moodledata
```

Εικόνα 20 - Quarantine file

Στην συνέχεια ακολουθώντας την διαδρομή Administration → Site administration → Security → Antivirus, έγιναν οι τελικές ρυθμίσεις για την ενεργοποίηση του.







Εικόνα 21 - Antivirus

### 2.3.6 Firewall

Ο όρος **firewall** ή **τείχος προστασίας** χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο. Στην περίπτωση αυτή τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/ δίκτυο. Στην περίπτωση που η εφαρμογή προστατεύεται από firewall. Θα πρέπει να επιτραπεί η πρόσβαση στις πόρτες του παρακάτω πίνακα:

Protocol	Port	Reason
HTTP	80	Web access
HTTPS	443	Secure Web access
TCP	9111	Chat
TCP	22	Administration for Unix
TCP	3389	Remote Desktop for windows

Το τείχος προστασίας εμποδίζει εισβολείς ή λογισμικό κακόβουλης λειτουργίας (όπως ιούς τύπου worm) να αποκτήσουν πρόσβαση στον υπολογιστή μέσω δικτύου ή του Internet. Το τείχος προστασίας εμποδίζει επίσης τον υπολογιστή να στείλει λογισμικό κακόβουλης λειτουργίας σε άλλους υπολογιστές.

### 3. Δημιουργία μαθήματος

#### 3.1 Εισαγωγή

Στόχος των μαθημάτων είναι οι εκπαιδευόμενοι – στελέχη των ενόπλων δυνάμεων να γνωρίσουν τα βασικά θέματα ασφαλείας, τα σχετικά με το δίκτυο ηλεκτρονικών υπολογιστών, τις απειλές, αδυναμίες που έχουν οι δικτυακές συσκευές και τις επιθέσεις που μπορούν να εκδηλωθούν σε ένα εταιρικό δίκτυο.

Τα μαθήματα είναι δομημένα στην μορφή σεμιναριακού μαθήματος. Το περιεχόμενο του μαθήματος είναι δομημένο σε δέκα θεματικές ενότητες, διάρκειας δύο εκπαιδευτικών εβδομάδων με συνολική διάρκεια δέκα εκπαιδευτικών ημερών. Κάθε εκπαιδευτική ημέρα περιλαμβάνει μία ξεχωριστή θεματική ενότητα. Όπως παρουσιάζεται στην εικόνα που ακολουθεί, κάθε σελίδα αποτελείται από μια διαφάνεια που συνοψίζει τα κυριότερα σημεία του μαθήματος ή παρέχει κάποιες σημαντικές πληροφορίες και στην συνέχεια επεξηγηματικό ή παραπεμπτικό κείμενο. Στην πλειοψηφία των μαθημάτων έχουν ανέβει και σχετικά video, για την καλύτερη κατανόηση του αντικειμένου.


#### Firewall

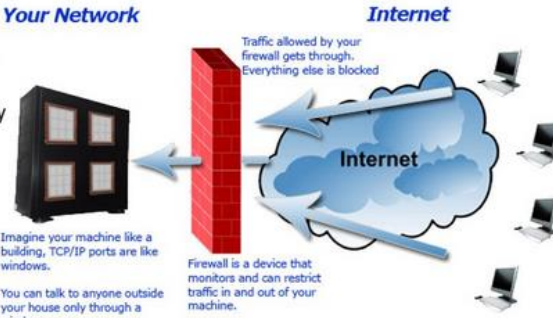
## Firewall

A firewall is a system that enforces an access control policy between network

Common properties of firewalls:

- The firewall is resistant to attacks
- The firewall is the only transit point between networks
- The firewall enforces the access control policy





**Your Network**      **Internet**

Imagine your machine like a building, TCP/IP ports are like windows.  
You can talk to anyone outside your house only through a window.

Traffic allowed by your firewall gets through. Everything else is blocked.

Firewall is a device that monitors and can restrict traffic in and out of your machine.

Configure your firewall to allow in-bound traffic for port 6060, which is used by SynaMan

Πρόκειται για συσκευές ή εφαρμογές ή στην πλειοψηφία των περιπτώσεων, συνδυασμό και των δύο, που κύριος σκοπός τους είναι η ρύθμιση της κυκλοφορίας των δεδομένων ανάμεσα σε δίκτυα υπολογιστών και κατά κανόνα αποτελούν την πρώτη γραμμή άμυνας, στην οποία εφαρμόζεται η πολιτική ασφαλείας ενός οργανισμού. Ένα firewall έχει τουλάχιστον δύο interfaces με σκοπό την απόρριψη ή αποδοχή της κίνησης που διέρχεται μέσω αυτών, βάση των πολιτικών ασφαλείας. Συνήθως αυτά τα δύο interfaces αφορούν το διαδίκτυο (internet) και το ιδιωτικό/τοπικό/εταιρικό μας δίκτυο. Σε πολλές περιπτώσεις όμως, ειδικά σε μεγάλους οργανισμούς, τα firewall χρησιμοποιούνται και για έλεγχο κίνησης και πρόσβασης μεταξύ των διαφόρων εσωτερικών δικτύων. Εν συντομία θα μπορούσαμε να πούμε ότι γενικά τα firewall χρησιμοποιούνται για να αποτρέψουν την είσοδο μη έμπιστων χρηστών στην εσωτερική μας υποδομή.

Τα firewall είναι άκρως απαραίτητα καθώς αποτελούν πολύ σημαντικά σημεία αποκλεισμού και ελέγχου στα οποία μπορούμε να εφαρμόσουμε κανόνες και πολιτικές ασφαλείας και να κάνουμε auditing. Επίσης τα firewall παρέχουν σημαντικές λειτουργίες καταγραφής (logging) στους εκάστοτε διαχειριστές συστημάτων δίνοντάς τους την δυνατότητα να εξετάσουν συνοπτικά τον τύπο και τον όγκο της κίνησης των δεδομένων που δρομολογήθηκαν μέσω των σημείων αυτών.

Η πρώτη επαφή του εκπαιδευόμενου γίνεται μέσω της σελίδας του καλωσορίσματος, όπου εν συντομία αναφέρονται οι στόχοι, ο τρόπος λειτουργίας και οργάνωσης, η διάρκεια των μαθημάτων, ο τρόπος αξιολόγησης καθώς και το που θα βρει το βοηθητικό υλικό.

Για όλους τους εκπαιδευόμενους είναι διαθέσιμος ο φάκελος «Βιβλιοθήκη» μέσα στον οποίο βρίσκονται αναρτημένα ηλεκτρονικά βιβλία (e-books σε μορφή αρχείων pdf) ή links σχετικά με την ασφάλεια του δικτύου και τα μαθήματα.

Επιπρόσθετα υπάρχει το *Forum ανακοινώσεων*, στο οποίο ο διαχειριστής και οι χρήστες με ρόλους manager ή εκπαιδευτή αναρτούν ανακοινώσεις, νέα και ενημερώσεις για τη λειτουργία της πλατφόρμας λογισμικού Moodle ή, σχετικές με τα μαθήματά της, προς ενημέρωση των εκπαιδευόμενων χρηστών.

Το *Forum επικοινωνίας με εκπαιδευτή-εκπαιδευόμενους*, είναι ξεχωριστό και σε αυτό αναρτώνται ερωτήσεις, απαντήσεις, σχόλια, θέματα προς συζήτηση, απόψεις από όλους τους τύπους των χρηστών με σκοπό την επίλυση αποριών, παροχή διευκρινήσεων και επεξηγήσεων επί του συγκεκριμένου μαθήματος ή επί της λειτουργίας της πλατφόρμας Moodle.

Τέλος, υπάρχουν δυο τεστ αυτό-αξιολόγησης και ένα τελικό τεστ αξιολόγησης με τελικό σκοπό την απονομή βεβαίωσης επιτυχούς παρακολούθησης, εφόσον το τελικό τεστ ολοκληρωθεί με επιτυχία δηλαδή με ποσοστό άνω το 70%.

Εκτός από τον εκπαιδευόμενο, αξιολογείται και η εκπαιδευτική διαδικασία προκειμένου αυτή να βελτιωθεί. Έτσι, υπάρχει ένα ερωτηματολόγιο με δέκα ερωτήσεις αξιολόγησης της όλης διαδικασίας από τους συμμετέχοντες.

## 3.2 Ενότητες Μαθήματος: Ασφάλεια Δικτύων Ηλεκτρονικών Υπολογιστών

### 3.2.1 Ενότητα: Δικτυακές επιθέσεις

Στην πρώτη ενότητα «Δικτυακές επιθέσεις» παρουσιάζονται τα κυριότερα είδη επιθέσεων και ο τρόπος εκτέλεσής τους. Πιο συγκεκριμένα γίνεται αναφορά σε επιθέσεις που στόχο έχουν την δικτυακή υποδομή του οργανισμού καθώς και το κέρδος από την επίτευξή τους. Αναλύονται οι σύγχρονες μέθοδοι επιθέσεων με στόχο την αποτύπωση του δικτύου, υποκλοπή συνθηματικών δικτυακών συσκευών κ.α. με τελικό σκοπό την υποκλοπή σημαντικής πληροφορίας ή την διακοπή παροχής υπηρεσίας. Τέλος, παρουσιάζονται τρόποι, προστασίας και αντιμετώπισής τους. Μέσα από αυτή την ενότητα θα γίνει μια πρώτη προσέγγιση των βασικών εννοιών που αφορούν μέτρα ασφάλειας, τα όποια θα αναλυθούν στις επόμενες ενότητες.

### 3.2.2 Ενότητα: Πρωτόκολλα Διαχείρισης

Στην ενότητα αυτή γίνεται αναφορά στα πρωτόκολλα διαχείρισης δικτυακού εξοπλισμού. Στόχος είναι να γίνουν αντιληπτές οι επιθέσεις και αδυναμίες στις οποίες αυτά υπόκεινται καθώς και τι μεθόδους και τακτικές πρέπει να ακολουθήσουμε προκειμένου να τις αποφύγουμε ή να τις αντιμετωπίσουμε. Επιπλέον, παρέχονται οδηγίες και πρακτικά παραδείγματα, βασισμένα σε οδηγούς μεγάλων εταιριών του χώρου για την καλύτερη ασφάλιση των συσκευών και των πρωτοκόλλων διαχείρισης τους.



### 3.2.3 Ενότητα: VPNs

Με στόχο την ασφαλή ανταλλαγή δεδομένων πάνω από δημόσιας χρήσης δίκτυα γίνεται αναφορά και ανάλυση των Virtual Private Networks. Συγκεκριμένα γίνεται αναφορά στα πλεονεκτήματα, τα μειονεκτήματα, τα είδη και τους τύπους τους. Ιδιαίτερη έμφαση δίνεται στα site-to-site VPNs και τον τρόπο υλοποίησης τους σε ένα Cisco device. Τέλος, γίνεται ανάλυση του IPSec (IP Security) πλαισίου και των βασικών αρχών που το διέπουν. Στην ενότητα γίνεται επίσης αναφορά σε επιθέσεις που αφορούν στα VPNs και σε επιθέσεις, στην κρυπτογραφία αλλά και στα πρωτόκολλα που τα υλοποιούν.

### 3.2.4 Ενότητα: Κρυπτογραφία για διαχειριστές δικτύου

Η κρυπτογραφία αποτελεί ένα από τους κυριότερους τρόπους για την διασφάλιση της εμπιστευτικότητάς και της ακεραιότητας κατά την μεταφορά ευαίσθητων δεδομένων. Για το λόγο αυτό χρησιμοποιείται και στα σύγχρονα εταιρικά δίκτυα. Στην ενότητα κρυπτογραφία για διαχειριστές δικτύου, γίνεται παρουσίαση όλων των μεθόδων κρυπτογράφησης που χρησιμοποιούνται για την κατασκευή ενός VPN. Γίνεται ανάλυση των αλγορίθμων κρυπτογράφησης και σύνοψής, ενώ παρουσιάζονται και σύντομα ιστορικά στοιχεία για την έως σήμερα ανάπτυξη της επιστήμης της κρυπτογραφίας.

### 3.2.5 Ενότητα: Μοντέλο του OSI και επιθέσεις στο TCP

Στην πέμπτη ενότητα, γίνεται αναφορά στο μοντέλο του OSI καθώς και το TCP/IP μοντέλο. Αφού γίνει κατανοητός ο τρόπος μετάδοσης της πληροφορίας και οι διάφορες φάσεις της ενθυλάκωσής της, γίνεται μια εκτενής αναφορά στις επιθέσεις που μπορούν εκδηλωθούν στο επίπεδα 3 και 4 του μοντέλου του OSI και στους τρόπους προλήψεως και αντιμετώπισης τους.

### 3.2.6 Ενότητα: Ενότητα Switching Security

Στην ενότητα switching security, επικεντρωνόμαστε στην τεχνολογία των Switch, στον τρόπο λειτουργίας τους και στον τρόπο που αυτά λειτουργούν μέσα στο εταιρικό περιβάλλον. Γίνεται αναφορά σε τεχνολογίες των switch που μελετούν την ανίχνευσή διπλών διόδων και την αποτροπή δημιουργίας τους. Τέλος, αναφέρεται ο τρόπος λειτουργίας τους μέσα στο εταιρικό περιβάλλον με την δημιουργία trunks και VLANs για την αποδοτικότερη, ομαλή και ασφαλέστερη διαχείριση των συσκευών και δεδομένων του οργανισμού.

### 3.2.7 Ενότητα: Επιθέσεις στο επίπεδο 2 του OSI

Στην ενότητα αυτή γίνεται εκτενής αναφορά στις γνωστότερες επιθέσεις με στόχο Layer2 συσκευές και στους τρόπους που μπορούμε να εφαρμόσουμε για να τις αποτρέψουμε. Μέσα από πρακτικά παραδείγματα αναλύονται οι επιθέσεις σε ένα switch και προτείνονται μέθοδοι που εταιρίες του χώρου έχουν αναπτύξει και συμπεριλάβει στα προϊόντα τους.



### 3.2.8 Ενότητα: Firewalls

Ένας από τους απαραίτητους μηχανισμούς ασφάλειας του εταιρικού δικτύου είναι το firewall, το οποίο αποτελεί αναπόσπαστο κομμάτι των σύγχρονων λύσεων ασφάλειας. Στην ενότητα αυτή παρουσιάζονται οι βασικοί τύποι του, καθώς και τα είδη του, οι λύσεις που προσφέρει όσον αφορά όχι μόνο στην περιμετρική ασφάλεια του δικτύου αλλά και το audit ή την υλοποίηση VPNs κ.τ.λ. Στην ενότητα αυτή γίνεται ειδική αναφορά και στο firewall των Linux το IP tables για την καλύτερη κατανόηση του τρόπου της λειτουργίας του.

### 3.2.9 Ενότητα: IPS/IDS

Ένας ακόμα μηχανισμός προστασίας του εταιρικού δικτύου, τα συστήματα ανίχνευσης και αποτροπής κυβερνοεπιθέσεων αναλύονται στην ενότητα IPS/IDS. Πιο συγκεκριμένα γίνεται αναφορά στα είδη στους τύπους και στον τρόπο λειτουργίας τους. Τέλος, γίνεται αναφορά και στον κυρίαρχο μηχανισμό της αγοράς το Snort.

### 3.2.10 Ενότητα: Subnetting, NAT, ACLs

Στην σύγχρονη εποχή του internet of things η ανάγκη για νέες IP διευθύνσεις που θα εξυπηρετούν τον ολοένα και αυξανόμενο ρυθμό απαιτήσεων για συνδεδεμένες συσκευές, λύθηκε με το IPv6. Πολλή πριν από την έλευση του, λύσεις που ακόμα και σήμερα χρησιμοποιούνται ευρέως είχαν εφαρμοστεί. Στην τελευταία αυτή ενότητα γίνεται αναφορά στο Subnetting και στην υπηρεσία του NAT. Τέλος, υπάρχει ειδική ενότητα για τις Access Control Lists, που μέσα από πρακτικά παραδείγματα καταλαβαίνει ο εκπαιδευόμενος την χρήση τους και την αξία τους.

### 3.2.11 Test

Η διδακτική διαδικασία ολοκληρώνεται με τα test αυτό-αξιολόγησης και το τελικό test αξιολόγησης. Με βάση την διδαχθείσα ύλη έχει δημιουργηθεί μια δεξαμενή από 195 ερωτήσεις. Το είδος των ερωτήσεων είναι είτε πολλαπλής επιλογής, είτε τύπου σωστό/λάθος. Από τις ερωτήσεις αυτές αρχικά δημιουργούνται 2 test αυτό-αξιολόγησης 50 ερωτήσεων, ο εκπαιδευόμενος έχει την δυνατότητα να απαντήσει στο καθένα από αυτά σε χρόνο 1 ώρας. Με τον τρόπο αυτό θα μπορέσει ο ίδιος με βάση και τα αποτελέσματα να αξιολογήσει σε ποια σημεία χρειάζεται επανάληψη ή ποια σημεία δεν έχει κατανοήσει. Τέλος, καλείται να απαντήσει στο τελικό test αξιολόγησης που αποτελείται από 100 ερωτήσεις και έχει διάρκεια 2 ώρες. Θα θεωρηθεί ως επιτυχημένη η προσπάθεια που συγκεντρώνει βαθμολογία πάνω από το 70%.



## 4. Επίλογος

### 4.1 Σύνοψη

Με την ολοκλήρωση της διπλωματικής εργασίας που στόχο έχει την εκπαίδευση των στελεχών των ενόπλων δυνάμεων σε θέματα ασφάλειας, μέσω ηλεκτρονικών μαθημάτων που αναρτήθηκαν στην ασφαλή πλατφόρμα του Moodle, παραδόθηκε μια ολοκληρωμένη σειρά ενοτήτων με κέντρο την ασφάλεια των δικτύων. Παρά το γεγονός ότι το προϊόν – πλατφόρμα της Moodle και παραδιδόμενα μαθήματα – έχει αναπτυχθεί με κέντρο την ασφάλεια, υπάρχουν και κάποια επιπλέον μέτρα που ο διαχειριστής θα μπορούσε να πάρει προκειμένου να ασφαλίσει ακόμα περισσότερο την πλατφόρμα, διασφαλίζοντας με αυτόν τον τρόπο και το αδιάβλητο των εξετάσεων.

### 4.2 Προτάσεις Βελτίωσης

#### 4.2.1 Κρυπτογράφηση της βάσης

Προς την κατεύθυνση της διασφάλισης των δεδομένων και της διαδικασίας αξιολόγησης θα πρέπει να δοθεί ιδιαίτερο βάρος στα δεδομένα της βάσης. Θα ήταν χρήσιμο να ληφθούν επιπλέον μέτρα προστασίας. Η κρυπτογράφηση των δεδομένων της βάσης και πιο συγκεκριμένα των test, εντός του εξυπηρετητή θα προφύλασσε το σύστημα από τυχόν επιτυχημένες εισβολές. Ενώ παράλληλα θα διασφαλιζόνταν και η αξιοπιστία της όλης διαδικασίας της αξιολόγησης, αφού ακόμα και αν οι ερωτήσεις είχαν με κάποιο τρόπο υποκλαπεί, ο κάτοχος του υλικού δεν θα μπορούσε να ωφεληθεί σε κάτι, αφού δεν θα είχε το κλειδί της κρυπτογράφησης.

#### 4.2.2 Επανασχεδιασμός με βάση το Three Tier Architecture

Μελλοντικά θα προτείναμε τον ανασχεδιασμό της αρχιτεκτονικής του Moodle με διαχωρισμό των εξυπηρετητών κατά τα πρότυπα της Three Tier Architecture (Τριών Επιπέδων Αρχιτεκτονική). Στην νέα αυτή εγκατάσταση θα υπάρξει σαφής διαχωρισμός των διάφορων υποσυστημάτων, δημιουργώντας τρία διακριτά επίπεδα:

1<sup>ο</sup> επίπεδο αρχιτεκτονικής: Database Servers

2<sup>ο</sup> επίπεδο αρχιτεκτονικής: Application Integration Servers

3<sup>ο</sup> επίπεδο αρχιτεκτονικής: Webservers

Τα τρία αυτά επίπεδα, χωρίζονται σαφώς μεταξύ τους, αφού τοποθετούνται σε διαφορετικές ζώνες firewalls, ενώ για την ακόμα καλύτερη προστασία της βάσης και των web servers θα μπορούσε να χρησιμοποιηθεί και κάποιο WAF (Web Application Firewall) για να αντιμετωπιστούν επιθέσεις τύπου SQL injection, XSS κ.τ.λ.



- Πρώτο επίπεδο αρχιτεκτονικής: Database Servers

Αποτελεί το βασικότερο επίπεδο του συστήματος, δεδομένου ότι στον εξυπηρετητή της βάσης υλοποιούνται όλες οι απαραίτητες λειτουργίες για την αποθήκευση, ανάκτηση, ενημέρωση και συντήρηση των δεδομένων των μαθημάτων, αξιολογήσεων, μαθητολογίου καθώς και του συστήματος. Περιέχει δε όλους τους απαραίτητους μηχανισμούς που δύναται να ενεργοποιηθούν για την ακεραιότητα των δεδομένων (Data Integrity).

- Δεύτερο επίπεδο αρχιτεκτονικής: Application Integration Servers

Αποτελεί το κύριο τμήμα του λογισμικού, στο οποίο εκτελούνται οι περισσότερες λειτουργίες. Επιπλέον, υπάρχει δυνατότητα εγκατάστασης περισσότερων του ενός Application Servers σε διαφορετικά μηχανήματα, αξιοποιώντας, με τον τρόπο αυτό, οποιαδήποτε διαθέσιμη υπολογιστική ισχύ και εξασφαλίζοντας εξαιρετικά αποτελέσματα ανταπόκρισης, αξιοπιστίας και επεκτασιμότητας. Στην περίπτωση που θα χρησιμοποιούσαμε την τεχνολογία του load balancing τότε τα αποτελέσματα θα είναι ακόμα καλύτερα αναφορικά με την ταχύτητα και την τελική αίσθηση από τους χρήστες.

- Τρίτο επίπεδο αρχιτεκτονικής: Webservers

Το τρίτο επίπεδο του λογισμικού αποτελεί τη επαφή του χρήστη με το σύστημα (User Interface). Στο επίπεδο αυτό, πραγματοποιείται η διαχείριση των Οθονών Εργασίας (User Screens) καθώς επίσης και η μορφοποίηση των δεδομένων που εμφανίζονται. Η επικοινωνία του Client με τον Webserver ή τους Application Servers πραγματοποιείται κάνοντας χρήση ενός μόνο πακέτου δεδομένων κάθε φορά. Έτσι, επιτυγχάνεται ο βέλτιστος χρόνος απόκρισης μεταξύ του Client και του Application Server, δεδομένου ότι τα δυο αυτά επίπεδα μπορούν να λειτουργήσουν πάνω σε μια τηλεπικοινωνιακή γραμμή.

Τα πλεονέκτημα και τα οφέλη της παραπάνω λύσης εκτός από τα προαναφερθέντα που αφορούν στην ασφάλεια είναι πολλά, με μοναδικό ίσως μειονέκτημα το κόστος υλοποίησης και συντήρησης. Πιο συγκεκριμένα επιτυγχάνεται:

- Ελαχιστοποίηση της επιβάρυνσης του δικτύου λόγω μεταφοράς μεγάλου όγκου δεδομένων π.χ. η εκτέλεση ενός query (ερώτημα προς τη βάση) για την ανάκτηση των αποτελεσμάτων των test από έναν πίνακα με πολλές εγγραφές γίνεται στο διακομιστή εφαρμογής, από τον οποίο μεταφέρεται στον εκπαιδευόμενο μόνο το αποτέλεσμα.
- Με τον διαχωρισμό του εξυπηρετητή της βάσης δεδομένων (Database Server) από το διακομιστή ή τους εξυπηρετητές της εφαρμογής (Application Servers), ώστε να εκτελούνται σε διαφορετικά μηχανήματα, μπορεί να γίνει πιο εύκολα το sizing (ο καθορισμός των κρίσιμων μεγεθών απόδοσης των αντίστοιχων μηχανών), παρέχοντας έτσι επεκτασιμότητα, χωρίς διακοπή της υπηρεσίας.
- Όσο αφορά στον εξυπηρετητή της βάσης δεδομένων, είναι δυνατή μεταγενέστερη αναβάθμιση του με την αλλαγή / αναβάθμιση του μηχανήματος, χωρίς να επηρεάζεται το υπόλοιπο σύστημα. Η εύκολη και άμεση αναβάθμιση του συστήματος είναι πολύ σημαντικό πλεονέκτημα δεδομένου ότι εμφανίζονται κατά καιρούς λάθη που αφορούν στην ασφάλεια της εφαρμογής και χρήζουν άμεσης διόρθωσης.



### 4.2.3 Επιπλέον μέτρα ασφαλείας

Φυσικά, ιδιαίτερη προσοχή θα πρέπει να δοθεί και στην απομακρυσμένη πρόσβαση των χρηστών. Για την ασφαλέστερη σύνδεσή τους προτείνουμε την σύνδεση τους στους servers μέσω κάποιου VPN client, όπως το Open VPN. Με τον τρόπο αυτό, εκτός από την προστασία του καναλιού ανταλλαγής δεδομένων, προσθέτουμε και άλλο ένα επίπεδο αυθεντικοποίησης.

Εφόσον η πλατφόρμα είναι προσβάσιμη μέσω Web κρίνεται αδήριτη η ανάγκη επικοινωνίας μέσω https πρωτοκόλλου. Σε αυτή την υλοποίηση πρέπει να εφαρμόζονται ενημερωμένες εκδόσεις των SSL πιστοποιητικών με κρυπτογράφηση TLS1.2/SHA256 ή νεότερη. Προτείνεται δε ο τερματισμός της SSL επικοινωνίας να γίνεται σε επίπεδο load balancer και όχι στον webserver για μεγαλύτερη προστασία.

Επιπρόσθετα, σε όλους τους διακομιστές, application servers, databases, webservers πρέπει να γίνονται κατά τακτά χρονικά διαστήματα οι εγκαταστάσεις των πιο πρόσφατων αναβαθμίσεων ασφαλείας σε επίπεδο λειτουργικού και εφαρμογών.

Τέλος, για την ώρα της εξέτασης του τελικού test θα προτείναμε αυτές να δίνονται σε κάποια ειδικά διαμορφωμένη αίθουσα, σε κοινό κεντρικό σημείο, από υπολογιστή που δεν θα δίνει δυνατότητα στον χρήστη για περιήγηση στο διαδίκτυο. Με τον τρόπο αυτό διασφαλίζεται η ακεραιότητα και το αδιάβλητο της διαδικασίας αξιολόγησής, αφού ο εκπαιδευόμενος δεν θα μπορεί να κάνει χρήση σημειώσεων, αριθμομηχανών ή και ακόμα του internet για ανεύρεση λύσεων.





## Βιβλιογραφία

- Darko Miletic, “Moodle Security”, 2011.
- Lawrence C. Miller, «Next Generation firewalls-for-dummies»
- CCNP ISCW Official Exam Certification Guide, Cisco Press
- Denise Donohue “CCNP ISCW Quick Reference Sheets”, Cisco Press
- Ξενάκης Χρ, “Σημειώσεις Μαθήματος ΜΠΣ Ασφάλεια Δικτύων”
- William Stallings, “Network Security Essentials: Applications and Standards”, 4<sup>th</sup> edition
- “Router Security Strategies Securing IP Network Traffic Planes”, Cisco Press 2008
- Anthony Sequeira, “CCNA Security 640-554 Quick Reference” Cisco Press
- Tanenbaum, Andrew S. “Computer Networks”, Fifth Edition
- International, 2003.
- moodle .org
- wikipedia.org
- ww.checkpoint.com
- <http://howdoesinternetnetwork.com/>
- <http://ciscoeasy.blogspot.gr/>

