ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Ψηφιακών Συστημάτων

ΜΠΣ Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων

Κατεύθυνση: Ασφάλεια Ψηφιακών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Πολιτική Ασφάλειας στο Ολοκληρωμένο Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων του Τμήματος Ψηφιακών Συστημάτων»

Συντάκτης: Παπαδημητρίου Γεώργιος, ΜΤΕ/1061, georpapajim@gmail.com

Επιβλέπων: Αναπληρωτής Καθηγητής, Κωνσταντίνος Λαμπρινουδάκης

Πειραιάς, Ιούνιος 2014

Περίληψη

Στην αρχή της παρούσας διπλωματικής εργασίας, γίνεται λόγος για το τι είναι υπηρεσίες ιστού (web services) και αναφέρονται αναλυτικά οι βασικές τεχνολογίες αυτών των υπηρεσιών (XML, SOAP, WSDL, UDDI).

Αμέσως μετά, παρουσιάζονται οι συχνότερες κακόβουλες επιθέσεις που πραγματοποιούνται σε αυτές τις υπηρεσίες και επισημαίνεται ο τρόπος που επηρεάζουν την ομαλή λειτουργία τους.

Εξαιτίας του ότι η οποιαδήποτε επίθεση χρήζει την κατάλληλη αντιμετώπιση, επισημαίνονται οι προδιαγραφές για την ασφάλεια αυτών των υπηρεσιών, καθώς και οι τρόποι με τους οποίους εντοπίζονται και αντιμετωπίζονται οι κακόβουλες επιθέσεις.

Στην συνέχεια, γίνεται λόγος για το πληροφοριακό σύστημα «ΕΥΔΟΞΟΣ» (Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων του Τμήματος Ψηφιακών Συστημάτων) και περιγράφεται η πολιτική ασφάλειας που πρέπει να ακολουθηθεί, για το συγκεκριμένο πληροφοριακό σύστημα.

Τέλος, αναφέρονται οι τύποι επιθέσεων ασφαλείας στους οποίους το πληροφοριακό σύστημα «ΕΥΔΟΞΟΣ» είναι ευπαθή και προτείνονται τρόποι αντιμετώπισης των επιθέσεων αυτών.

Abstract

At the beginning of this thesis, it is discussed about the meaning of the web services and the core technologies of these services (XML, SOAP, WSDL, UDDI) are also mentioned in detail.

Following this, the most frequent malicious attacks made on these services are presented and the way that affects their normal functioning is also highlighted.

For the reason that any attack requires a proper treatment, the security standards of these services are indicated, as well as, the ways to identify and deal with these malicious attacks.

Furthermore, it is discussed about the information system "EVDOXOS" (Course Management System of the Department of Digital Systems) and the security policy to be followed for the specific information system.

Finally, the types of security attacks are mentioned, to which the information system "EVDOXOS" is vulnerable and suggested ways to encounter such attacks.

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμότερες ευχαριστίες μου στον Αναπληρωτή Καθηγητή κ. Κωνσταντίνο Λαμπρινουδάκη, για την άρτια επιστημονική καθοδήγηση, για τις πολύτιμες υποδείξεις του, για το ενδιαφέρον καθώς και για την υπομονή που επέδειξε καθ' όλη την διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας, στοιχεία που συνέβαλαν στην επιτυχή περάτωση της.

Επιπλέον, ευχαριστώ από καρδίας τα μέλη της επιτροπής αξιολόγησης κ. Σωκράτη Κάτσικα και κ. Χρήστο Ξενάκη, για την αξιολόγηση της διπλωματικής μου εργασίας και τις χρήσιμες παρατηρήσεις τους.

Επίσης, εκφράζω την ευγνωμοσύνη μου στους γονείς μου και στην αδερφή μου για την διαρκή υποστήριξη και βοήθειά τους σε όλη την διάρκεια των μεταπτυχιακών μου σπουδών.

Τέλος, ευχαριστώ τον Θεό για την δύναμη, το κουράγιο και την υπομονή που μου δώρισε προκειμένου να φέρω εις πέρας την εργασία αυτή.

Πάντα πρέπει να σταθμίζεις
το κόστος προστασίας ενός αγαθού,
με το κόστος απώλειας του.

Πίνακας Περιεχομένων

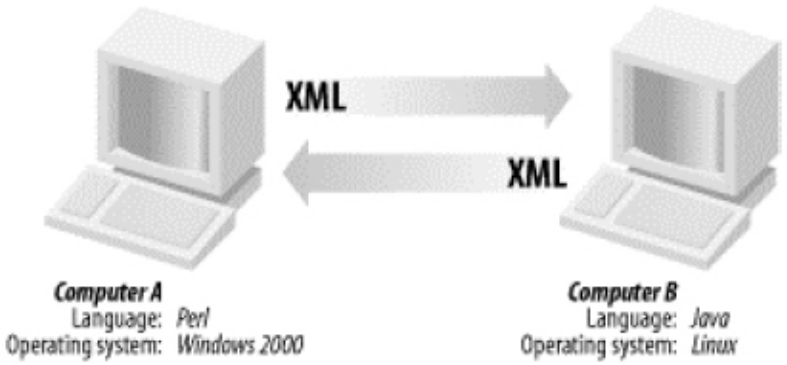
Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

Κεφάλαιο 1: Υπηρεσίες Ιστού (web services)

Εισαγωγή

Σύμφωνα με την IBM, «οι *υπηρεσίες ιστού* (web services)» είναι μια τεχνολογία, που επιτρέπει στις εφαρμογές να επικοινωνούν μεταξύ τους ανεξαρτήτως πλατφόρμας και γλώσσας προγραμματισμού (Εικόνα 1). Μία υπηρεσία ιστού είναι μια διεπαφή λογισμικού (software interface), που περιγράφει μια συλλογή από λειτουργίες, οι οποίες μπορούν να προσεγγιστούν από το δίκτυο μέσω προτύπων XML μηνυμάτων. Επίσης, χρησιμοποιεί πρότυπα βασισμένα στη γλώσσα σήμανσης XML, για να περιγράψει μία λειτουργία (operation) προς εκτέλεση και τα δεδομένα προς ανταλλαγή με κάποια άλλη εφαρμογή. Μια εφαρμογή υπηρεσίας ιστού καθορίζεται από μια ομάδα από υπηρεσίες ιστού, οι οποίες αλληλεπιδρούν μεταξύ τους».



Εικόνα 1: Μοντέλο Υπηρεσιών Ιστού (Chappell and Jewell, 2002)

Μια υπηρεσία ιστού χαρακτηρίζεται από τα πρότυπα «*SOAP*», «*WSDL*», και «*UDDI*», που στο σύνολό τους υλοποιούν μια βασική λειτουργία «*αίτησης και απόκρισης*». Ποιο αναλυτικά και σύμφωνα με την Microsoft, οι υπηρεσίες ιστού έχουν τρία (3) κοινά χαρακτηριστικά:

- Οι υπηρεσίες ιστού εκθέτουν χρήσιμη λειτουργικότητα σε χρήστες του διαδικτύου μέσα από ένα πρότυπο δικτυακό πρωτόκολλο. Στις περισσότερες περιπτώσεις αυτό το πρωτόκολλο είναι το «*SOAP* (Simple Object Access Protocol)».
- Οι υπηρεσίες ιστού παρέχουν ένα τρόπο να περιγράψουν τις διεπαφές τους με αρκετή λεπτομέρεια, ώστε να επιτρέψουν στο χρήστη τους να χτίσει μια εφαρμογή πελάτη, η οποία να επικοινωνήσει μαζί τους. Η περιγραφή συνήθως παρέχεται σε ένα XML έγγραφο, το οποίο ονομάζεται «*WSDL* (Web Services Description Language)».
- Οι υπηρεσίες ιστού καταχωρούνται, ώστε οι δυνητικοί χρήστες να μπορούν να τις βρουν εύκολα. Αυτό γίνεται με το «*UDDI* (Universal Discovery Description and Integration)».

Μια υπηρεσία ιστού μπορεί να είναι *μια επιχειρησιακή διαδικασία* η οποία δρα αυτόνομα, *μια ολοκληρωμένη επιχειρησιακή εργασία*, *μια εφαρμογή, ένας πόρος παροχής υπηρεσιών*. Μερικά απλά παραδείγματα υπηρεσιών ιστού είναι η υπηρεσία η οποία δέχεται το ISBN ενός βιβλίου και επιστρέφει την τιμή του, η υπηρεσία η οποία δέχεται το όνομα μίας χώρας και επιστρέφει τον πληθυσμό της και η υπηρεσία η οποία δέχεται την τιμή της θερμοκρασίας σε βαθμούς κελσίου και επιστρέφει την αντίστοιχη τιμή σε βαθμούς Φαρενάιτ.

Συμπερασματικά, με την χρήση των υπηρεσιών ιστού επιτυγχάνεται η γρήγορη και εύκολη ανάπτυξη πληροφοριακών συστημάτων και η αποδοτική ανάπτυξη εφαρμογών. Μειώνεται το κόστος διασύνδεσης της εφαρμογής και περιορίζεται η πολυπλοκότητα.

Επιπρόσθετα, οι υπηρεσίες ιστού αποτελούνται από ένα σύνολο από πρότυπα τα οποία επιτρέπουν στους προγραμματιστές (developers), να υλοποιήσουν κατανεμημένες εφαρμογές -χρησιμοποιώντας διαφορετικά εργαλεία από διαφορετικούς προμηθευτές- ώστε να κατασκευάσουν εφαρμογές, που χρησιμοποιούν ένα συνδυασμό από ενότητες λογισμικού, οι οποίες καλούνται από συστήματα που ανήκουν σε διαφορετικά τμήματα ενός οργανισμού ή σε διαφορετικούς οργανισμούς.

Τεχνολογίες Υπηρεσιών Ιστού

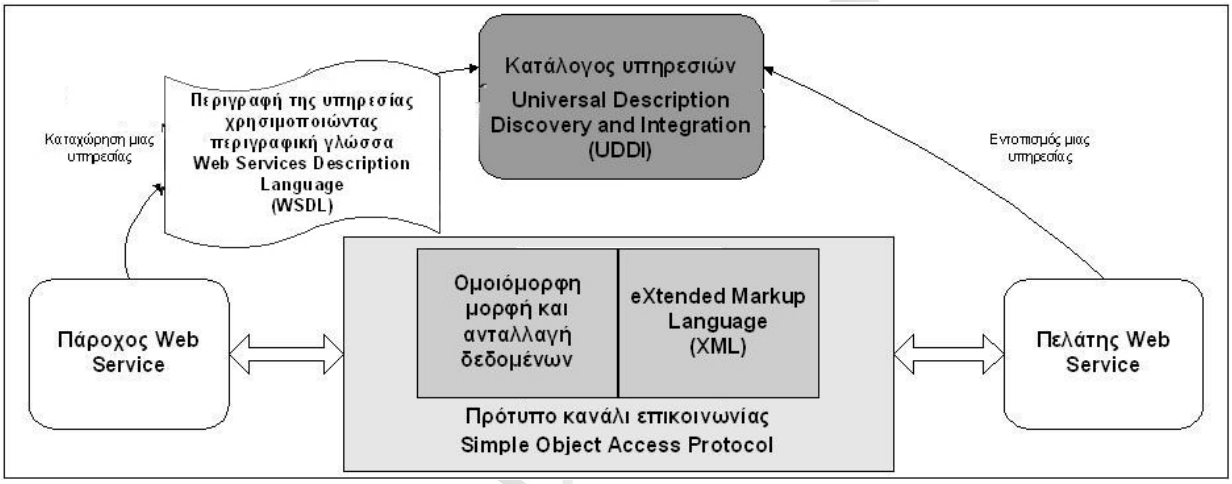
Οι υπηρεσίες ιστού απαιτούν αρκετές συγγενικές τεχνολογίες βασισμένες στην XML, για να μεταφέρουν και να μετασχηματίζουν δεδομένα μέσα και έξω από προγράμματα και βάσεις δεδομένων. Οι βασικές τεχνολογίες στις οποίες βασίζονται οι υπηρεσίες ιστού συνοψίζονται στον παρακάτω πίνακα (Chitnis et al, 2002).

Πίνακας 1: Οι Βασικές Τεχνολογίες στις οποίες Βασίζονται οι Υπηρεσίες Ιστού

Επίπεδο	Τεχνολογία	Περιγραφή
Ομοιόμορφη περιγραφή και ανταλλαγή δεδομένων.	**XML**	Η XML είναι μια περιγραφική γλώσσα (μετα-γλώσσα), η οποία έχει μια καλά καθορισμένη σύνταξη και σημασιολογία. Τα «αυτοπεριγραφικά» χαρακτηριστικά της, την κάνουν ένα απλό αλλά και δυνατό μηχανισμό για τη σύλληψη και την ανταλλαγή στοιχείων μεταξύ των διαφορετικών εφαρμογών.
Πρότυπο κανάλι επικοινωνίας.	**SOAP**	Το SOAP είναι το κανάλι που χρησιμοποιείται για επικοινωνία μεταξύ μιας εφαρμογής, που παρέχεται από μία υπηρεσία ιστού και μιας εφαρμογής πελάτη. Η απλότητα του SOAP έγκειται στο ότι δεν καθορίζει κανένα νέο πρωτόκολλο μεταφοράς. Αντίθετα, επαναχρησιμοποιεί το «Hyper Text Transfer Protocol (HTTP)» ή το «Simple Mail Transfer Protocol (SMTP)» για μεταφορά δεδομένων ως απλά μηνύματα. Αυτή η χρήση, εξασφαλίζει την επικοινωνία μέσω διαδικτύου. Εξαιτίας της χρήσης του SOAP οι ικανότητες των υπηρεσιών ιστού πολλαπλασιάζονται.
Πρότυπη περιγραφική γλώσσα για την περιγραφή των παρεχόμενων υπηρεσιών.	**WSDL**	Οι εφαρμογές που παρέχουν υπηρεσίες ιστού, διαφημίζουν τις διάφορες υπηρεσίες που παρέχουν, χρησιμοποιώντας μια πρότυπη περιγραφική γλώσσα που ονομάζεται WSDL. Η WSDL βασίζεται στην XML και χρησιμοποιεί ένα ειδικό σύνολο ετικετών (tags), για να περιγράψει μια υπηρεσία ιστού, τις υπηρεσίες που παρέχονται, που να εντοπιστεί κ.λ.π. Οι εφαρμογές πελάτες λαμβάνουν πληροφορίες για μια υπηρεσία ιστού πριν

Επίπεδο	Τεχνολογία	Περιγραφή
		από την πρόσβασή τους σε αυτή και τελικά τη χρήση της.
Καταχώρηση και εντοπισμός των παρεχόμενων υπηρεσιών	**UDDI**	Το UDDI, είναι μια κεντρική υπηρεσία καταλόγου και βασίζεται στην XML. Οι εφαρμογές που παρέχουν υπηρεσίες ιστού παρατίθενται σε ένα κατάλογο από παρόχους υπηρεσιών χρησιμοποιώντας το UDDI. Οι εφαρμογές πελάτες εντοπίζουν τους παρόχους εφαρμογών υπηρεσιών ιστού, χρησιμοποιώντας UDDI.

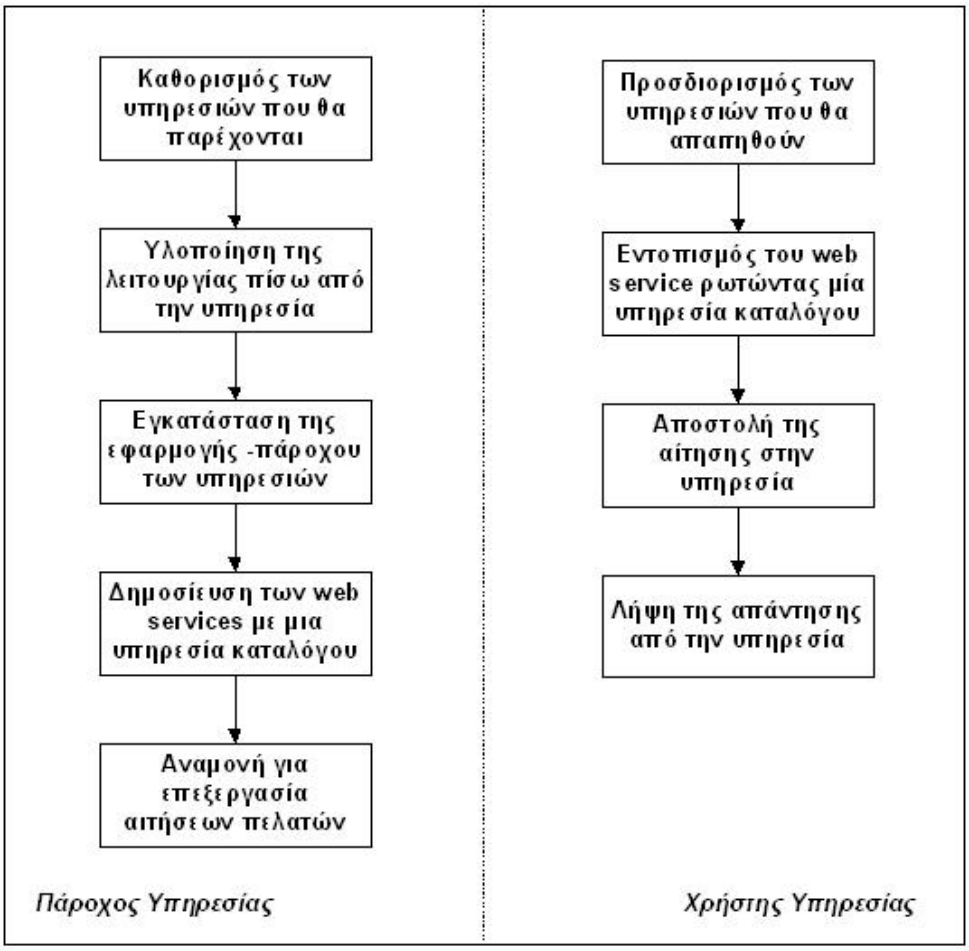
Στην παρακάτω εικόνα αναπαρίστανται οι βασικές τεχνολογίες υπηρεσιών ιστού.



Εικόνα 2: Τεχνολογίες Υπηρεσιών Ιστού

Βασικά Βήματα για την Ανάπτυξη Εφαρμογών με την Χρήση Υπηρεσίων Ιστού

Στην Εικόνα 3 παρουσιάζονται τα βασικά βήματα για την ανάπτυξη μίας εφαρμογής υπηρεσίας ιστού τόσο από την μεριά του παρόχου της όσο και από την μεριά του χρήστη αυτής. Τα βήματα αυτά, είναι τα ίδια ανεξαρτήτου τεχνολογίας και γλώσσας προγραμματισμού.



Εικόνα 3: Βήματα Ανάπτυξης Εφαρμογών Υπηρεσιών Ιστού (Δημητρίου, 2007)

Γλώσσα Σήμανσης XML (XML)

Μία γλώσσα σήμανσης είναι ένας μηχανισμός που καθορίζει δομές σε ένα έγγραφο. Οι δομημένες πληροφορίες περιλαμβάνουν περιεχόμενο και κάποιες διευκρινίσεις για το ρόλο του περιεχόμενου.

Η «*γλώσσα σήμανσης XML* (eXtensible Markup Language)» σχεδιάστηκε από μια Ομάδα Εργασίας κάτω από την επίβλεψη του διεθνούς οργανισμού «World Wide Web Consortium (W3C)» το 1996, για να υποστηρίζει τη δημιουργία και τη διαχείριση δυναμικού περιεχομένου καλύτερα από ότι έκανε η «HyperText Markup Language (HTML)».

Η XML, δίνει στα έγγραφα ένα μεγαλύτερο επίπεδο προσαρμοστικότητας στη μορφή και τη δομή από αυτό που υπήρχε παλαιότερα στην HTML και παρέχει την δυνατότητα στους χρήστες να καθορίζουν τις ετικέτες (tags). Επίσης, είναι ένα σύνολο προκαθορισμένων κανόνων (συντακτικό πλαίσιο) που πρέπει να ακολουθηθεί κατά τη δόμηση των δεδομένων. Επιπρόσθετα, έχει ενσωματωμένο ένα μηχανισμό επικύρωσης δεδομένων, ο οποίος εγγυάται ότι η δομή των δεδομένων που λαμβάνεται είναι έγκυρη. Τέλος, είναι μια γλώσσα ανεξάρτητη από σύστημα και υλικό και χρησιμοποιείται πρώτα από όλα για την ανταλλαγή πληροφοριών μέσω διαδικτύου.

Τα πλεονεκτήματα αυτά, έκαναν την XML το πλέον κατάλληλο πρότυπο για επικοινωνία μεταξύ υπηρεσιών ιστού.

Παράδειγμα Αναπαράστασης Δεδομένων με Χρήση της XML

```
<?xml version="1.0"?>
<note>
      <to>Tove</to>
      <from>Jani</from>
      <heading>Reminder</heading>
      <body>Don't forget me this weekend!</body>
</note>
```

Στο παραπάνω παράδειγμα (Refsnes Data, 2013a), αναπαρίσταται μια υπενθύμιση. Η XML χρησιμοποιεί τις διακριτικές ετικέτες "<>" και "</>", παρόμοια με τις ετικέτες που χρησιμοποιούνται στην HTML. Αυτό συμβαίνει, επειδή η XML είναι μια γλώσσα σήμανσης σαν την HTML με κύρια διαφορά ότι η XML *σχεδιάστηκε για να περιγράφει δεδομένα και να εστιάσει στο τί είναι αυτά τα δεδομένα* ενώ η HTML σχεδιάστηκε για να προβάλει δεδομένα και να εστιάσει στο πώς φαίνονται αυτά τα δεδομένα.

Οι δύο αρχικές δομικές μονάδες XML, που αναλύονται παρακάτω, είναι τα *στοιχεία* (elements) και οι *ιδιότητες* (attributes).

Στοιχεία (Elements)

Τα «*στοιχεία* (elements)» είναι ετικέτες και περιέχουν τιμές. Επιπλέον, είναι δομημένα σαν δένδρο και έχουν συγκεκριμένα *χαρακτηριστικά*, ορισμένα από τα οποία είναι (Ηλιακόπουλος, 2009):

- μπορεί να περιέχουν δεδομένα.
- μπορεί να μην περιέχουν δεδομένα αλλά μόνο ιδιότητες.
- μπορεί να περιέχουν ταυτόχρονα και ιδιότητες αλλά και δεδομένα, αλλά επίσης και στοιχεία-παιδιά.

Επιπλέον, τα στοιχεία έχουν κάποιους κανόνες:

- Όλα τα στοιχεία πρέπει να έχουν ετικέτα κλεισίματος αντίθετα με την HTML όπου υπάρχουν και ετικέτες που δε χρειάζονται κλείσιμο όπως για παράδειγμα η `<br>`.
- Οι ετικέτες των στοιχείων είναι «case sensitive», δηλαδή υπάρχει διαχωρισμός μεταξύ κεφαλαίων και πεζών και τα ονόματά τους υπακούουν σε κανόνες ονοματολογίας.
- Τα στοιχεία πρέπει να είναι τοποθετημένα με την σωστή σειρά (`<b><i>This text is bold and italic</i></b>`).
- Τα έγγραφα της XML πρέπει να έχουν ακριβώς ένα αρχικό στοιχείο (root element).

Ιδιότητες (Attributes)

Οι «*ιδιότητες* (attributes)» δίνουν νόημα και περιγράφουν τα στοιχεία πιο αποτελεσματικά και με σαφήνεια. Με αυτό τον τρόπο, τα δεδομένα σε ένα XML έγγραφο γίνονται αυτοπεριγραφικά. Κύριος σκοπός των ιδιοτήτων είναι να παρέχουν περισσότερη πληροφορία σχετική με ένα στοιχείο.

Όπως και τα στοιχεία έτσι και οι ιδιότητες έχουν *κανόνες* (Ηλιακόπουλος, 2009):

- Οι τιμές των ιδιοτήτων πρέπει να εσωκλείονται σε "" ή σε ''.
- Τα ονόματα των ιδιοτήτων ακολουθούν τους ίδιους κανόνες με αυτά των ετικετών.

Ορισμός Τύπου Εγγράφου (DTD)

Ο «*Ορισμός Τύπου Εγγράφου* (Document Type Definition)» είναι μία προδιαγραφή, η οποία πρέπει να ακολουθηθεί, όταν πρόκειται να δημιουργηθεί ένα XML έγγραφο. Επίσης, υπάρχουν οι «XML parsers», οι οποίοι χρησιμοποιούν το DTD για να ελέγξουν την εγκυρότητα ενός XML εγγράφου.

Ένα DTD καθορίζει τη δομή ενός XML εγγράφου και ελέγχει την *εγκυρότητα* και την *ακεραιότητα* των δεδομένων που περιέχονται σε ένα XML έγγραφο. Το DTD αποτελείται από τα παρακάτω στοιχεία (Ηλιακόπουλος, 2009):

Πίνακας 2: Στοιχεία του DTD

Στοιχείο	Περιγραφή
DTD Element (Στοιχεία)	Μέτα-δεδομένα για ένα στοιχείο. Καθορίζει τι είδους δεδομένα θα έχει το στοιχείο, τον αριθμό των περιστατικών κάθε στοιχείου, τις σχέσεις μεταξύ των στοιχείων και ούτω καθ' εξής.
DTD Attributes (Ιδιότητες)	Καθορίζει διάφορους κανόνες και ορισμούς που σχετίζονται με τα δεδομένα.
DTD Entities (Οντότητες)	Χρησιμοποιείται για να αναφέρει ένα εξωτερικό αρχείο ή για να παρέχει συντομεύσεις σε κοινό κείμενο

XML Schema

Το «*XML Schema*» είναι μία προδιαγραφή, η οποία πρέπει να ακολουθηθεί, όταν πρόκειται να δημιουργηθεί ένα XML έγγραφο. Δημιουργήθηκε επειδή το DTD δεν υποστηρίζει ισχυρούς τύπους δεδομένων, δεν είναι επεκτάσιμο και η σύνταξη του είναι διαφορετική από αυτήν της XML.

Τα κυριότερα χαρακτηριστικά του «XML Schema» είναι τα παρακάτω (Ηλιακόπουλος, 2009):

- Η σύνταξη είναι όμοια με της XML. Αυτό σημαίνει ότι ο χρήστης μπορεί να επεξεργαστεί το «schema» με οποιοδήποτε επεξεργαστή XML.
- Δεν καθορίζονται μόνο οι βασικοί τύποι δεδομένων όπως αλφαριθμητικό, ακέραιος, πραγματικός και ούτω καθ' εξής, αλλά ο χρήστης μπορείς να καθορίσει τους δικούς του τύπους δεδομένων. Παραδείγματος χάριν, `<xs:element name="name" type="xs:string" />`.

  Οι νέοι τύποι μπορεί να είναι απλοί ή σύνθετοι. Οι σύνθετοι τύποι μπορεί να περιέχουν και άλλα στοιχεία ή και ιδιότητες, ενώ οι απλοί τύποι μπορούν να περιέχουν μόνο δεδομένα.

- Παρέχει επικύρωση βασισμένη στο περιεχόμενο (content-based validation). Μπορεί δηλαδή, να ορίσει την σειρά με την οποία τα στοιχεία-παιδιά εμφανίζονται. Επίσης παρέχει επικύρωση στους ίδιους τους τύπους δεδομένων.

  Για παράδειγμα, ο χρήστης μπορεί να ορίσει έναν απλό τύπο «year» με τιμές μεταξύ 2000 και 2100:

```
<xs:simpleType name="year">
      <xs:restriction base="xs:integer">
          <xs:minInclusive value="2000"/>
          <xs:maxInclusive value="2100"/>
      </xs:restriction>
</xs:simpleType>
```

  Παρομοίως οι σύνθετοι τύποι μπορεί να ορίσουν τη σειρά, με την οποία τα στοιχεία-παιδιά θα εμφανίζονται.

```
<complexType name="Employee">
      <xs:sequence>
          <xs:element name="Name" type="xs:string" />
          <xs:element name="Address" type="xs:string" />
          <xs:element name="Phone" type="xs:string" />
      </xs:sequence>
</xs:complexType>
```

- Παρέχει τη δυνατότητα στον χρήστη να παράγει νέους τύπους δεδομένων, βάσει παλαιών τύπων.
- Παρέχει υποστήριξη για «Namespaces» (χρησιμοποιώντας URI). Δηλαδή, παρέχει σε κάθε στοιχείο ένα μοναδικό αναγνωριστικό, με το οποίο αποφεύγονται συγκρούσεις ονομάτων μεταξύ των στοιχείων. Στην ουσία, βοηθάει στο να ξεχωρίζουν στοιχεία και ιδιότητες με ίδιο όνομα και διαφορετικό νόημα.
- Τέλος είναι εύκολα επεκτάσιμο και επομένως, μπορεί να ενσωματώσει και άλλες λειτουργίες στο μέλλον.

Παράδειγμα XML Schema

Στο παρακάτω παράδειγμα (Refsnes Data, 2013c), αναπαρίσταται ένα «XML Schema» με το όνομα «note.xsd» και η αναφορά σε αυτό μέσα σε ένα XML αρχείο.

XML Schema:

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
      <xs:element name="note">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="to" type="xs:string"/>
```

```
            <xs:element name="from" type="xs:string"/>
            <xs:element name="heading" type="xs:string"/>
            <xs:element name="body" type="xs:string"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
</xs:schema>
```

XML αρχείο:

```
<?xml version="1.0"?>
<note
    xmlns="http://www.w3schools.com"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.w3schools.com note.xsd">

      <to>Tove</to>
      <from>Jani</from>
      <heading>Reminder</heading>
      <body>Don't forget me this weekend!</body>
</note>
```

Απλό Πρωτόκολλο Πρόσβασης σε Αντικείμενα (SOAP)

Καθώς η XML είναι η γλώσσα που χρησιμοποιείται για την αναπαράσταση δεδομένων και της μορφής τους σε ένα έγγραφο, θα πρέπει να υπάρχει και ένα πρωτόκολλο για την μεταφορά των δεδομένων ανάμεσα στον αποστολέα και στον παραλήπτη, είτε αυτή πρόκειται να γίνει ανάμεσα σε προγράμματα λογισμικού, είτε ανάμεσα σε μηχανήματα ή οργανισμούς. Το πρωτόκολλο αυτό ονομάζεται «*Απλό Πρωτόκολλο Πρόσβασης σε Αντικείμενα* (Simple Object Access Protocol)»

Σύμφωνα με το W3C, το SOAP είναι ένα ελαφρύ πρωτόκολλο προορισμένο για την ανταλλαγή δομημένων πληροφοριών σε ένα αποκεντρωμένο, διανεμημένο περιβάλλον. Χρησιμοποιεί τεχνολογίες XML για να καθορίσει ένα επεκτάσιμο πλαίσιο παρέχοντας μια δομή μηνυμάτων, η οποία μπορεί να ανταλλαχθεί πάνω από ποικίλα πρωτόκολλα διαδικτύου, συμπεριλαμβανομένων των των «HTTP», «Simple Mail Transfer Protocol (SMTP)» και «File Transfer Protocol (FTP)». Έχει σχεδιαστεί να είναι ανεξάρτητο από οποιοδήποτε προγραμματιστικό μοντέλο και σημασιολογία υλοποίησης.

Οι δύο βασικοί στόχοι, κατά το σχεδιασμό του SOAP είναι η *απλότητα* και η *επεκτασιμότητα*. Για να επιτευχθούν οι ανωτέρω στόχοι, το SOAP παραλείπει χαρακτηριστικά γνωρίσματα, τα οποία συνήθως συναντούνται σε κατανεμημένα συστήματα, από το πλαίσιο μηνυμάτων. Μερικά από αυτά τα γνωρίσματα είναι η «*αξιοπιστία* (reliability)», η «*ασφάλεια* (security)», ο «*συσχετιμός* (correlation)», η «*δρομολόγηση* (routing)» και τα «*σχέδια ανταλλαγής μηνυμάτων* (message exchange patterns - MPEs)».

Συνοψίζοντας, τα χαρακτηριστικά γνωρίσματα του πρωτόκολλου SOAP είναι ότι είναι απλό, *ανεξάρτητο από πλατφόρμα και γλώσσα προγραμματισμού*, *ευέλικτο*, *επεκτάσιμο* και βασίζεται στην γλώσσα XML.

Δομή ενός Μηνύματος SOAP

Ένα μήνυμα SOAP είναι ένα έγγραφο XML, το οποίο περιέχει τα παρακάτω στοιχεία (elements) (Refsnes Data, 2013b):

- Ένα απαιτούμενο στοιχείο «***Envelope***», το οποίο προσδιορίζει ότι το XML έγγραφο είναι ένα SOAP μήνυμα και καθορίζει την αρχή και το τέλος του μηνύματος.
- Ένα προαιρετικό στοιχείο ***Header***», το οποίο περιέχει πληροφορίες επικεφαλίδας. Είναι ένας ευέλικτος μηχανισμός για πρόσθεση χαρακτηριστικών στο SOAP μήνυμα.
- Ένα απαιτούμενο στοιχείο «***Body***», το οποίο παρέχει έναν απλό μηχανισμό για ανταλλαγή υποχρεωτικών πληροφοριών, οι οποίες προορίζονται για τον τελικό αποδέκτη του μηνύματος.
- Ένα προαιρετικό στοιχείο «***Fault***», το οποίο περιέχει πληροφορίες για λάθη που τυχόν εμφανίστηκαν κατά την επεξεργασία του μηνύματος. Αυτό το στοιχείο εμφανίζεται μόνο σε απαντητικά μηνύματα και δεν πρέπει να εμφανίζεται πάνω από μία φορά μέσα στο «Body» του μηνύματος.

Η βασική δομή ενός SOAP μηνύματος είναι η παρακάτω:

```
<?xml version="1.0"?>
<soap:Envelope
    xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
    soap:encodingStyle=" http://www.w3.org/2001/12/soap-encoding">

<soap:Header>
      ...
</soap:Header>

<soap:Body>
      ...
</soap:Body>

</soap:Envelope>
```

Όταν ένα μήνυμα SOAP περιέχει το στοιχείο «Fault», έχει την παρακάτω μορφή (Refsnes Data, 2013b):

```
<?xml version="1.0"?>
<soap:Envelope
    xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
    soap:encodingStyle=" http://www.w3.org/2001/12/soap-encoding">

<soap:Header>
```

```
      ...
</soap:Header>

<soap:Body>
      ...
         <soap:Fault>
            ...
         </soap:Fault>
</soap:Body>
</soap:Envelope>
```

Μοντέλα Ανταλλαγής Μηνυμάτων

Το SOAP είναι ένα πλαίσιο μηνυμάτων για ανταλλαγή μηνυμάτων σε XML μορφή μεταξύ ενός *αρχικού αποστολέα* και ενός *τελικού αποδέκτη*. Η πιο απλή περίπτωση ανταλλαγής μηνυμάτων μεταξύ των δύο αυτών κόμβων είναι η μορφή *αίτηση-απάντηση* (request-response).

Πλαίσιο Συνδέσεων (Binding Framework)

Τα μηνύματα SOAP μπορούν να ανταλλάσσονται χρησιμοποιώντας μια πληθώρα από πρωτόκολλα δικτύου συμπεριλαμβανομένων και πρωτοκόλλων επιπέδου εφαρμογών (application layer protocols). Η προδιαγραφή για το πώς SOAP μηνύματα μπορούν να μεταφέρονται από ένα κόμβο σε ένα άλλο χρησιμοποιώντας ένα πρωτόκολλο, ονομάζεται «*σύνδεση SOAP* (SOAP binding)» (Δημητρίου, 2007).

Σύνδεση HTTP (HTTP Binding)

Το HTTP έχει ένα ευρέως γνωστό μοντέλο σύνδεσης και μορφή ανταλλαγής μηνυμάτων. Ο πελάτης αναγνωρίζει τον εξυπηρετητή μέσω ενός «URI», συνδέεται σε αυτόν χρησιμοποιώντας το «TCP/IP», εκτελεί μία αίτηση HTTP και λαμβάνει μία απάντηση HTTP πάνω από την ίδια σύνδεση TCP.

Το HTTP συνδέει το μήνυμα αίτησης με το μήνυμα απάντησης. Για το λόγο αυτό, μια εφαρμογή που χρησιμοποιεί αυτή τη σύνδεση μπορεί να επιλέξει να συνδέσει ένα SOAP μήνυμα που στάλθηκε στο σώμα μιας αίτησης HTTP, με ένα SOAP μήνυμα που επιστράφηκε στο σώμα μιας απάντησης HTTP.

Η απλότητα χρήσης του HTTP είναι και ο λόγος για τον οποίο είναι το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο για την αποστολή SOAP μηνυμάτων (Δημητρίου, 2007).

Παράδειγμα SOAP μηνύματος

Στα παρακάτω παράδειγμα (Refsnes Data, 2013c), αναπαρίσταται, με την μορφή SOAP μηνυμάτων, η αίτηση και η απάντηση μιας διαδικασίας με όνομα «GetStockPrice», η οποία δέχεται ένα όρισμα με όνομα «StockName» τύπου αλφαριθμητικού και επιστρέφει μία τιμή τύπου πραγματικού, μέσω HTTP σύνδεσης.

Αίτηση:

```
POST /InStock HTTP/1.1
Host: www.example.org
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>
<soap:Envelope
    xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
    soap:encodingStyle=" http://www.w3.org/2001/12/soap-encoding">

      <soap:Body xmlns:m="http://www.example.org/stock">
         <m:GetStockPrice>
            <m:StockName>IBM</m:StockName>
         </m:GetStockPrice>
      </soap:Body>

</soap:Envelope>
```

Απάντηση:

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>
<soap:Envelope
    xmlns:soap="http://www.w3.org/2003/12/soap-envelope"
    soap:encodingStyle=" http://www.w3.org/2001/12/soap-encoding">

      <soap:Body xmlns:m="http://www.example.org/stock">
         <m:GetStockPriceResponse>
            <m:Price>34.5</m:Price>
         </m:GetStockPriceResponse>
      </soap:Body>

</soap:Envelope>
```

Γλώσσα Περιγραφής Υπηρεσιών Ιστού (WSDL)

Για να ολοκληρωθεί η αρχιτεκτονική επικοινωνίας των υπηρεσιών ιστού, πρέπει να καθοριστεί το πως οι χρήστες θα έχουν πρόσβαση σε μία υπηρεσία, μόλις αυτή τεθεί σε εφαρμογή. Αυτό επιτυγχάνεται με την προδιαγραφή «*Γλώσσα Περιγραφής Υπηρεσιών Ιστού* (Web Services Description Language)», που παρέχει ένα συμβόλαιο μεταξύ του αιτούντος και του παροχέα της υπηρεσίας.

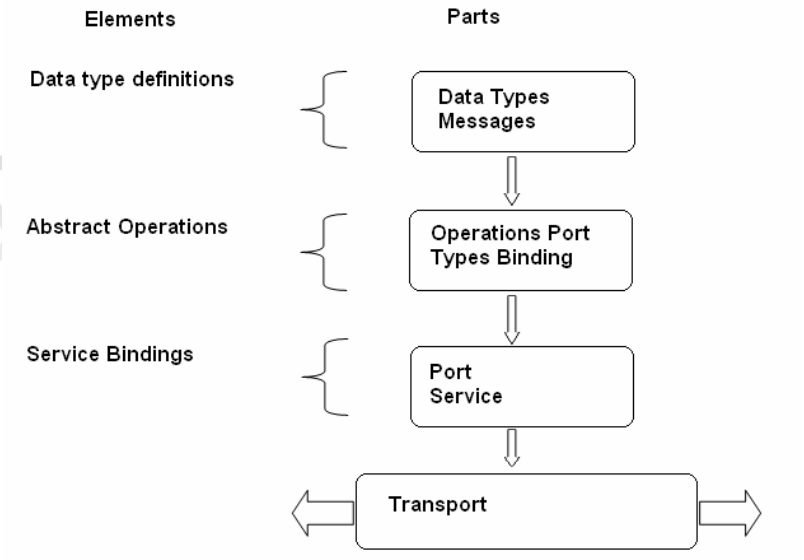
Η WSDL περιγράφει *ένα σύνολο από μηνύματα και το πώς αυτά τα μηνύματα ανταλλάσσονται*. Παρέχει ένα κοινό τρόπο στον οποίο παρουσιάζονται οι τύποι των δεδομένων που λαμβάνουν χώρα στα μηνύματα, οι λειτουργίες οι οποίες πρόκειται να εκτελεστούν στα μηνύματα και η αντιστοίχιση των μηνυμάτων πάνω σε συναλλαγές του δικτύου.

Επιπλέον, η WSDL καθορίζει τι πρέπει να περιέχει ένα μήνυμα και πώς πρέπει να είναι ένα μήνυμα απάντησης με σαφή σήμανση. Η σήμανση που χρησιμοποιείται σε ένα αρχείο WSDL, προκειμένου να περιγράψει μορφές μηνυμάτων, βασίζεται στο πρότυπο «XML Schema», το οποίο σημαίνει ότι η WSDL είναι ταυτόχρονα ανεξάρτητη από γλώσσα προγραμματισμού και βασισμένη σε πρότυπα. Αυτό το γεγονός την κάνει κατάλληλη, για να περιγράψει διεπαφές υπηρεσιών ιστού, οι οποίες είναι προσβάσιμες από μία μεγάλη ποικιλία πλατφορμών και γλωσσών προγραμματισμού (Ηλιακόπουλος, 2009).

Τέλος, εκτός του ότι η WSDL περιγράφει τα περιεχόμενα των μηνυμάτων, ορίζει πού είναι διαθέσιμη μία υπηρεσία και ποιά πρωτόκολλα επικοινωνίας χρησιμοποιούνται για να επικοινωνήσει ο χρήστης με αυτή την υπηρεσία.

Τεχνική Περιγραφή της WSDL

Η WSDL παρέχει ένα τρόπο στους παροχείς υπηρεσιών για να περιγράψουν τη βασική μορφή των αιτήσεων και απαντήσεων των υπηρεσιών, πάνω από διαφορετικά πρωτόκολλα και κωδικοποιήσεις. Έχει XML μορφή και χρησιμοποιείται για να περιγράψει ***τί*** μπορεί να κάνει μια υπηρεσία, ***πού*** βρίσκεται και ***πώς*** να την καλέσει κανείς. Επίσης, διαιρείται σε τρία βασικά στοιχεία και επτά τμήματα, τα όποια απεικονίζονται στην παρακάτω εικόνα (Newcomer, 2002).



Εικόνα 4: Βασικά Στοιχεία και Τμήματα της WSDL

Κάθε βασικό στοιχείο είτε μπορεί να καθοριστεί σε ένα ξεχωριστό XML έγγραφο και να εισαχθεί σε διαφορετικούς συνδυασμούς, για να δημιουργήσει μια τελική περιγραφή υπηρεσιών ιστού είτε όλα τα βασικά στοιχεία μπορούν να οριστούν σε ένα μόνο έγγραφο. Τα «*Data type definitions*» (Data types, Messages) προσδιορίζουν τη δομή και το περιεχόμενο των μηνυμάτων. Τα «*Abstract Operations*» (Operations, Port Types, Binding) προσδιορίζουν τις λειτουργίες που εκτελούνται στο περιεχόμενο του μηνύματος και τα «*Service Bindings*» (Port, Service) προσδιορίζουν τη μετάδοση δεδομένων, η οποία θα μεταφέρει το μήνυμα στον προορισμό του.

Πιο αναλυτικά τα στοιχεία που χρησιμοποιεί ένα WSDL αρχείο είναι (Δημητρίου, 2007):

- «***types***», είναι ένα περίβλημα για ορισμούς τύπων δεδομένων χρησιμοποιώντας ένα σύστημα τύπων (όπως για παράδειγμα το XML Schema).
- «***message***», είναι ένας περιγραφικός ορισμός των δεδομένων που ανταλλάσσονται.
- «***operation***», είναι μία περιγραφή μίας λειτουργίας που υποστηρίζεται από μία υπηρεσία
- «***portType***», είναι ένα περιγραφικό σύνολο από λειτουργίες που υποστηρίζονται από ένα ή περισσότερα τελικά σημεία.
- «***binding***», είναι ένα συγκεκριμένο πρωτόκολλο και μορφή δεδομένων για ένα συγκεκριμένο τύπο τελικών σημείων.
- «***port***», είναι ένα μοναδικό τελικό σημείο που ορίζεται σαν συνδυασμός μίας σύνδεσης και μιας διεύθυνσης δικτύου.
- «***service***», είναι μία συλλογή από σχετικά τελικά σημεία.

Παράδειγμα WSDL

Το παρακάτω παράδειγμα (Δημητρίου, 2007), είναι ένα έγγραφο WSDL που περιγράφει μια υπηρεσία για τις τιμές μετοχών:

```
<?xml version="1.0"?>
<definitions name="StockQuote"
   targetNamespace="http://example.com/stockquote.wsdl"
         xmlns:tns="http://example.com/stockquote.wsdl"
         xmlns:xsd1="http://example.com/stockquote.xsd"
         xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
         xmlns="http://schemas.xmlsoap.org/wsdl/">

      <types>
        <schema targetNamespace="http://example.com/stockquote.xsd"
          xmlns="http://www.w3.org/2000/10/XMLSchema">
         <element name="TradePriceRequest">
           <complexType>
             <all>
                <element name="tickerSymbol" type="string"/>
             </all>
            </complexType>
```

```
            </element>
            <element name="TradePrice">
             <complexType>
               <all>
                  <element name="price" type="float"/>
               </all>
             </complexType>
            </element>
      </schema>
    </types>

    <message name="GetLastTradePriceInput">
      <part name="body" element="xsd1:TradePriceRequest"/>
    </message>

    <message name="GetLastTradePriceOutput">
      <part name="body" element="xsd1:TradePrice"/>
    </message>

    <portType name="StockQuotePortType">
      <operation name="GetLastTradePrice">
      <input message="tns:GetLastTradePriceInput"/>
      <output message="tns:GetLastTradePriceOutput"/>
    </operation>
    </portType>

    <binding name="StockQuoteSoapBinding" type="tns:StockQuotePortType">
      <soap:binding style="document"
         transport="http://schemas.xmlsoap.org/soap/http"/>
      <operation name="GetLastTradePrice">
       <soap:operation soapAction="http://example.com/GetLastTradePrice"/>
       <input>
          <soap:body use="literal"/>
       </input>
       <output>
          <soap:body use="literal"/>
       </output>
      </operation>
    </binding>

    <service name="StockQuoteService">
       <documentation>My first service</documentation>
```

```
         <port name="StockQuotePort" binding="tns:StockQuoteBinding">
            <soap:address location="http://example.com/stockquote"/>
         </port>
      </service>

</definitions>
```

Πρωτόκολλο Περιγραφής, Ανακάλυψης και Ολοκλήρωσης (UDDI)

Το «*Πρωτόκολλο Περιγραφής, Ανακάλυψης και Ολοκλήρωσης* (Universal Description, Discovery and Integration)», ως τεχνική προδιαγραφή, παρέχει μια μέθοδο για δημοσίευση και εύρεση των περιγραφών μιας υπηρεσίας. Είναι μια κεντρική υπηρεσία καταλόγου, όπου υπηρεσίες ιστού μπορούν να καταχωρηθούν και να προσδιοριστούν σε έναν παροχέα υπηρεσιών.

Βασισμένο σε ένα κοινό σύνολο από βιομηχανικά πρότυπα, συμπεριλαμβανομένων των HTTP, XML, XML Schema και SOAP, το UDDI παρέχει μια διαλειτουργική, θεμελιώδη υποδομή για ένα περιβάλλον λογισμικού προσανατολισμένο στις υπηρεσίες τόσο για δημόσια διαθέσιμες υπηρεσίες όσο και για υπηρεσίες που εκτίθενται μόνο εσωτερικά ενός οργανισμού.

Η δομή των δεδομένων τα οποία αποθηκεύονται στον κατάλογο είναι σε μορφή XML. Τα δεδομένα, τα οποία συλλέγονται εντός του καταλόγου χωρίζονται σε τρεις κατηγορίες: *λευκές σελίδες* (white pages), *κίτρινες σελίδες* (yellow pages) και *πράσινες σελίδες* (green pages).

Ένας κατάλογος UDDI έχει δύο ειδών πελάτες: επιχειρήσεις που θέλουν να δημοσιεύσουν μια υπηρεσία (και τις διεπαφές της), και πελάτες που θέλουν να χρησιμοποιήσουν συγκεκριμένες υπηρεσίες και συνδέονται προγραμματιστικά με αυτές.

Ο παρακάτω πίνακας (Ηλιακόπουλος, 2009; Vasudevan, 2001), περιγράφει περιληπτικά τις προσφερόμενες υπηρεσίες του UDDI:

Πίνακας 3: Προσφερόμενες Υπηρεσίες του UDDI

Πληροφορία	**Λειτουργίες**	**Λεπτομέρειες (που υποστηρίζονται από το API)**
White pages: Πληροφορίες όπως το όνομα, η διεύθυνση, το τηλέφωνο και άλλες πληροφορίες επικοινωνίας για μία επιχείρηση.	**Publish**: Πώς ο προμηθευτής μιας υπηρεσίας ιστού καταχωρεί τον εαυτό του.	**Business Information:** Περιλαμβάνεται σε ένα αντικείμενο «*BusinessEntity*», το οποίο με τη σειρά του περιλαμβάνει πληροφορίες για υπηρεσίες, κατηγορίες, επαφές, «URLs», και άλλα αναγκαία στοιχεία για να αλληλεπιδράσουμε με μία επιχείρηση.
Yellow Pages: Πληροφορίες που κατηγοριοποιούν επιχειρήσεις. Βασίζονται σε υπάρχοντα πρότυπα κατηγοριοποίησης (μη ηλεκτρονικά).	**Find:** Πώς μία εφαρμογή βρίσκει μια συγκεκριμένη υπηρεσία ιστού.	**Service Information**: Περιγράφει μία ομάδα από υπηρεσίες ιστού. Αυτές περιλαμβάνονται σε ένα αντικείμενο «*BusinessService*».

Green Pages:	**Bind**:	**Binding Information**:
Τεχνικές πληροφορίες για τις υπηρεσίες ιστού που παρέχονται από μία επιχείρηση.	Πώς μία εφαρμογή συνδέεται, και αλληλεπιδρά με μια υπηρεσία ιστού, εφόσον αυτή βρεθεί.	Οι απαραίτητες τεχνικές λεπτομέρειες για την κλήση μιας υπηρεσίας ιστού. Περιλαμβάνουν τα «URLs», πληροφορίες για ονόματα μεθόδων, τύπους ορισμάτων και ούτω καθ'εξής. Το αντικείμενο «**BindingTemplate**» αναπαριστά αυτά τα δεδομένα. **Service Specification Detail**: Πρόκειται για μεταδεδομένα, για διάφορες προδιαγραφές που υλοποιούνται από μια υπηρεσία ιστού και ονομάζονται «*tModels*».

Η UDDI καταχώρηση λειτουργεί όπως το «Domain Name System (DNS)». Οι εταιρείες μπορούν να καταχωρηθούν σε οποιονδήποτε «host», όπως IBM, HP, SAP, ή Microsoft και οι πληροφορίες που παρέχουν, τοποθετούνται στην αντίστοιχη βάση του «host».

Οι «host» αναρτούν WSDL περιγραφές των υπηρεσιών ιστού για καταχώρηση και ανακάλυψη. Η WSDL παρέχει ξεχωριστά αρχεία για καταχώριση και ανακάλυψη υπηρεσιών, χρησιμοποιώντας την δική της XML μορφή εγγράφου. Κάθε ένας χρήστης μπορεί να διαβάζει τον κατάλογο, να ερευνά για μια επιθυμητή υπηρεσία και να φορτώνει την περιγραφή σε περίπτωση που ταιριάζει από οποιονδήποτε «host». Οι χρήστες δεν θα διαβάσουν απευθείας μια UDDI καταχώρηση από τη στιγμή που η πληροφορία, η οποία είναι αποθηκευμένη εντός του καταλόγου δεν είναι απαραίτητα φιλική προς τον αναγνώστη.

Όταν χρειαστεί να γίνει ενημέρωση των δεδομένων, ο χρήστης θα πρέπει να επιστρέψει στον «host», όπου έγινε η αρχική καταχώρηση των δεδομένων, έτσι ώστε να μπορέσει να εκτελέσει τη λειτουργία της ενημέρωσης.

Παράδειγμα UDDI

Στο παρακάτω παράδειγμα (Δημητρίου, 2007), φαίνεται ένα ερώτημα σε SOAP και η απάντηση από ένα κατάλογο UDDI:

Ερώτημα: το παρακάτω ερώτημα, τοποθετημένο σε ένα φάκελο SOAP, επιστρέφει λεπτομέρειες για τη Microsoft:

```
<find_business generic="1.0" xmlns="urn:uddi-org:api">
      <name>Microsoft</name>
</find_business>
```

Αποτέλεσμα: Λεπτομερείς καταχωρήσεις για τη Microsoft, οι οποίες περιλαμβάνουν πληροφορίες και για το ίδιο το UDDI.

```
<businessList generic="1.0"
   operator="Microsoft Corporation"
   truncated="false"
   xmlns="urn:uddi-org:api">
<businessInfos>
 <businessInfo
```

```
   businessKey="0076B468-EB27-42E5-AC09-9955CFF462A3">
 <name>Microsoft Corporation</name>
 <description xml:lang="en">
      Empowering people through great software -
      any time, any place and on any device is Microsoft's
      vision. As the worldwide leader in software for personal
      business computing, we strive to produce innovative
      products and services that meet our customer's
 </description>
<serviceInfos>
 <serviceInfo
      businessKey="0076B468-EB27-42E5-AC09-9955CFF462A3"
      serviceKey="1FFE1F71-2AF3-45FB-B788-09AF7FF151A4">
      <name>Web services for smart searching</name>
 </serviceInfo>
 <serviceInfo
      businessKey="0076B468-EB27-42E5-AC09-9955CFF462A3"
      serviceKey="8BF2F51F-8ED4-43FE-B665-38D8205D1333">
      <name>Electronic Business Integration Services</name>
 </serviceInfo>
 <serviceInfo
      businessKey="0076B468-EB27-42E5-AC09-9955CFF462A3"
      serviceKey="611C5867-384E-4FFD-B49C-28F93A7B4F9B">
      <name>Volume Licensing Select Program</name>
 </serviceInfo>
 <serviceInfo
      businessKey="0076B468-EB27-42E5-AC09-9955CFF462A3"
      serviceKey="A8E4999A-21A3-47FA-802E-EE50A88B266F">
      <name>UDDI Web Sites</name>
 </serviceInfo>
</serviceInfos>
</businessInfo>
</businessInfos>
</businessList>
```

Κεφάλαιο 2: Επιθέσεις Ασφάλειας στις Υπηρεσίες Ιστού

Εισαγωγή

Το κλειδί για την ασφάλεια της αρχιτεκτονικής κάθε εφαρμογής είναι η ερμηνεία του προφίλ της απειλής και το πόσο πιθανός είναι ο κίνδυνος της απειλής. Ο κίνδυνος υπολογίζεται βάσει ενός αξιολογημένου επιπέδου αδυναμιών πλατφορμών ή ευπαθειών μαζί με την πιθανότητα πραγματοποίησης της επίθεσης ή της απειλής. Κάθε φορά που εισάγεται μία νέα τεχνολογία, το προφίλ του κινδύνου αλλάζει.

Ως «*επίθεση*» ορίζεται οποιαδήποτε προσβολή ενός συστήματος που προκύπτει από σκόπιμη χρήση μίας ευπάθειάς του, ενώ ως «*hacking*» ορίζεται η οποιαδήποτε τροποποίηση υλικού ή λογισμικού υπολογιστών, ώστε να επιτευχθεί κάποιος διαφορετικός σκοπός από αυτόν του δημιουργού.

Επειδή, τα παραπάνω ισχύουν και για τις υπηρεσίες ιστού, στο κεφάλαιο αυτό περιγράφονται οι επιθέσεις ασφάλειας σε αυτές τις υπηρεσίες.

Συλλογή Πληροφοριών (Footprinting)

Η «*συλλογή πληροφοριών*» είναι το στάδιο που προηγείται κάθε επιθέσεως. Ο επιτιθέμενος προσπαθεί να συγκεντρώσει όσες περισσότερες πληροφορίες μπορεί για έναν πάροχο υπηρεσιών ιστού. Πληροφορίες, όπως η οργάνωση, η επιχειρησιακή περιγραφή, οι διαθέσιμες υπηρεσίες ιστού, οι τεχνικές απαιτήσεις για πρόσβαση κτλ. μπορούν να βρεθούν σε ένα UDDI κατάλογο.

Παράδειγμα 1: Συλλογή Πληροφοριών για Όνομα Εταιρείας

Στο παρακάτω παράδειγμα (Shah, 2007), αναπαρίσταται, με την μορφή SOAP μηνυμάτων, η αίτηση και η απάντηση για τη «συλλογή πληροφοριών» περί του *ονόματος* της εταιρείας «amazon».

Αίτηση:

```
POST /inquire HTTP/1.1
Host: uddi.microsoft.com
Content-Type: text/xml;
charset=utf-8
Content-Length: 229
SOAPAction: ""

<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/">
     <Body>
        <find_business generic="2.0" maxRows="100" xmlns="urn:uddi-
           org:api_v2">
          <name>amazon</name>
        </find_business>
```

```
    </Body>
</Envelope>
```

Απάντηση:

```
HTTP/1.1 200 OK
Date: Tue, 28 Sep 2004 09:53:53 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 1339

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <soap:Body>
         <businessList generic="2.0" operator="Microsoft Corporation"
            truncated="false" xmlns="urn:uddi-org:api_v2">
          <businessInfos>
           <businessInfo businessKey="bfb9dc23-adec-4f73-bd5f-5545abaeaa1b">
             <name xml:lang="en-us">Amazon Web Services for Testing</name>
             <description xml:lang="ko">Amazon Web Services 2.0 - We now
                 offer software developers the opportunity to integrate
                 Amazon.com </description>
           <serviceInfos>
            <serviceInfo serviceKey="41213238-1b33-40f4-8756-c89cc3125ecc"
               businessKey="bfb9dc23-adec-4f73-bd5f-5545abaeaa1b">
             <name xml:lang="enus">Amazon Web Services 2.0</name>
            </serviceInfo>
           </serviceInfos>
           </businessInfo>

           <businessInfo businessKey="18b7fde2-d15c-437c-8877-ebec8216d0f5">
             <name xml:lang="en">Amazon.com</name>
             <description xml:lang="en"> E-commerce website and platform for
                  finding, discovering, and buying products online
             </description>
           <serviceInfos>
```

```
            <serviceInfo serviceKey="ba6d9d56-ea3f-4263-a95aeeb17e5910db"
               businessKey="18b7fde2-d15c-437c-8877-ebec8216d0f5">
             <name xml:lang="en">Amazon.com Web Services </name>
            </serviceInfo>
           </serviceInfos>
           </businessInfo>

          </businessInfos>
         </businessList>
      </soap:Body>
</soap: Envelope>
```

Παράδειγμα 2: Συλλογή Πληροφοριών για Υπηρεσίες Εταιρείας

Στο παρακάτω παράδειγμα (Shah, 2007), αναπαρίσταται, με την μορφή SOAP μηνυμάτων, η αίτηση και η απάντηση για τη «συλλογή πληροφοριών» περί των *υπηρεσιών* της εταιρείας «amazon».

Αίτηση:

```
POST /inquire HTTP/1.1
Host: uddi.microsoft.com
Content-Type: text/xml;
charset=utf-8
Content-Length: 213
SOAPAction: ""

<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/">
     <Body>
        <find_service generic="2.0" xmlns="urn:uddi-org:api_v2">
           <name>amazon</name>
     </find_service>
     </Body>
</Envelope>
```

Απάντηση:

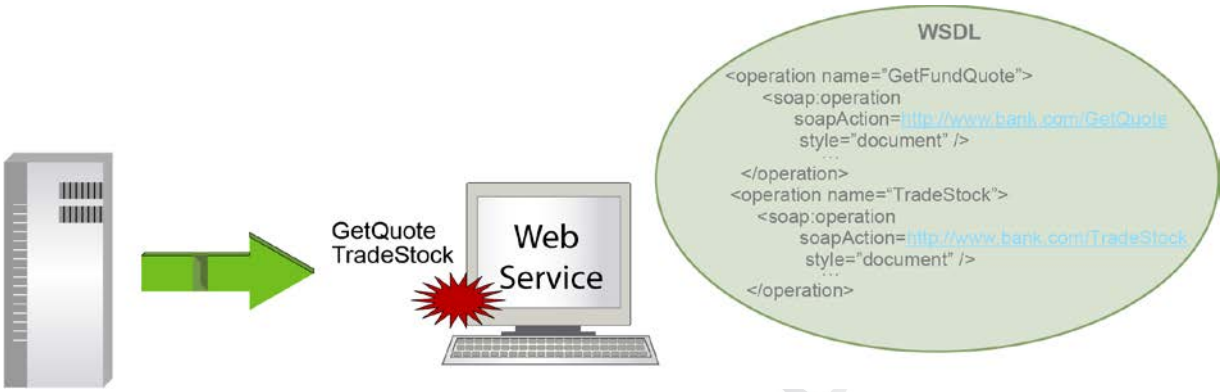
```
HTTP/1.1 200 OK
Date: Tue, 28 Sep 2004 10:07:42 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.432
```

```
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 1272

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema- instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <soap:Body>
         <serviceList generic="2.0" operator="Microsoft Corporation"
            truncated="false" xmlns="urn:uddi-org:api_v2">
           <serviceInfos>
              <serviceInfo serviceKey="6ec464e0-2f8d-4daf-b4dd-5dd4ba9dc8f3"
               businessKey="914374fb-f10f-4634-b8ef- c9e34e8a0ee5">
                 <name xml:lang="en-us">Amazon Research Pane</name>
           </serviceInfo>
           <serviceInfo serviceKey="41213238-1b33-40f4-8756-c89cc3125ecc"
               businessKey="bfb9dc23-adec-4f73-bd5f- 5545abaeaa1b">
                 <name xml:lang="en-us">Amazon Web Services 2.0</name>
           </serviceInfo>
           <serviceInfo serviceKey="ba6d9d56-ea3f-4263-a95a-eeb17e5910db"
               businessKey="18b7fde2-d15c-437c-8877- ebec8216d0f5">
                 <name xml:lang="en">Amazon.com Web Services</name>
           </serviceInfo>
           <serviceInfo serviceKey="bc82a008-5e4e-4c0c-8dba-c5e4e268fe12"
               businessKey="18785586-295e-448a-b759- ebb44a049f21">
                 <name xml:lang="en">AmazonBookPrice</name>
           </serviceInfo>
           <serviceInfo serviceKey="8faa80ea-42dd-4c0d-8070-999ce0455930"
               businessKey="ee41518b-bf99-4a66-9e9e- c33c4c43db5a">
                <name xml:lang="en">AmazonBookPrice</name>
           </serviceInfo>
           </serviceInfos>
         </serviceList>
      </soap:Body>
</soap: Envelope>
```

Σάρωση WSDL (WSDL Scanning)

Το βήμα που έπεται της συλλογής πληροφοριών μίας επιθέσεως σε υπηρεσία ιστού είναι η απόκτηση ενός «*WSDL αρχείου*». Ένα WSDL αρχείο προσφέρει μία σαφή εικόνα, για τον τρόπο με το οποίο μπορεί να αλληλεπιδράσει κάποιος με μία υπηρεσία ιστού. Ο επιτιθέμενος

μπορεί να διαβάσει το αρχείο αυτό, ώστε να πάρει πληροφορίες, όπως τις διαθέσιμες διαδικασίες, τις αναμενόμενες παραμέτρους και τους τύπους μηνυμάτων. Στην συνέχεια, ακολουθεί η αποστολή SOAP μηνυμάτων, ώστε να γίνουν ορατές στον επιτιθέμενο οι αδυναμίες της υπηρεσίας ιστού. Για παράδειγμα, με την αποστολή διάφορων «pattern» μηνυμάτων αιτήσεων, ο επιτιθέμενος βλέπει ποιες διεργασίες υποστηρίζονται, αλλά δεν έχουν δημοσιευθεί στο αρχείο WSDL.



Εικόνα 5: Σάρωση WSDL (Actional Corporation, 2004)

Στο παραπάνω παράδειγμα (Εικόνα 5), εμφανίζονται οι λειτουργίες «GetQuote» και «TradeStock». Η WSDL ενδέχεται να αποκαλύψει περισσότερες πληροφορίες από τις επιθυμητές, ακόμη και αν υπάρχει αυθεντικοποίηση και έλεγχος δικαιωμάτων.

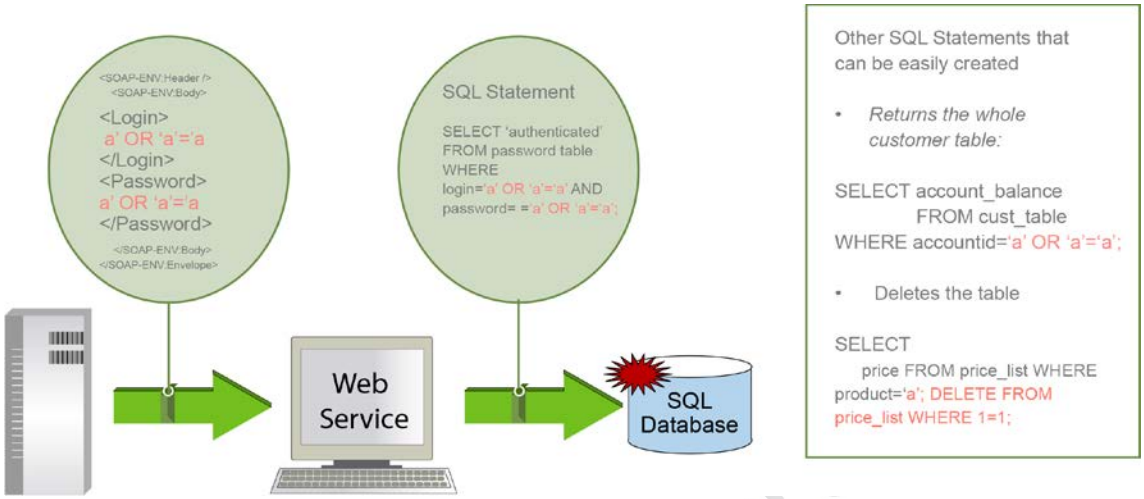
Αλλοίωση Παραμέτρων (Parameter Tampering)

Οι «*παράμετροι*» χρησιμοποιούνται για να σταλούν συγκεκριμένες πληροφορίες από τον πελάτη (client) στην υπηρεσία ιστού, έτσι ώστε μία συγκεκριμένη λειτουργία να εκτελεστεί. Οδηγίες για το πώς μπορούν να χρησιμοποιηθούν οι παράμετροι μπορούν να βρεθούν σε ένα WSDL αρχείο. Επομένως, ο επιτιθέμενος θα μπορούσε να χρησιμοποιήσει τις παραμέτρους, ώστε να αποκτήσει πρόσβαση σε μη εξουσιοδοτημένες λειτουργίες.

Επιθέσεις SQL/XPath Injection

Οι επιθέσεις «*SQL/XPath Injection*» προέρχονται από την κακόβουλη είσοδο δεδομένων και την έλλειψη ελέγχου της εισόδου και απαιτούν κάποια γνώση για την τεχνολογία που χρησιμοποιεί το σύστημα. Η επίθεση «*SQL Injection*» επιτρέπει στον επιτιθέμενο να εκτελέσει πολλές εντολές σε έναν τομέα εισαγωγής, με την χρησιμοποίηση των διαχωριστών εντολής όπως «**;**» ή «**|**». Αυτή η ικανότητα μπορεί να επιτρέψει στον επιτιθέμενο να ανακτήσει, να μεταβάλλει ή να διαγράψει δεδομένα, να εκτελεί SQL εντολές, να ανακτήσει πληροφορίες χωρίς άδεια, να τροποποιήσει την βάση δεδομένων ή/και να μεταβάλλει τις ρυθμίσεις του κεντρικού συστήματος.

Η «XML Path Language (*XPath*)» είναι μία γλώσσα ερωτημάτων (query language) με σκοπό την αναζήτηση, εύρεση και αναγνώριση μερών ενός XML εγγράφου. Η Xpath χρησιμοποιείται για ερωτήματα σε XML βάσεις δεδομένων, καθώς επίσης και για να αναγνωρίζει στοιχεία ενός XML εγγράφου, στα οποία απευθύνεται η ψηφιακή υπογραφή. Η επίθεση «*Xpath Injection*» κινείται στην ίδια λογική με αυτήν της «SQL Injection». Με την χρήση Xpath ερωτημάτων, ο επιτιθέμενος μπορεί να εξάγει ολόκληρο το XML έγγραφο.



Εικόνα 6: SQL / XPath Injection (Actional Corporation, 2004)

Στο παραπάνω παράδειγμα (Εικόνα 6), ένας πίνακας συνθηματικών εκθέτεται, με το να αλλάξει ο επιτιθέμενος την συμβολοσειρά αυθεντικοποίησης, με τέτοιο τρόπο ώστε να είναι πάντα αληθής. Αυτό ενεργοποιεί απλή αυθεντικοποίηση στο σύστημα. Άλλες εντολές «SQL Injection» μπορούν να προκαλέσουν είσοδο σε μη εξουσιοδοτημένες πληροφορίες ή να διαγράψουν έναν ολόκληρο πίνακα.

Καταναγκαστική Ανάλυση (Coercive Parsing)

Η «*καταναγκαστική ανάλυση*» είναι ένας τύπος επίθεσης, όπου η ίδια η XML αναγκάζεται να λειτουργήσει ενάντια στον εαυτό της. Κάποιος αναλυτής XML πρέπει να αναλύσει τα XML έγγραφα, έτσι ώστε οι κατάλληλες μέθοδοι και οι λειτουργίες να υλοποιηθούν. Καθώς η ίδια η διαδικασία της αναλύσεως βρίσκεται επιτιθέμενη, κατόπιν μπορεί να επιτευχθεί άρνηση υπηρεσίας (D.o.S.) ή μπορεί να εισαγχθεί κακόβουλος κώδικας. Η καταναγκαστική ανάλυση εκμεταλλεύεται τις αδυναμίες κάποιων «XML αναλυτών», με σκοπό να καταβάλλει την επεξεργαστική δυνατότητα του συστήματος. Πιο συγκεκριμένα:

Αναδρομικά Φορτία (Recursive Payloads)

Στην επίθεση «*αναδρομικά φορτία*» (Εικόνα 7), ο επιτιθέμενος εκμεταλλεύεται το μοντέλο εμφωλεύσεως των XML εγγράφων. Η ιδέα της επίθεσης είναι η υπερτροφοδότηση του XML αναλυτή με πολλές εμφωλεύσεις (π.χ. 10.000), έτσι ώστε κατά την διαδικασία της αναλύσεως ενός XML στοιχείου (element) να εξαντληθούν οι υπολογιστικοί πόροι.

```
<element1>
    <element2>
        <element3>
            <element4>
                .....
                .....
                .....
            </element4>
        </element3>
    </element2>
</element1>
```

Εικόνα 7: Υπερβολικά Μεγάλος Αριθμός Εμφωλεύσεων

Υπερμεγέθη Φορτία (Oversised Payloads)

Το «μέγεθος» ενός SOAP μηνύματος έχει άμεση επίπτωση στην διαδικασία της αναλύσεως. Έτσι ένα υπερμέγεθες XML έγγραφο μπορεί να επιβαρύνει πολύ την κεντρική μονάδα επεξεργασίας με αποτέλεσμα να επιτυγχάνεται πιο εύκολα η επίθεση «άρνηση υπηρεσίας». Οι δενδροειδείς (DOM-based) XML αναλυτές είναι ιδιαίτερα ευάλωτοι σε αυτήν την επίθεση, εξαιτίας του ότι, πρέπει να τοποθετήσουν ολόκληρο το έγγραφο στην μνήμη πριν να το επεξεργαστούν.

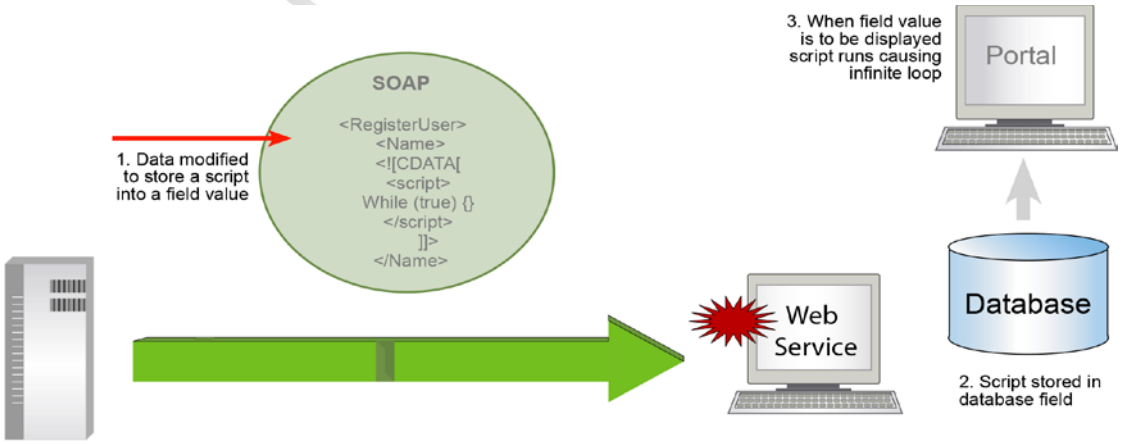
Κατακλυσμός Μηνυμάτων SOAP (SOAP Messages Flooding)

Σκοπός της επίθεσης «κατακλυσμός *SOAP μηνυμάτων*» είναι η υπερφόρτωση μίας υπηρεσίας ιστού, στέλνοντας επαναλαμβανόμενες αιτήσεις SOAP μηνυμάτων. Τα ίδια τα μηνύματα είναι έγκυρα, αλλά ο XML αναλυτής μπορεί να μην δύναται να επεξεργαστεί μεγάλο αριθμό μηνυμάτων σε μικρό χρονικό διάστημα, με αποτέλεσμα να απορρίπτονται μη-κακόβουλα SOAP μηνύματα αιτήσεων.

Επίθεση Cross-Site Scripting (XSS)

Το SOAP και η XML είναι πρότυπα που χρησιμοποιούνται για να γίνεται εύκολη η περιγραφή δεδομένων. Από την μία μεριά το SOAP παρέχει πληροφορίες, μέσω μηνυμάτων, σε ετερογενείς εφαρμογές και από την άλλη η XML εμπεριέχει μετα-δεδομένα (metadata), για να περιγράψει την δομή των πληροφοριών. Στα στοιχεία (elements) ή στα δεδομένα χαρακτήρων (CDATA - character data) μπορεί να εμφωλευθεί κακόβουλος κώδικας. Τα δεδομένα χαρακτήρων (CDATA) χρησιμοποιούνται για να περιγράψουν πληροφορίες στο μήνυμα, που δεν πρέπει να αναλυθεί. Εμφωλευμένοι χαρακτήρες ή κακόβουλο περιεχόμενο μπορεί να σταλεί και η εφαρμογή δέκτης μπορεί ακούσια να εκτελέσει τα δεδομένα.

Η επίθεση «*cross-site scripting*» χρησιμοποιείται για να εμφωλεύσει εντολές, που θα εξαντλήσουν τους υπολογιστικούς πόρους του συστήματος ή θα παράσχουν μη-εξουσιοδοτημένη πρόσβαση.



Εικόνα 8: Cross Site Scripting (Actional Corporation, 2004)

Στο παραπάνω παράδειγμα (Εικόνα 8), κακόβουλος «javascript» κώδικας, έχει εμφωλευθεί μέσα στα «CDATA» του μηνύματος. Το πεδίο τιμών το οποίο απεικονίζεται στον

φυλλομετρητή, εκτελεί ουσιαστικά κώδικα «javascript» προκαλώντας μία άπειρη επανάληψη.

Δηλητηριασμός του XML Schema (XML Schema Poisoning)

Το «XML schema» παρέχει την δομή και διευκρινίσεις για το περιεχόμενο των XML εγγράφων. Κάθε XML έγγραφο πρέπει να είναι σύμφωνο με το «schema» του. Ο επιτιθέμενος διαφθείρει ή τροποποιεί το περιεχόμενο του «schema», με σκοπό όταν ο XML αναλυτής συγκρίνει το έγγραφο με το «schema» του να το θεωρήσει μη-έγκυρο και να το απορρίπτει ως άκυρο. Ως εκ τούτου, επιτυγχάνεται άρνηση υπηρεσίας (D.o.S.). Για παράδειγμα, το αρχικό «schema» μπορεί να απαιτεί ένα χαρακτηριστικό τύπου «@όνομα» σε όλα τα υποβληθέντα έγγραφα. Αν ο επιτιθέμενος αφαιρέσει αυτό το χαρακτηριστικό από το «schema», τότε όλα τα έγγραφα δεν θα έχουν αυτό το χαρακτηριστικό και ενδέχεται η εφαρμογή επεξεργασίας να περιέλθει σε μια απρόσμενη κατάσταση, έτσι ώστε να επιτευχθεί άρνηση υπηρεσίας (D.o.S.).

Επίθεση Εξωτερικών Οντοτήτων (External Entity Attack)

Η λειτουργικότητα της XML, βασιζόμενη σε δεδομένα που εισάγει από «εξωτερικές οντότητες», επιτρέπει την δημιουργία δυναμικών εγγράφων. Όμως, δεν υπάρχει καμία εγγύηση ως προς την ασφάλεια των εξωτερικών οντοτήτων, με αποτέλεσμα τα έγκυρα δεδομένα να μπορούν να αντικατασταθούν με κακόβουλα. Η ανάλυση ενός XML εγγράφου από κάποια κακόβουλη εξωτερική οντότητα μπορεί να έχει ως αποτέλεσμα μια υπηρεσία ιστού να ανοίξει αυθαίρετα αρχεία ή συνδέσεις δικτύου.

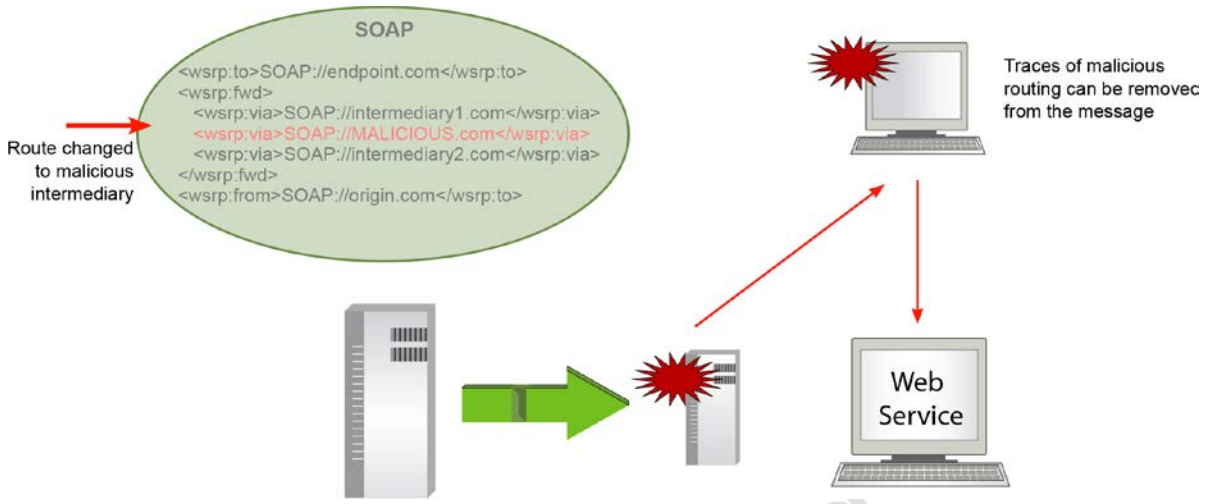
Κακόβουλο Περιεχόμενο (Malicious Contents)

Στην επίθεση «*κακόβουλο περιεχόμενο*», ο επιτιθέμενος εισάγει κακόβουλο περιεχόμενο σε ένα έγκυρο XML έγγραφο. Το κακόβουλο περιεχόμενο μπορεί να προκαλέσει αρκετά προβλήματα όπως «υπερχείλιση μνήμης (buffer overflow)» ή/και «SQL Injection». Στην χειρότερη περίπτωση, στο κακόβουλο περιεχόμενο μπορεί να περιλαμβάνονται προγράμματα και να μεταδοθούν «ιοί», «σκουλίκια (worms)» ή «δούρειοι ίπποι (trojan horses)» σε ολόκληρη την αρχιτεκτονική των υπηρεσιών ιστού.

Παρακάμψεις Δρομολογήσεων (Routing Detours)

Το πρωτόκολλο «WS-Routing» είναι ένα πρωτόκολλο για την ανταλλαγή SOAP μηνυμάτων, από τον αρχικό αποστολέα στον τελικό παραλήπτη, μέσω ενός αριθμού ενδιαμέσων κόμβων. Οι «*παρακάμψεις δρομολογήσεων*» είναι ένας «man-in-the-middle» τύπος επίθεσης, όπου κάποιος από τους ενδιαμέσους κόμβους ελέγχεται από τον επιτιθέμενο με αποτέλεσμα:

- *το μήνυμα να δρομολογηθεί σε μία κακόβουλη τοποθεσία*. Αυτό έχει σαν αποτέλεσμα, ο επιτιθέμενος να κλέψει την κρίσιμη πληροφορία και εν συνεχεία δύναται να διαβιβάσει το μήνυμα στον αρχικό του προορισμό αφαιρώντας τα ίχνη.
- *το μήνυμα να δρομολογηθεί σε μία ανύπαρκτη υπηρεσία*. Αυτό μπορεί να προκαλέσει άρνηση υπηρεσίας (D.o.S.), εφόσον το μήνυμα δεν πρόκειται να δρομολογηθεί ποτέ στον αρχικό προορισμό του.



Εικόνα 9: Παρακάμψεις Δρομολογήσεων (Actional Corporation, 2004)

Στη παραπάνω εικόνα (Εικόνα 9), ένας ενδιάμεσος τροποποιεί τις επιγραφές «WS-routing», για να στείλει την ευαίσθητη πληροφορία σε έναν εξωτερικό κεντρικό υπολογιστή. Οι πληροφορίες είτε καθοδηγούνται πίσω στον ενδιάμεσο είτε στην υπηρεσία ιστού, αφού πρώτα έχουν αφαιρεθεί όλα τα ίχνη.

Επιθέσεις Επαναλήψεως (Replay Attacks)

Στην επίθεση «*επαναλήψεως*» ο επιτιθέμενος υποκλέπτει το SOAP μήνυμα και το ξαναστέλνει επανειλημμένως. Αυτή η ενέργεια δεν θα ανιχνευθεί ως επίθεση αφού η διεύθυνση IP του αποστολέα θα είναι έγκυρη, η συμπεριφορά των πακέτων θα είναι έγκυρη και το HTTP αίτημα θα είναι καλώς σχηματισμένο (well formed). Η παραπάνω ενέργεια μπορεί να οδηγήσει σε άρνηση υπηρεσίας (D.o.S.).

Υπερχείλιση Μνήμης (Buffer Overflow)

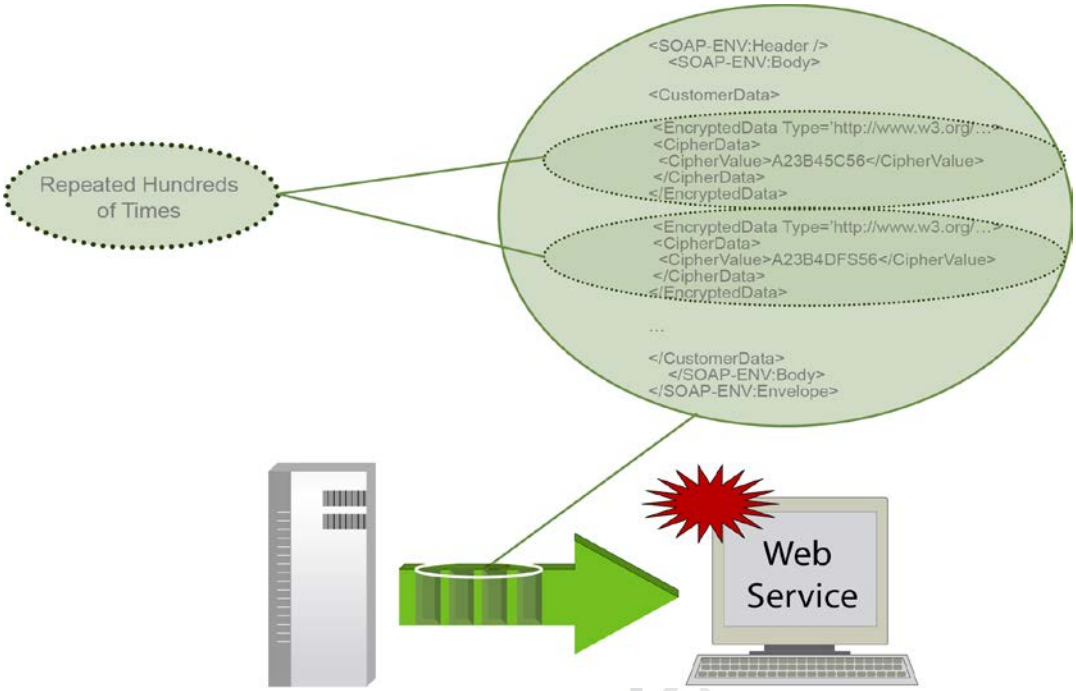
Κατά την επίθεση «*υπερχείλισης μνήμης*», ο επιτιθέμενος εισάγει έναν υπερβολικά μεγαλύτερο αριθμό δεδομένων από τον αναμενόμενο σαν μεταβλητή προγράμματος και έτσι μπορεί να εκτελέσει αυθαίρετο κώδικα συνήθως με τα δικαιώματα του χρήστη, που εκτελεί το πρόγραμμα. Το πλήθος της μνήμης που δεσμεύεται για την διαδικασία είναι μικρότερο από το πλήθος των δεδομένων που γράφονται στην μνήμη. Ως αποτέλεσμα των παραπάνω, τα επιπλέον δεδομένα χάνονται. Επιθέσεις υπερχειλίσης μνήμης παράγονται από κακό προγραμματισμό αφού ο κώδικας του προγράμματος δεν ελέγχει το μέγεθος των εισαγομένων δεδομένων.

Εικόνα 10: Υπερχείλιση Μνήμης (Actional Corporation, 2004)

Στο παραπάνω παράδειγμα (Εικόνα 10), μεγάλο πλήθος δεδομένων τοποθετείται στο «<parameter1>» και στέλνεται στην εφαρμογή η οποία μπορεί να μην είναι προετοιμασμένη να χειριστεί τόσο μεγάλο πλήθος δεδομένων.

Άρνηση Υπηρεσίας (Denial of Service)

Υπάρχουν πολλοί μηχανισμοί αρνήσης υπηρεσίας (D.o.S.). Η πιο κοινή επίθεση «*άρνησης υπηρεσίας*» είναι η υπερτροφοδότηση του συστήματος με περισσότερα μηνύματα από όσα είναι ικανό να διαχειριστεί. Σημειωτέον ότι υπάρχουν και άλλοι τρόποι για να προκληθεί μία επίθεση άρνησης υπηρεσίας. Ο επιτιθέμενος μπορεί να στείλει συνημμένα μεγάλου μεγέθους ή μηνύματα μεγάλου μεγέθους. Άλλη μία μορφή επίθεσης, είναι αυτή όπου ο επιτιθέμενος στέλνει μηνύματα με πολλά κρυπτογραφημένα ή υπογεγραμμένα στοιχεία. Εξαιτίας του γεγονότος ότι τόσο η κρυπτογράφηση όσο και η υπογραφή απαιτούν πλήθος υπολογιστικών πόρων για την επεξεργασία τους, το σύστημα μπορεί να «εξαντληθεί» προσπαθώντας να χειριστεί αυτά τα μηνύματα.

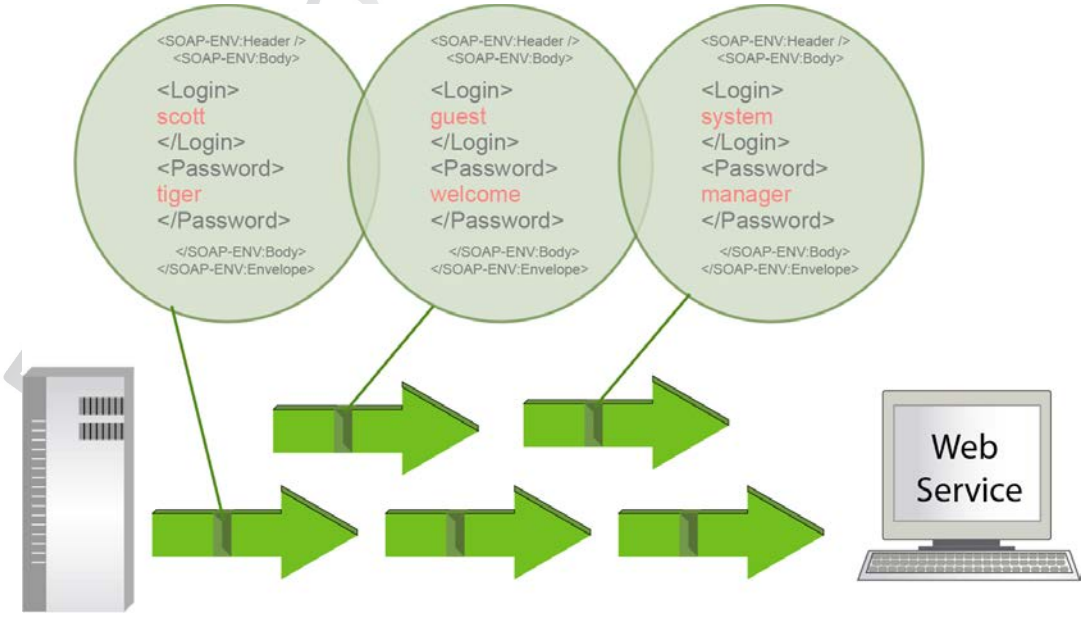


Εικόνα 11: Άρνηση Υπηρεσίας (Actional Corporation, 2004)

Στο παραπάνω παράδειγμα (Εικόνα 11), ένα μήνυμα με ένα μεγάλο πλήθος κρυπτογραφημένων δεδομένων στέλνεται, εξαντλεί την επεξεργασία της λαμβάνουσας αίτησης και προκαλεί άρνηση της υπηρεσίας.

Επιθέσεις Λεξικού στα Συνθηματικά (Dictionary Password Attacks)

Οι επιθέσεις «*λεξικού στα συνθηματικά*» είναι ένας αρκετά κοινός τρόπος επίθεσης, ώστε ο επιτιθέμενος να αποκτήσει πρόσβαση στο σύστημα. Εισάγει επαναλαμβανόμενα κοινούς συνδυασμούς ονομάτων χρηστών και συνθηματικών, μέχρι να αποκτήσει πρόσβαση.



Εικόνα 12: Επιθέσεις λεξικού στα Συνθηματικά (Actional Corporation, 2004)

Όπως φαίνεται στο παραπάνω παράδειγμα (Εικόνα 12), πλήθος κοινών συνδυασμών δοκιμάζονται για να επιτευχθεί πρόσβαση στο σύστημα. Για παράδειγμα «SCOTT/TIGER» είναι ένας κοινός-προεπιλεγμένος συνδυασμός ονόματος χρήστη/συνθηματικού στις βάσεις δεδομένων Oracle.

Κεφάλαιο 3: Τρόποι Αντιμετώπισης Επιθέσεων Ασφάλειας στις Υπηρεσίες Ιστού

Εισαγωγή

Για να αποτραπούν οι επιθέσεις ασφάλειας στις υπηρεσίες ιστού, οι οποίες αναφέρθηκαν στο κεφάλαιο 2, πρέπει να ληφθούν προληπτικά μέτρα από την πρώτη φάση δημιουργίας της εφαρμογής.

Μια πρόταση αντιμετώπισης των διάφορων επιθέσεων είναι η εφαρμογή «άμυνας σε βάθος». Η εφαρμογή αυτή μπορεί να υλοποιηθεί όχι μόνο με τη χρήση ενός «firewall» ανάμεσα στο «Internet» και τον «web server», αλλά με τη χρήση «firewall» ανάμεσα στον «web server» και στους «servers» της εφαρμογής (application servers), όπως επίσης και μεταξύ αυτών και της βάσης (Εικόνα 13). Από την άλλη μεριά, η άμυνα που προσφέρουν τα «firewalls» δεν μπορεί να αντιμετωπίσει τα πάντα.

Για το λόγο αυτό, ο καλύτερος τρόπος για προστασία είναι να τηρηθούν οι απαιτήσεις ασφάλειας (*εμπιστευτικότητα*, *ακεραιότητα*, *αυθεντικοποίηση* και *εξουσιοδότηση*), για τις υπηρεσίες ιστού μέσω προτύπων όπως τα «*XML-Encrypt*», «*XML-Sign*», «*XKMS*», «*SAML*», «*XACML*».

Εικόνα 13: Εφαρμογή Άμυνας σε Βάθος

Απαιτήσεις Ασφάλειας

Οι τέσσερις βασικές απαιτήσεις ασφάλειας που εφαρμόζονται για την επικοινωνία σε περιβάλλον ιστού είναι η *εμπιστευτικότητα* (confidentiality), η *ακεραιότητα* (integrity), η *αυθεντικοποίηση* (authentication) και η *εξουσιοδότηση* (authorization).

Εμπιστευτικότητα (Confidentiality)

Η «*εμπιστευτικότητα*» είναι το κομμάτι της ασφάλειας που αφορά τη *διατήρηση της μυστικότητας της πληροφορίας*.

Για παράδειγμα σε μια εφαρμογή όπου ανταλλάσσονται «SOAP» μηνύματα, τα οποία περιέχουν ευαίσθητα δεδομένα όπως πληροφορίες για πελάτες και συναλλαγές, είναι σημαντικό να υπάρχει προστασία από απειλές.

Ακεραιότητα (Integrity)

Ο στόχος ασφάλειας της «*ακεραιότητας*» είναι η διασφάλιση της πληρότητας και της ακρίβειας των δεδομένων.

Μηνύματα που αποστέλλονται από μια πηγή, μπορεί να περάσουν από ενδιάμεσα σημεία πριν φτάσουν στον τελικό προορισμό τους. Είναι σημαντική η ύπαρξη ενός μηχανισμού για τον παραλήπτη του μηνύματος, έτσι ώστε να επιβεβαιώσει ότι το μήνυμα δεν έχει αλλάξει ή τροποποιηθεί κατά τη μετάδοσή του.

Αυθεντικοποίηση (Authentication)

Η «*αυθεντικοποίηση*» επιβεβαιώνει την ταυτότητα του αποστολέα ή παραλήπτη, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια (credentials) που κατέχει ο χρήστης.

Τα διαπιστευτήρια ενσωματώνονται είτε στην επικεφαλίδα (header), είτε στο κυρίως μέρος (body) του «SOAP» μηνύματος. Πρότυπες τεχνολογίες ιστού που χρησιμοποιούν «passwords», «X.509 πιστοποιητικά», «Kerberos», «LDAP» και «Active Directory», μπορούν να χρησιμοποιηθούν για την αυθεντικοποίηση των αιτούντων μιας υπηρεσίας. Τόσο οι αιτούντες της υπηρεσίας όσο και οι πάροχοι πρέπει να αυθεντικοποιηθούν για επικοινωνία, που περιλαμβάνει αποστολή ευαίσθητων δεδομένων. Επιπλέον, πρέπει να αυθεντικοποιηθεί και το «WSDL» αρχείο.

Εξουσιοδότηση (Authorization)

Η «*εξουσιοδότηση*» είναι πολύ σημαντική καθώς οι υπηρεσίες ιστού παρέχουν πολύπλοκα επίπεδα πρόσβασης. Πρέπει να υπάρχει εξουσιοδότηση, όχι μόνο για το σε ποιες πληροφορίες οι χρήστες/εφαρμογές έχουν δικαίωμα πρόσβασης αλλά και ποιες λειτουργίες έχει δικαίωμα να εκτελέσουν.

Πρότυπα Ασφάλειας

XML Κρυπτογράφηση (XML Encryption)

Το πρότυπο «*XML Κρυπτογράφηση*» περιγράφει τους κανόνες για την κρυπτογράφηση και αποκρυπτογράφηση ψηφιακών δεδομένων καθώς και τον τρόπο με τον οποίο το αποτέλεσμα της κρυπτογράφησης πρέπει να αναπαρασταθεί σε μια δομημένη μορφή, όπως ένα XML αρχείο, για να εξασφαλιστεί η από άκρη-σε άκρη εμπιστευτικότητα των δεδομένων, χωρίς να μπορεί το περιεχόμενο να ανακτηθεί ή να χρησιμοποιηθεί κακόβουλα από τρίτους.

Η «*XML Κρυπτογράφηση*» είναι ένα XML έγγραφο, υποστηρίζει την κρυπτογράφηση ενός ολόκληρου XML κειμένου ή μόνο επιλεγμένων κομματιών του και περιέχει τα παρακάτω στοιχεία (Κεμάλης κ.α., 2005):

- Ένα προαιρετικό στοιχείο «***EncryptionMethod***», το οποίο περιγράφει τον αλγόριθμο κρυπτογράφησης που εφαρμόζεται στα «cipher» δεδομένα. Εάν το στοιχείο απουσιάζει, ο αλγόριθμος κρυπτογράφησης πρέπει να γίνει γνωστός από τον παραλήπτη αλλιώς η αποκρυπτογράφηση θα αποτύχει.
- Ένα προαιρετικό στοιχείο «***ds:KeyInfo***», το οποίο περιέχει πληροφορίες για το κλειδί που χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα.
- Ένα απαραίτητο στοιχείο «***CipherData***», το οποίο παρέχει τα κρυπτογραφημένα δεδομένα. Επίσης, πρέπει να περιέχει την κρυπτογραφημένη ακολουθία ως κωδικοποιημένο κείμενο του στοιχείου «CipherValue», χρησιμοποιώντας την μορφή «base64», ή να παρέχει μια αναφορά σε μια εξωτερική θέση που περιέχει την κρυπτογραφημένη ακολουθία μέσω του στοιχείου «CipherReference».

```
<element name='CipherData' type='xenc:CipherDataType'/>
  <complexType name='CipherDataType'>
     <choice>
       <element name='CipherValue' type='base64Binary'/>
       <element ref='xenc:CipherReference'/>
     </choice>
   </complexType
```

Στο παρακάτω παράδειγμα «XML κρυπτογράφησης» το κρυπτογραφημένο περιεχόμενο, που αναπαριστά τον αριθμό της πιστωτικής κάρτας (ευαίσθητη πληροφορία) του John Smith, αντικαθιστά το αρχικό περιεχόμενο μέσα στο XML έγγραφο. Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται είναι ο 3DES σε μορφή «cipher block chaining - CBC» και το κλειδί που θα χρησιμοποιηθεί για να αποκρυπτογραφηθούν τα δεδομένα ονομάζεται «mykey».

```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
    <Name>John Smith</Name>
    <CreditCard Limit='5,000' Currency='USdollars'>
    <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
        Type='http://www.w3.org/2001/04/xmlenc#Element'/>
     <EncryptionMethod
        Algorithm='http://www.w3.org/2001/04/xmlenc#tripledes-cbc'/>
       <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
         <ds:KeyName>mykey</ds:KeyName>
       </ds:KeyInfo>
       <CipherData>
        <CipherValue>A23B45C56</CipherValue>
        </CipherData>
    </EncryptedData>
</PaymentInfo>
```

XML Ψηφιακή Υπογραφή (XML Signature)

Το πρότυπο «*XML Ψηφιακή Υπογραφή*» καθορίζει την διαδικασία για την δημιουργία και αναπαράσταση μιας XML υπογραφής καθώς και την επαλήθευση της εγκυρότητάς της. Επίσης, καθορίζει τον τρόπο με τον οποίο υπογράφονται ψηφιακά δεδομένα και το πώς το αποτέλεσμα της υπογραφής, μπορεί να αναπαρασταθεί σε XML.

Η «XML ψηφιακή υπογραφή» παρέχει ασφαλείς υπηρεσίες με τη μορφή ακεραιότητας δεδομένων από άκρη-σε-άκρη σε πολλαπλά συστήματα και πιστοποίησης μηνυμάτων. Επιπλέον, με αυτήν μπορεί να υπογραφεί ένα ολόκληρο XML έγγραφο ή επιλεγμένα κομμάτια του.

Η βασική δομή της «XML ψηφιακής υπογραφής» είναι η παρακάτω:

```
<element name="Signature" type="ds:SignatureType"/>
<complexType name="SignatureType">
      <sequence>
         <element ref="ds:SignedInfo"/>
         <element ref="ds:SignatureValue"/>
         <element ref="ds:KeyInfo" minOccurs="0"/>
         <element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
      </sequence>
      <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Η «XML ψηφιακή υπογραφή» είναι ένα XML έγγραφο, το οποίο περιέχει τα παρακάτω στοιχεία:

- Ένα απαραίτητο στοιχείο «***SignedInfo***», το οποίο περιλαμβάνει τον αλγόριθμο «canonicalization», έναν αλγόριθμο υπογραφής και μια ή περισσότερες αναφορές.

```
<element name="SignedInfo" type="ds:SignedInfoType"/>
<complexType name="SignedInfoType">
<sequence>
   <element ref="ds:CanonicalizationMethod"/>
   <element ref="ds:SignatureMethod"/>
   <element ref="ds:Reference" maxOccurs="unbounded"/>
</sequence>
<attribute name="Id" type="ID" use="optional"/>
</complexType>
```

- Ένα απαραίτητο στοιχείο «***SignatureValue***», το οποίο περιέχει την πραγματική τιμή της ψηφιακής υπογραφής και κωδικοποιείται πάντα χρησιμοποιώντας την μορφή «base64».

```
<element name="SignatureValue" type="ds:SignatureValueType"/>
<complexType name="SignatureValueType">
  <simpleContent>
     <extension base="base64Binary">
        <attribute name="Id" type="ID" use="optional"/>
     </extension>
  </simpleContent>
</complexType>
```

- Ένα προαιρετικό στοιχείο «***KeyInfo***», το οποίο επιτρέπει στον παραλήπτη να λάβει το κλειδί που απαιτείται για να επικυρώσει την υπογραφή. Το «KeyInfo» μπορεί να περιέχει κλειδιά, ονόματα, πιστοποιητικά και άλλες πληροφορίες διαχείρισης δημόσιου κλειδιού.
- Ένα προαιρετικό στοιχείο «***Object***», το οποίο μπορεί να εμφανιστεί μια ή περισσότερες φορές. Όταν εμφανίζεται, αυτό το στοιχείο μπορεί να περιέχει

οποιαδήποτε δεδομένα. Το στοιχείο «Object» μπορεί να περιλαμβάνει τον τύπο MIME, την ταυτότητα και τα χαρακτηριστικά κωδικοποίησης.

Διαχείριση Κλειδιού με XML (XKMS)

Το πρότυπο «Διαχείριση Κλειδιού με XML (XML Key Management Specification - XKMS)» αναπτύχθηκε από την W3C και αποτελεί ένα σύνολο προδιαγραφών για την εγγραφή και την διανομή δημόσιων κλειδιών.

Το «XKMS» χρησιμοποιείται σε συνδυασμό με της «ψηφιακές υπογραφές XML» και την «κρυπτογράφηση XML» και αντιμετωπίζει θέματα εμπιστοσύνης, που έχουν να κάνουν με την διαχείριση κλειδιών. Εξαιτίας αυτού, οι υπηρεσίες μπορούν εισέλθουν σε έναν «XKMS server», προκειμένου να αποκτήσουν πληροφορίες κλειδιού για κρυπτογράφηση και αυθεντικοποίηση.

Γλώσσα Προδιαγραφής Ισχυρισμών Ασφαλείας (SAML)

Η «Γλώσσα Προδιαγραφής Ισχυρισμών Ασφαλείας (Security Assertion Markup Language - SAML)», αποτελεί πρότυπο του οργανισμού «OASIS» (OASIS XML-Based Security Services Technical Committee - SSTC). Είναι ένα πλαίσιο βασισμένο σε XML κατάλληλο για την ανταλλαγή ασφαλούς πληροφορίας. Περιλαμβάνει ένα πρωτόκολλο ανταλλαγής μηνυμάτων (standard message exchange protocol) και καθορίζει τον τρόπο με τον οποίο ζητείται η πληροφορία που χρειάζεται. Επίσης, καθορίζει τους κανόνες για τον τρόπο μεταφοράς, επιτυγχάνοντας με αυτό τον τρόπο την διαλειτουργικότητα (interoperability). Επιπλέον, εκφράζει την ασφάλεια με την μορφή ισχυρισμών (assertions) σχετικά με τα αντικείμενα, το οποίο είναι ιδιαίτερα σημαντικό εξαιτίας του ότι στις υπηρεσίες ιστού, τα ασφαλή δεδομένα μεταφέρονται μέσω αρκετών συστημάτων για την υλοποίηση μιας συναλλαγής. Ένας ισχυρισμός «SAML» μπορεί να περιέχει πληροφορία για πράξεις *αυθεντικοποίησης* (aythentication assertion) που επιτελούνται από ισχυρισμούς, χαρακτηριστικά ισχυρισμών (attribute assertion) και ισχυρισμούς για έλεγχο πρόσβασης (authorization assertion) σε συγκεκριμένους πόρους μια περιοχής ασφάλειας. (Πολέμη κ.α., 2008).

Η «SAML» καθορίζει τρία διαφορετικά είδη δηλώσεων ισχυρισμών που μπορούν να δημιουργηθούν από μια *Αρχή* «SAML». Τα είδη είναι τα ακόλουθα:

- *Αυθεντικοποίηση*: Υποδεικνύει ότι η καθορισμένη ταυτότητα έχει αυθεντικοποοιηθεί από μια δεδομένη αρχή σε ένα δεδομένο χρόνο.

```
<saml: Assertion>
 <saml:AuthenticationStatment AuthenticationMethod=”password”
     AuthenticationInstant=”2001-12-03T10:02:00Z”>
     <saml:Subject>
           <saml: NameIndentifier SecurityDomain=“smitho.com”
                 Name=“joeuser” />
           <saml: ConfirmationMethod>
                 http://...core-25/sender-vouches
           </saml: ConfirmationMethod>
      </saml:Subject>
 </saml:AuthenticationStatment>
```

```
<saml: Assertion>
```

- *Χαρακτηριστικό*: Η καθορισμένη ταυτότητα είναι συνδεδεμένη με τα καθορισμένα χαρακτηριστικά.

```
<saml: Assertion>
 <saml:AttributeStatement>
      <saml:Subject> ……</saml:Subject>
      <saml: Attribute AttributeName=“PaidStatus”
            AttributeNamespace=“http://smitho.com”>
      <saml: AttributeValue>
            PaidUp
      </saml: AttributeValue>
      </saml: Attribute>

      <saml: Attribute AttributeName=“CreditLimit”
            AttributeNamespace=“http://smitho.com”>
      <saml: AttributeValue>
            <my: amount currency=”USD”> 500.00 </my:amount>
      </saml: AttributeValue>
      </saml: Attribute>

 </saml:AttributeStatement>
</saml: Assertion>
```

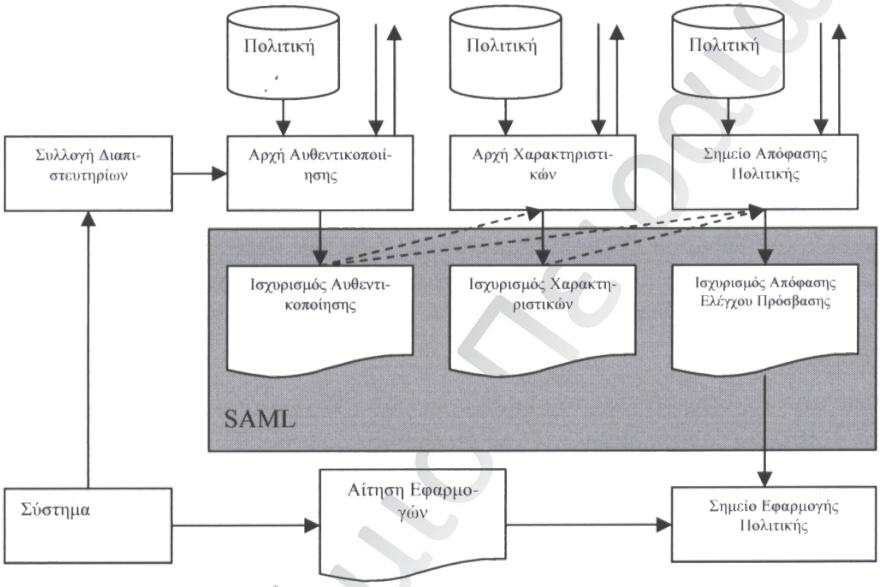
- *Απόφαση ελέγχου πρόσβασης*: Μια συγκεκριμένη απόφαση ελέγχου πρόσβασης σε ένα πόρο βασισμένη σε μια αίτηση ελέγχου πρόσβασης.

```
<saml: Assertion>
 <saml:AuthorizationStatment Decision=”permit”
      Resource=”http://jonesco.com/rpt_12345.htm”>
      <saml:Subject>…</saml:Subject>
      <saml:Actions ActionNamespace=“http://...core-25/rwedc”>
            <saml:Action>Read</saml:Action>
      </saml:Actions>
 </saml:AuthorizationStatment>
</saml: Assertion>
```

Στην Εικόνα 14 απεικονίζεται ο τρόπος που η «SAML» μπορεί να επιτρέψει σε μια οντότητα ενός συστήματος να επιτελέσει μια δραστηριότητα πάνω σε συγκεκριμένο πόρο. Τα βήματα της διαδικασίας είναι τα ακόλουθα (Πολέμη κ.α., 2008):

- Ο πελάτης αυθεντικοποιείται και ζητά από την αρχή αυθεντικοποίησης να του επιστρέψει έναν ισχυρισμό «SAML» ως απόδειξη της αυθεντικοποίσησησης.
- Ο πελάτης εκδίδει μια αίτηση πρόσβασης στον πόρο και την στέλνει στον οργανισμό που διαχειρίζεται τον πόρο μαζί με τον ισχυρισμό αυθεντικοποίησης του βήματος 1.

- Ο οργανισμός που θα δεχτεί την αίτηση, πρώτα εξετάζει τον ισχυρισμό αυθεντικοποίησης και έπειτα επικοινωνεί με την *Αρχή Χαρακτηριστικών SAML*, για να της δώσει τον ισχυρισμό αυθεντικοποίησης και να ζητήσει έναν ισχυρισμό χαρακτηριστικών.
- Ο οργανισμός αποστέλλει μια αίτηση ελέγχου πρόσβασης «SAML» στην *Αρχή Ελέγχου Πρόσβασης* (σημείο ελέγχου πολιτικής) μαζί με τον πόρο στον οποίο ζητά πρόσβαση ο πελάτης και τον ισχυρισμό χαρακτηριστικών.
- Η *Αρχή Ελέγχου Πρόσβασης* αποφαίνεται για το αν θα δώσει πρόσβαση ή όχι και επιστρέφει μια απόφαση αποδοχής ή απόρριψης στη μορφή ενός ισχυρισμού απόφασης ελέγχου πρόσβασης.



Εικόνα 14: Μοντέλο Διαχείρισης SAML (Πολέμη κ.α., 2008)

Επεκτάσιμη Γλώσσα Ελέγχου Πρόσβασης (XACML)

Η «Επεκτάσιμη Γλώσσα Ελέγχου Πρόσβασης (XML Access Control Markup Language-XACML)», αποτελεί πρότυπο του οργανισμού «OASIS» και είναι μια γενικευμένη γλώσσα προδιαγραφής πολιτικών ελέγχου πρόσβασης, που βασίζονται στην XML, για την έκφραση πληροφορίας ασφάλειας.

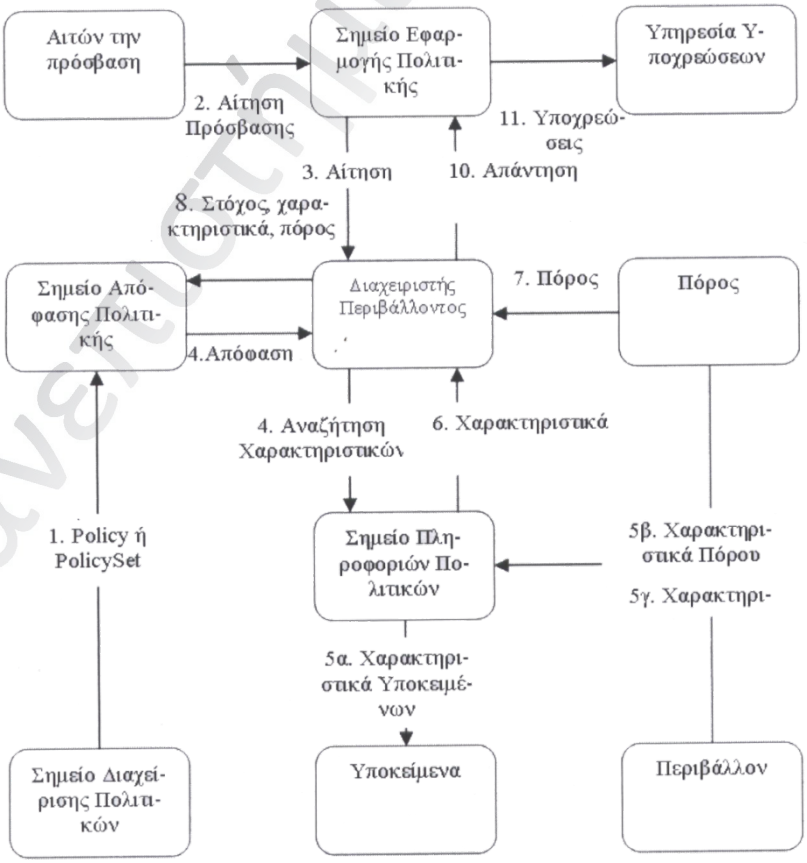
Η «XACML» είναι μια γλώσσα που επιτρέπει σε οργανισμούς να επικοινωνούν οι πολιτικές τους προς απόκτηση πρόσβασης σε πληροφορίες και πόρους.

Επίσης, η «XCAML» επιτρέπει τη χρήση αυθαίρετων χαρακτηριστικών στις πολιτικές, τον έλεγχο προσπέλασης βασισμένο σε ρόλους (role based access control), τις πολιτικές ευρετηρίου, τις ετικέτες ασφάλειας, τις πολιτικές βασισμένες σε ώρα/ημέρα, δυναμικές πολιτικές και όλα αυτά χωρίς να απαιτούνται αλλαγές στις εφαρμογές οι οποίες χρησιμοποιούν «XACML». (Κεμάλης κ.α., 2005).

Οι κύριες οντότητες που εμπλέκονται σε μια περιοχή διαχείρισης που χρησιμοποιεί «XACML» παρουσιάζονται στην Εικόνα 15 και αναλύονται παρακάτω (Πολέμη κ.α., 2008).

- Το *Σημείο Διαχείρισης Πολιτικών* - ΣΔΠ (Policy Administration Point - PAP) γράφει πολιτικές για τους πόρους που διαχειρίζεται και τις γνωστοποιεί στο *Σημείο Απόφασης Πολιτικής* - ΣΑΠ (Policy Decision Point - PDP), το οποίο αποτιμά τις πολιτικές και παίρνει τις αποφάσεις ελέγχου πρόσβασης.

- Η οντότητα που ζητά την πρόσβαση σε κάποιο πόρο στέλνει μια αίτηση πρόσβασης στο *Σημείο Εφαρμογής Πολιτικής* - ΣΕΠ (Policy Enforcement Point - PEP) προκειμένου να υλοποιηθεί ο έλεγχος πρόσβασης.
- Το ΣΕΠ αποστέλλει την αίτηση για πρόσβαση στον διαχειριστή περιβάλλοντος (context handler) σε μια μορφή που αυτός καταλαβαίνει. Ο διαχειριστής περιβάλλοντος κατασκευάζει μια αίτηση «XACML» βάσει της πληροφορίας που περιέχεται στην αίτηση.
- Πληροφορίες για τον πόρο προς πρόσβαση και χαρακτηριστικά του περιβάλλοντος ενδέχεται να ζητηθούν από έναν *Σημείο Πληροφοριών Πολιτικών* - ΣΠΠ (Policy Information Point - PIP), το οποίο τελεί χρέη πηγής τιμών χαρακτηριστικών.
- Το «ΣΠΠ» αναζητά και λαμβάνει τα χαρακτηριστικά του υποκειμένου που ζητά πρόσβαση, τον πόρο που ζητείται προς πρόσβαση και το περιβάλλον.
- Το «ΣΠΠ» επιστρέφει τα χαρακτηριστικά που έχουν ζητηθεί στον διαχειριστή περιβάλλοντος.
- Ο διαχειριστής περιβάλλοντος ενδέχεται να συμπεριλάβει τον πόρο στην αίτηση.
- Ο διαχειριστής περιβάλλοντος στέλνει την αίτηση για απόφαση πρόσβασης στο «ΣΑΠ» για να αποτιμήσει την πολιτική.
- Το «ΣΑΠ» επιστρέφει την απάντηση.
- Ο διαχειριστής περιβάλλοντος μεταφράζει την απάντηση από «XACML» στην μορφή που κατανοεί το «ΣΕΠ». Αποστέλλει την απάντηση αυτή στο «ΣΕΠ».
- Το «ΣΕΠ» εφαρμόζει την πολιτική. Εάν η πρόσβαση επιτρέπεται σύμφωνα με την απάντηση, τότε το «ΣΕΠ» επιτρέπει πρόσβαση στον πόρο, αλλιώς απορρίπτει την αίτηση πρόσβασης.



Εικόνα 15: Διάγραμμα Ροής XAMCL (Πολέμη κ.α., 2008)

Μοντέλο Ασφάλειας Υπηρεσιών Ιστού (Web Services Security Model)

Οι εταιρείες IBM και Microsoft συνεργάστηκαν για να δημιουργήσουν μια αρχιτεκτονική για την αντιμετώπιση ζητημάτων ασφαλείας σε υπηρεσίες ιστού. Ο σκοπός της είναι να περιέχει μοναδικό, ευέλικτο και ευρύ πεδίο ασφάλειας. Η αρχιτεκτονική αυτή ορίζει υψηλού επιπέδου απαιτήσεις ασφάλειας και μια μεθοδολογία ώστε να συνδυαστούν όλες οι τεχνολογίες που την αφορούν. Τα χαρακτηριστικά της χωρίζονται σε δύο κατηγορίες (Πολέμη κ.α., 2008):

- Η πρώτη κατηγορία περιλαμβάνει τα χαρακτηριστικά τα οποία χρειάζεται μια υπηρεσία ιστού όταν συναλλάσεται με έμπιστους δικτυακούς τόπους (Πολέμη κ.α., 2008):
    - **Πολιτική Υπηρεσιών Ιστού** (*WS-Policy*): Ορίζει τις απαιτήσεις, τις δυνατότητες, τις αναφορές και τις πολιτικές ασφαλείας, στο εσωτερικό και στο εξωτερικό επίπεδο μιας υπηρεσίας ιστού.
    - **Εμπιστευτικότητα Υπηρεσιών Ιστού** (*WS-Trust*): Ορίζει το μοντέλο ασφαλείας, επιτρέποντας διαλειτουργικότητα με όλους τους έμπιστους διαδικτυακούς τόπους.
    - **Μυστικότητα Υπηρεσιών Ιστού** (*WS-Policy*): Ορίζει ένα μοντέλο για εξυπηρετητές και εξυπηρετητές υπηρεσιών ιστού, για να δηλώσει πρακτικές και προτιμήσεις.
- Η δεύτερη κατηγορία περιλαμβάνει χαρακτηριστικά που απαντούν σε πιο εξειδικευμένες απαιτήσεις ασφαλείας (Πολέμη κ.α., 2008):
    - **Ασφαλείς Επικοινωνία Υπηρεσιών Ιστού** (*WS-Secure Conversation*): Ορίζει τον τρόπο με τον οποίο επιλέγονται δυναμικά έμπιστοι δικτυακοί τόποι χρησιμοποιώντας ανταλλαγή κλειδιών.
    - **Ομοσπονδία Υπηρεσιών Ιστού** (*WS-Federation*): Ορίζει τον τρόπο με τον οποίο γίνεται η αναγνώριση και η ανταλλαγή πληροφοριών ανάμεσα σε ετερογενή ομοσπονδιακά συστήματα.
    - **Εξουσιοδότηση Υπηρεσιών Ιστού** (*WS-Authorization*): Ορίζει τον τρόπο με τον οποίο διεξάγεται η διαχείριση πληροφοριών και πολιτικών πρόσβασης στο περιβάλλον μιας υπηρεσίας ιστού.

Επιθέσεις Ασφάλειας και Προστασία

Ακολουθεί συνοπτικός πίνακας παρουσίασης επιθέσεων και αντιμέτρων:

Πίνακας 4: Παρουσίαση Επιθέσεων και Αντιμέτρων

Κατηγορία Επιθέσεων	***Επιθέσεις***	**Περιγραφή**	**Αντίμετρα**
Επιθέσεις Ταυτότητας (Identity)	*Επιθέσεις Λεξικού* (Dictionary attacks)	Εξασφαλίζοντας «usernames» και «passwords» ο εισβολέας αποκτά πρόσβαση στην υπηρεσία σαν	*Τεχνολογία Κρυπτογραφίας*: ψηφιακά πιστοποιητικά, ψηφιακές

Κατηγορία Επιθέσεων	***Επιθέσεις***	**Περιγραφή**	**Αντίμετρα**
		νόμιμος χρήστης.	υπογραφές, SSL.
	IP Spoofing	Ο εισβολέας προσποιούμενος ότι είναι μια υπηρεσία, δελεάζει τον χρήστη-πελάτη να κάνει αιτήσεις στον κατάλογό του.	
	Υποκλοπές μηνυμάτων (Message eavesdropping)	Όταν ο επιτιθέμενος συλλέγει πληροφορίες από την ανάλυση των μηνυμάτων υπηρεσίας ιστού.	
	Αλλοίωση μηνυμάτων (data tampering)	Ένας επιτιθέμενος μπορεί να τροποποιήσει νόμιμο μήνυμα με παράνομα δεδομένα. Αποτέλεσμα να φτάνουν στον προορισμό αλλοιωμένα δεδομένα.	
Επιθέσεις Session	*Επαναληπτικές επιθέσεις (replay attacks)*	Για να επιτύχει υπερφόρτωση της υπηρεσίας ιστού ένας εισβολέας κλέβει μηνύματα και τα στέλνει επαναληπτικά.	Χρησιμοποιούμε αναγνωριστικό μηνύματος ή έναν σειριακό αριθμό για να εξασφαλίσουμε, ότι το μήνυμα χρησιμοποιείται μόνο μία φορά.
	Man-in-the-middle	Ο επιτιθέμενος εισάγει ψεύτικες πληροφορίες δρομολόγησης, ώστε το μήνυμα να ταξιδέψει σε κακόβουλη τοποθεσία. Στη συνέχεια στέλνει κακόβουλες πληροφορίες και στον αρχικό προορισμό.	Τεχνολογία Κρυπτογράφησης.
Επιθέσεις Ανάλυσης	*Αναδρομικά Φορτία*	Ο επιτιθέμενος	Πρέπει να

Κατηγορία Επιθέσεων	***Επιθέσεις***	**Περιγραφή**	**Αντίμετρα**
(Parsing)	(Recursive payloads)	προσπαθεί να «σπάσει» έναν «XML parser».	χρησιμοποιείται καλό «XML parsing».
	Υπερμεγέθη ωφέλιμα φορτία (oversize payloads)	Απεριόριστο μέγεθος αρχείου επιτρέπει στον εισβολέα να υπερφορτώσει τον «parser».	Έλεγχος του «parser» για ασυνήθιστες περιπτώσεις (μεγάλα στοιχεία και ονόματα ιδιοτήτων).
	Δηλητηρίασμός του XML Schema (XML Schema Poisoning)	Ένας επιτιθέμενος αντικαθιστά το «XML Schema» με κάποιο παρόμοιο αλλά τροποποιημένο.	Επικύρωση του «XML Schema».
Επιθέσεις υπερχείλισης (Overflow)	*Επιθέσεις υπερχείλισης μνήμης* (Buffer overflow attacks)	Αυτή η επίθεση αποσκοπεί στην μηχανή SOAP μέσω «web server». Ένας εισβολέας στέλνει παραπάνω είσοδο από όση μπορεί να χειριστεί το πρόγραμμα, και μπορεί να προκαλέσει στην υπηρεσία να συντριβεί.	Εκτέλεση ελέγχου-επικύρωσης εισόδου.
Επιθέσεις Κώδικα (Code)	*SQL Injection*	Ένας εισβολέας εισάγει και εκτελεί κακόβουλες εντολές SQL στην XML.	Επικύρωση ροής εισόδου, έλεγχος εξαιρέσεων.
	XPath Injection	Ένας εισβολέας δημιουργεί «SQL-like» επερωτήσεις σε ένα XML αρχείο χρησιμοποιώντας «XPath» για να εξάγει μια βάση δεδομένων XML.	Η ροή εισόδου του χρήστη πρέπει να ελέγχεται εξονυχιστικά. Μονά και διπλά εισαγωγικά (δηλ. ″ ή ′) δεν πρέπει να επιτρέπονται.
Επιθέσεις XDoS	*Επιθέσεις XML Denial-of-Service*	Ένας εισβολέας προσπαθεί να αποτρέψει τους νόμιμους χρήστες από την πρόσβαση σε μια υπηρεσία «βομβαρδίζοντας» την υπηρεσία με	Απόρριψη της επισκεψιμότητας από μια διεύθυνση όταν είναι σαφές ότι έχει αρχίσει μια επίθεση.

Κατηγορία Επιθέσεων	***Επιθέσεις***	**Περιγραφή**	**Αντίμετρα**
		χιλιάδες αιτήσεις.	
Επιθέσεις WSDL	*Σάρωση WSDL* (WSDL Scanning)	Μέσα από στοιχεία που αποκαλύπτονται από την ανάλυση του WSDL αρχείου, ένας εισβολέας μπορεί να μαντέψει μεθόδους.	Δεν πρέπει να υπάρχει καμία διαρροή, χρήση SSL, χρήση μόνο αναγκαίων μεθόδων.
	Αλλοίωση Παραμέτρων (Parameter Tampering)	Ο εισβολέας τροποποιεί τις παραμέτρους προκειμένου να αποκτήσει μη εξουσιοδοτημένη πληροφορία.	Τεχνολογία Κρυπτογραφίας
Εσωτερικές Επιθέσεις(Internal)		Αυτές οι επιθέσεις ασκούνται στα πλαίσια των «firewalls» από έναν υπάλληλο ή πρώην υπάλληλο που συνήθως έχει πρόσβαση σε εμπιστευτικές πληροφορίες και είναι εξοικειωμένος με το εσωτερικό σύστημα του οργανισμού.	Χρήση τεχνικών ελαχίστων προνομίων και χορήγηση μόνο απολύτως απαραίτητης για την εργασία πρόσβασης.

Κεφάλαιο 4: Πολιτική Ασφάλειας

Εισαγωγή

Η πολιτική ασφάλειας των πληροφοριακών συστημάτων αποτελεί το βασικό εργαλείο για τη διαχείριση της ασφάλειας αυτών. Περιλαμβάνει το *σκοπό* και τους *στόχους* της ασφάλειας, καθώς και *οδηγίες*, *διαδικασίες*, *κανόνες*, *ρόλους* και *υπευθυνότητες* που αφορούν την προστασία των πληροφοριακών συστημάτων και εγκαταστάσεων ενός οργανισμού.

Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην πολιτική ασφάλειας υλοποιούνται με την εφαρμογή των μέτρων προστασίας ή ασφάλειας.

Η πολιτική ασφάλειας μαζί με το σύνολο των μέτρων προστασίας αποτελούν το Σχέδιο Ασφάλειας, για τα πληροφοριακά συστήματα ενός οργανισμού.

Η πολιτική ασφάλειας διατυπώνεται σε ένα έγγραφο, το οποίο θα πρέπει να γνωρίζουν και να εφαρμόζουν όλα τα μέλη του οργανισμού. Αυτό σημαίνει ότι η τήρηση των διαδικασιών και οδηγιών που προβλέπει η πολιτική ασφάλειας είναι υποχρεωτική για όλους τους χρήστες των πληροφοριακών συστημάτων.

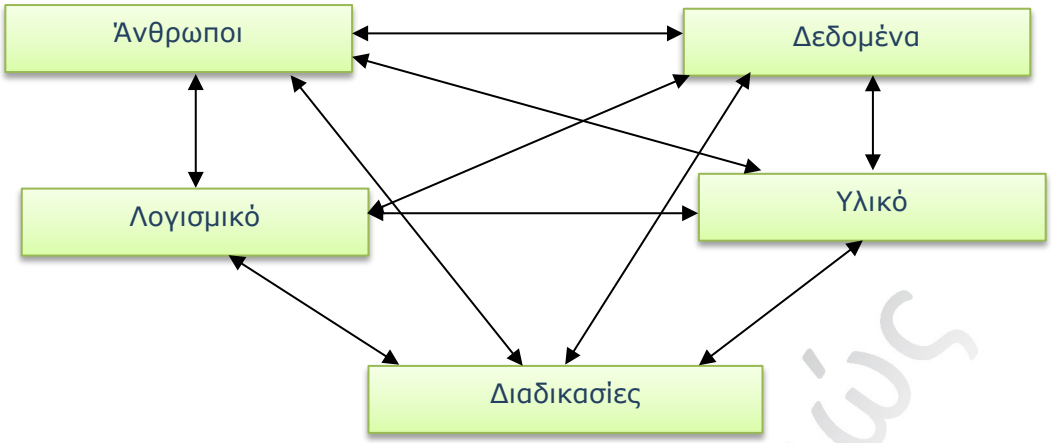
Η αποτελεσματική εφαρμογή της πολιτικής ασφάλειας εξαρτάται, από τη συμβολή της στην επίτευξη των στόχων του οργανισμού, από τη συμμετοχή της διοίκησης του οργανισμού στη διαμόρφωση της, από την ενεργή υποστήριξη της διοίκησης του οργανισμού σε όλες των διαδικασιών για την εφαρμογή της, από την σταδιακή εφαρμογή της, από την συμβατότητα με την οργανωσιακή κουλτούρα, από την ενημέρωση και ευαισθητοποίηση των χρηστών σε ζητήματα ασφάλειας, από την εκπαίδευση και κατάρτιση, από την αξιολόγηση, από τον υπεύθυνο ασφάλειας (Καρύδα, 2004).

Πληροφοριακό Σύστημα

Πληροφοριακό Σύστημα είναι ένας οργανωμένος συνδυασμός ανθρώπων, υλικού, λογισμικού, δικτύων επικοινωνίας, και πηγών δεδομένων, το οποίο συλλέγει, μετασχηματίζει, και διαχέει πληροφορίες σε έναν οργανισμό (Εικόνα 16).

Ποιο αναλυτικά:

- *το υλικό* (hardware), είναι ένα σύνολο συσκευών όπως επεξεργαστές, οθόνες, πληκτρολόγια που δέχονται δεδομένα και πληροφορίες, τα επεξεργάζονται και τα εμφανίζουν.
- *το λογισμικό* (software), είναι ένα σύνολο προγραμμάτων που δίνουν τη δυνατότητα στο υλικό να επεξεργαστεί τα δεδομένα.
- *η βάση δεδομένων* (database), είναι μία συλλογή σχετιζόμενων αρχείων, πινάκων, σχέσεων κλπ που αποθηκεύει δεδομένα και τις μεταξύ τους σχέσεις.
- *το δίκτυο*, είναι το σύστημα που επιτρέπει το μοίρασμα των (πληροφοριακών) πόρων σε διαφορετικούς Η/Υ.
- *οι διαδικασίες*, είναι ένα σύνολο οδηγιών/εντολών για το πώς συνδυάζονται τα ανωτέρω συστατικά μέρη έτσι ώστε να γίνεται η επεξεργασία των πληροφοριών και να παράγονται οι επιθυμητές εκροές και τέλος,
- *οι άνθρωποι*, δηλαδή τα άτομα που εργάζονται με το σύστημα ή χρησιμοποιούν τις εκροές του (το προσωπικό, τους ερευνητές, παραγωγούς, προμηθευτές και διαθέτες του συστήματος).

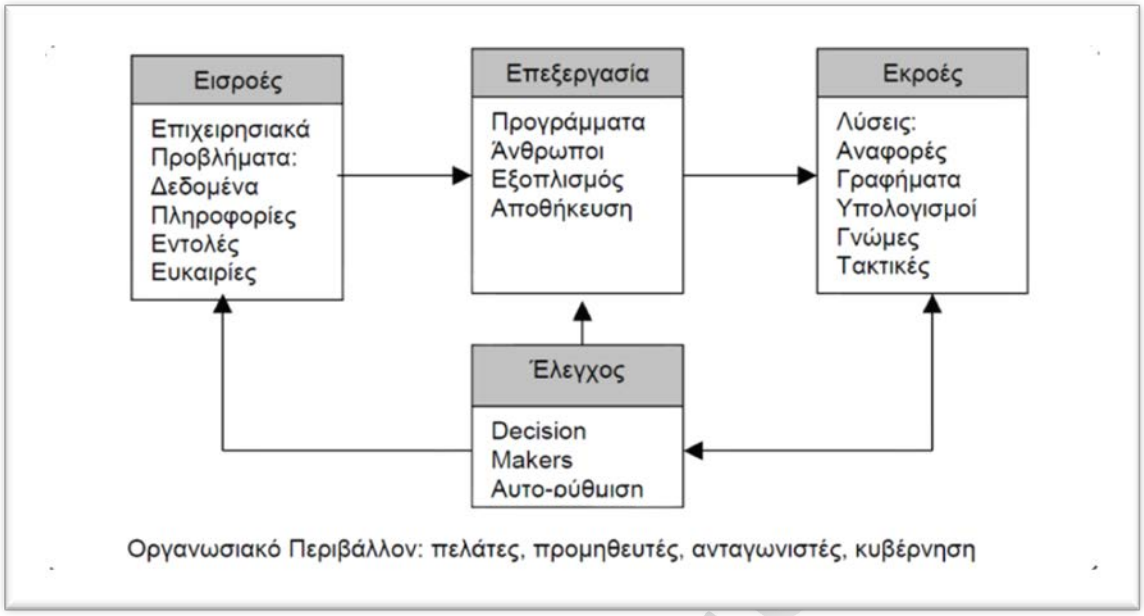


Εικόνα 16: Πληροφοριακό Σύστημα

Όπως όλα τα συστήματα έτσι και τα πληροφοριακά διακρίνονται συνήθως από κάποια συστατικά μέρη, τα οποία αποτελούν διακριτά χαρακτηριστικά του συστήματος. Τα μέρη αυτά, που ονομάζονται υποσυστήματα, έχουν εισροές, που μέσω κάποιας επεξεργασίας μετατρέπονται σε εκροές, λειτουργούν μέσα σε κάποιο περιβάλλον το οποίο και τα χαρακτηρίζει, ενώ υπάρχει και ένας μηχανισμός ανατροφοδότησής τους. Ειδικότερα, οι έννοιες εισροές, εκροές, επεξεργασία και ανατροφοδότηση στα πληροφοριακά συστήματα έχουν το εξής περιεχόμενο:

- *Εισροές*: η συλλογή ακατέργαστων δεδομένων (raw data), που μπορεί να είναι της μορφής «alpha», «numeric» ή «alphanumeric» και που προέρχονται είτε από το εσωτερικό της επιχείρησης είτε από το εξωτερικό περιβάλλον της (υλικά, πληροφορίες, ανθρώπινο δυναμικό, πόροι κ.λ.π.).
- *Επεξεργασία*: η μετατροπή, ο χειρισμός και η ανάλυση των ακατέργαστων δεδομένων σε τέτοια μορφή που έχουν περισσότερη σημασία για τα άτομα.
- *Εκροές*: η διανομή και διάχυση των επεξεργασμένων πληροφοριών στα άτομα ή στις δραστηριότητες που θα χρησιμοποιηθούν.
- *Ανατροφοδότηση (feedback)*: εκροή του συστήματος που επιστρέφει στα κατάλληλα μέλη της επιχείρησης για να τα βοηθήσει στην αξιολόγηση και διόρθωση των εισροών.

Σχηματικά μπορούμε να απεικονίσουμε τα συστατικά μέρη ενός πληροφοριακού συστήματος ως εξής:



Εικόνα 17: Συστατικά Μέρη ενός Πληροφοριακού Συστήματος

«ΕΥΔΟΞΟΣ» - Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων του Τμήματος Ψηφιακών Συστημάτων

Το λογισμικό «Open eClass», είναι η ελληνοποιημένη έκδοση του λογισμικού «*Claroline*» και αποτελεί την πρόταση του ακαδημαϊκού διαδικτύου GUnet, για την υποστήριξη της Υπηρεσίας Ασύγχρονης Τηλεκπαίδευσης. Αναπτύχθηκε και υποστηρίζεται ενεργά από την ομάδα ασύγχρονης τηλεκπαίδευσης του GUnet και διανέμεται ελεύθερα, ως λογισμικό ανοικτού κώδικα σύμφωνα με τη γενική δημόσια άδεια GNU General Public License (GNU GPL).

Το λογισμικό «Open eClass» είναι λογισμικό ανοικτού κώδικα, που σημαίνει ότι είναι δυνατή η διόρθωση προβλημάτων και η μετατροπή ή η εξέλιξη χαρακτηριστικών από εξειδικευμένο τεχνικό προσωπικό. Αυτό σημαίνει πως το λογισμικό «Open eClass» έχει την δυνατότητα περαιτέρω ανάπτυξης και προσαρμογής ανάλογα με τις απαιτήσεις του ιδρύματος που το φιλοξενεί.

Επιπλέον, έχει την δυνατότητα να προσαρμόζεται στις εκπαιδευτικές ανάγκες του κάθε καθηγητή και στις ιδιαιτερότητες του κάθε μαθήματος. Είναι δυνατή η ενεργοποίηση και απενεργοποίηση χαρακτηριστικών, ανάλογα με τις ανάγκες των χρηστών, δηλαδή είναι δυνατή η παραμετροποίηση του περιβάλλοντος εργασίας. Είναι ένα πλήρες και ολοκληρωμένο πρόγραμμα μαθησιακού περιεχομένου, που συμφέρει τα εκπαιδευτικά ιδρύματα να υποστηρίξουν.

Η πλατφόρμα ασύγχρονης τηλεκπαίδευσης του τμήματος Ψηφιακών Συστημάτων «ΕΥΔΟΞΟΣ», αποτελεί ένα ολοκληρωμένο Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων και βασίζεται στο λογισμικό ανοιχτού κώδικα «Open eClass».

Έχει σχεδιαστεί με προσανατολισμό την ενίσχυση της συμβατικής διδασκαλίας αξιοποιώντας την ήδη σε υψηλό βαθμό αφομοιωμένη στο χώρο της εκπαίδευσης πληροφορική τεχνολογία. Ακολουθεί τη φιλοσοφία του λογισμικού ανοικτού κώδικα και υποστηρίζει την υπηρεσία Ασύγχρονης Τηλεκπαίδευσης χωρίς περιορισμούς και δεσμεύσεις. Η πρόσβαση

στην υπηρεσία γίνεται με τη χρήση ενός απλού φυλλομετρητή, χωρίς την απαίτηση εξειδικευμένων τεχνικών γνώσεων.

Στόχος είναι η ενίσχυση της εκπαιδευτικής διαδικασίας, προσφέροντας στους συμμετέχοντες ένα δυναμικό περιβάλλον αλληλεπίδρασης και συνεχούς επικοινωνίας εκπαιδευτή - εκπαιδευόμενου. Ειδικότερα, επιτρέπει στον εκπαιδευτή την ηλεκτρονική οργάνωση, αποθήκευση και παρουσίαση του εκπαιδευτικού υλικού και παρέχει στον εκπαιδευόμενο ένα εναλλακτικό κανάλι εξατομικευμένης μάθησης ανεξάρτητο από χωροχρονικές δεσμεύσεις.

Τα βασικά στοιχεία που συνθέτουν την λειτουργία της είναι οι διακριτικοί ρόλοι των χρηστών, οι κατηγορίες των μαθημάτων και τα στοιχεία που συνθέτουν ένα μάθημα.

Ρόλοι Χρηστών

Η πλατφόρμα «ΕΥΔΟΞΟΣ» υποστηρίζει τρεις κατηγορίες χρηστών, *του καθηγητή*, του *εκπαιδευόμενου* και του *διαχειριστή*.

Ο καθηγητής μπορεί να δημιουργήσει όσα μαθήματα επιθυμεί, να διαχειριστεί τους εκπαιδευόμενους, να εισάγει και να επεξεργαστεί το εκπαιδευτικό υλικό του μαθήματος (κείμενα, εικόνες, παρουσιάσεις, video, κλπ.), να δημιουργήσει ομάδες συζητήσεων καθώς και ασκήσεις αυτοαξιολόγησης. Ο λογαριασμός του καθηγητή δημιουργείται από τους διαχειριστές της πλατφόρμας, κατόπιν αίτησης του ενδιαφερομένου και τα στοιχεία του λογαριασμού του αποστέλλονται αυτόματα μέσω ηλεκτρονικού ταχυδρομείου.

Ο εκπαιδευόμενος μπορεί να εγγραφεί σε όσα μαθήματα του επιτρέπεται, να μελετήσει το ψηφιακό υλικό, να συμμετάσχει σε ομάδες συζητήσεων καθώς και σε ασκήσεις αυτοαξιολόγησης. Ο λογαριασμός του εκπαιδευόμενου δημιουργείται αυτόματα με την εγγραφή του χωρίς την ανάγκη μεσολάβησης του διαχειριστή.

Τέλος ο διαχειριστής είναι αυτός που έχει την εποπτεία όλης της πλατφόρμας, δημιουργεί τους λογαριασμούς των καθηγητών, παρακολουθεί και διαχειρίζεται το «server» που φιλοξενεί την πλατφόρμα, παρακολουθεί και διαχειρίζεται τη βάση δεδομένων, μπορεί να διαχειρίζεται τα μαθήματα όλων των καθηγητών και διαχειρίζεται τους λογαριασμούς όλων των χρηστών.

Κατηγορίες Μαθημάτων

Η πλατφόρμα «ΕΥΔΟΞΟΣ» υποστηρίζει τρεις κατηγορίες μαθημάτων, *ανοικτά μαθήματα*, *ανοικτά σε εγγραφή μαθήματα*, *κλειστά μαθήματα*. Η κατηγορία στην οποία θα ανήκει ένα μάθημα καθορίζεται από τον καθηγητή κατά τη δημιουργία του μαθήματος. Η κατηγορία του μαθήματος μπορεί να αλλάζει δυναμικά από τον καθηγητή μέσα από την διεπαφή διαχείρισης του μαθήματος. Αναλυτικότερα οι κατηγορίες των μαθημάτων είναι:

- Ανοικτά μαθήματα θεωρούνται τα μαθήματα στα οποία μπορεί να έχει πρόσβαση ένας χρήστης ακόμα κι αν δεν έχει λογαριασμό στην πλατφόρμα. Τα μαθήματα αυτά παρουσιάζονται στην πρώτη σελίδα. Η κατηγορία αυτή είναι η εξ' ορισμού κατάσταση κατά τη δημιουργία νέου μαθήματος.
- Ανοικτά σε εγγραφή θεωρούνται τα μαθήματα στα οποία μπορεί να έχει πρόσβαση ένας χρήστης μόνο αν έχει λογαριασμό στην πλατφόρμα και έχει εγγραφεί σε αυτά.
- Κλειστά μαθήματα θεωρούνται τα μαθήματα στα οποία δεν μπορεί να εγγραφεί ένας χρήστης ακόμα κι αν έχει λογαριασμό στην πλατφόρμα. Πρόσβαση στα μαθήματα αυτά έχουν όσοι χρήστες εγγράφηκαν όταν το μάθημα ήταν σε άλλη κατάσταση

(ανοικτό, ανοικτό σε εγγραφή) ή εγγράφηκαν από τον ίδιο τον καθηγητή. Επίσης, στην κατηγορία αυτή περιέρχονται τα μαθήματα που ήταν ανοικτά σε εγγραφή και παρήλθε ο χρόνος εγγραφής.

Στοιχεία που Συνθέτουν ένα Μάθημα

Τα στοιχεία που εισάγονται από τον καθηγητή και συνθέτουν ένα ψηφιακό μάθημα στην πλατφόρμα «ΕΥΔΟΞΟΣ» είναι τα ακόλουθα:

- Η *Ατζέντα*, παρουσιάζει χρονικά τα γεγονότα σταθμούς του μαθήματος (διαλέξεις, συναντήσεις, αξιολογήσεις, κλπ).
- Τα *Έγγραφα*, περιέχουν το ψηφιακό υλικό του μαθήματος (κείμενα, εικόνες, παρουσιάσεις).
- Οι *Εργασίες Φοιτητών*, είναι η περιοχή που οι εκπαιδευόμενοι τοποθετούν τις εργασίες τους, τις οποίες διαχειρίζεται μόνο ο καθηγητής του μαθήματος.
- Η *Περιοχή Συζητήσεων*, για θέματα που αφορούν το μάθημα, τα οποία καθορίζονται από τον καθηγητή.
- Οι *Ομάδες Χρηστών*, είναι το εργαλείο που επιτρέπει τη δημιουργία και τη διαχείριση ομάδων εργασίας.
- Η *Κουβέντα*, περιοχή στην οποία μπορούν να πραγματοποιούνται συζητήσεις σε πραγματικό χρόνο ανάμεσα στον καθηγητή και στους εκπαιδευόμενους που είναι εγγεγραμμένοι στο μάθημα.
- *Σύνδεσμοι*, χρήσιμοι Σύνδεσμοι από το διαδίκτυο που αφορούν το μάθημα
- Στην περιοχή *Βίντεο*, που υπάρχουν αρχεία βίντεο (τύπου mpeg, avi κ.λπ.) που έχει ανεβάσει στην πλατφόρμα ο καθηγητής.
- Οι *Ανακοινώσεις*, από τον καθηγητή προς τους εκπαιδευόμενους.
- *Ασκήσεις αυτοαξιολόγησης*, τις οποίες δημιουργεί ο καθηγητής του μαθήματος.
- Ο χώρος *Ανταλλαγής Αρχείων*, που είναι ένα εργαλείο ανταλλαγής οποιουδήποτε τύπου αρχείων μεταξύ καθηγητή και εκπαιδευόμενων.
- Η *Περιγραφή Μαθήματος*, δίνει πληροφορίες που αφορούν τους στόχους του μαθήματος, τη δομή του, τους καθηγητές που το υποστηρίζουν κλπ.

Σε όλα τα παραπάνω στοιχεία δίνεται η δυνατότητα να ενεργοποιούνται ή να απενεργοποιούνται από τον καθηγητή ανάλογα με τη δομή και το υλικό του μαθήματος που διαθέτει, ώστε να απλοποιείται ακόμα περισσότερο το περιβάλλον του εκπαιδευομένου, και να εμφανίζονται μόνο οι απολύτως απαραίτητες ενότητες.

Παράλληλα δίνεται η δυνατότητα στον καθηγητή να παρακολουθεί στατιστικά στοιχεία που αφορούν τη συμμετοχή στο μάθημα, καθώς επίσης και η δυνατότητα να αλλάζει δυναμικά την κατάσταση στην οποία βρίσκεται το μάθημα (ανοικτό, ανοικτό σε εγγραφή, κλειστό).

Πολιτική Ασφαλείας στο Πληροφοριακό Σύστημα «ΕΥΔΟΞΟΣ»

Σκοπός της πολιτικής ασφάλειας είναι η αποφυγή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένους χρήστες (Εμπιστευτικότητα), η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας (Ακεραιότητα) και η αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες (Διαθεσιμότητα).

Ο οργανισμός με την βοήθεια της πολιτικής ασφάλειας καλείται να επιτύχει:

- Παροχή ποιοτικών υπηρεσιών του πληροφοριακού συστήματος και διασφάλιση της επιχειρησιακής του ικανότητας, στο βαθμό που αυτή εξαρτάται από την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα πληροφοριών και επικοινωνιών.
- Βελτιστοποίηση της αξιοποίησης της πληροφοριακής υποδομής του.
- Συμμόρφωση με τις απαιτήσεις που απορρέουν από την Ελληνική Νομοθεσία.
- Προστασία της επένδυσης που συνεπάγεται η ανάπτυξη και λειτουργία του Π.Σ.

Οι οδηγίες και τα μέτρα προστασίας που καθορίζει η πολιτική ασφάλειας του πληροφοριακού συστήματος «ΕΥΔΟΞΟΣ» πρέπει να καλύπτουν τις ακόλουθες κατηγορίες απαιτήσεων ασφαλείας: *Ζητήματα Προσωπικού*, *Διαχείριση Υλικού και Λογισμικού*, *Φυσική Ασφάλεια*, *Συμμόρφωση με Νομικές Υποχρεώσεις*, *Έλεγχος Πρόσβασης στα Πληροφοριακά συστήματα*, *Σχέδιο Συνεχής Λειτουργίας*, *Διαδικασίες Διαχείρισης της Πολιτικής Ασφάλειας*, *Οργανωτική Δομή* (Καρύδα, 2004).

Ρόλοι και Υποχρεώσεις Προσωπικού

Διαχειριστής Ασφάλειας

Διασφαλίζει ότι όλα τα συστήματα «ΙΤ» που χρησιμοποιούνται έχουν αξιολογηθεί δεόντως για τη συμμόρφωση με τις αρχές ασφάλειας και προστατεύονται από την πολιτική ασφάλειας.

Παρακολουθεί τη τήρηση των νόμων, για τη προστασία δεδομένων προσωπικού χαρακτήρα και διασφαλίζει τη φυσική ασφάλεια των υπολογιστών και του σχεδιασμού επιχειρησιακής συνέχειας.

Είναι υπεύθυνος για την παραλαβή όλων των αιτήσεων για την πρόσβαση των υποκειμένων στα δεδομένα τους που διατηρούνται, ελέγχει τις διαδικασίες ολοκλήρωσης αυτών των αιτήσεων, εξασφαλίζει ότι οι πληροφορίες που παρέχονται για τον εντοπισμό των δεδομένων είναι επαρκής και διασφαλίζει τη κοινοποίηση των σχετικών πληροφοριών στους αιτούντες εντός συγκεκριμένου χρονικού διαστήματος (το οποίο πρέπει να καθοριστεί).

Είναι υπεύθυνος για τη διασφάλιση ότι οι εργαζόμενοι είναι ενήμεροι για τις απαιτήσεις της προστασίας δεδομένων προσωπικού χαρακτήρα.

Διατηρεί τις εφαρμογές και τα «sites» ενημερωμένα.

Υπεύθυνος Ασφάλειας

Εστιάζει εντός του οργανισμού σε όλα τα θέματα ασφάλειας «ΙΤ».

Παραλαμβάνει και εξετάζει τις εκθέσεις για περιστατικά ασφάλειας «ΙΤ», προβαίνει στις κατάλληλες πράξεις και διαβιβάζει τις εκθέσεις στον υπεύθυνο «ΙΤ».

Παρέχει ενεργό ρόλο στη δημιουργία και εφαρμογή διαδικασιών που αφορούν την «IT» ασφάλεια και την ευαισθητοποίηση των εργαζομένων σε θέματα ασφάλειας.

Χρήστες

Υποχρεούνται να τηρούν την πολιτική ασφάλειας.

Υποχρεούνται να συμμορφώνονται με τη νομοθεσία.

Ειδοποιούν άμεσα το διαχειριστή ασφάλειας ή τον υπεύθυνο ασφάλειας αν διαπιστώσουν κάποιο περιστατικό ασφάλειας.

Ενημερώνουν άμεσα τον υπεύθυνο «IT» για οποιοδήποτε περιστατικό σχετικό με την προστασία δεδομένων προσωπικού χαρακτήρα.

Διαχείριση Υλικού και Λογισμικού

Έλεγχος Ιών

Κανένα αρχείο από δισκέτα, CD/DVD ή USB δεν πρέπει να μεταφερθεί σε οποιοδήποτε σύστημα αν δεν έχει ελεγχθεί από το τμήμα «IT».

Δισκέτες, CD/DVD ή USB που χρησιμοποιούνται για την αποστολή αρχείων σε εξωτερικούς χρήστες μπορούν να ελεγχθούν για ιούς πριν αποσταλθούν. Αν απαιτείται τότε το τμήμα «IT» είναι αρμόδιο για τον έλεγχο.

Όλοι οι servers και οι προσωπικοί υπολογιστές πρέπει να έχουν εγκατεστημένο «antivirus».

Όταν ανιχνευθεί ένας ιός τότε πρέπει να ενημερώνεται άμεσα το τμήμα «IT» που θα προσπαθήσει να «καθαρίσει», να επαναφέρει τον υπολογιστή και να ενημερώσει το «antivirus».

Προστασία Υλικού (hardware) από Κλοπή

Το «server room» πρέπει να είναι κλειδωμένο συνέχεια. Η πρόσβαση σε αυτό είναι περιορισμένη και εφόσον απαιτείται πρόσβαση τότε αυτή γίνεται υπό την επίβλεψη αρμόδιου από το τμήμα «IT».

Πρέπει να διατηρείται ένα αρχείο με το «hardware» και το ποιος είναι υπεύθυνος για αυτό.

Δεν επιτρέπεται η μετακίνηση «hardware» χωρίς την έγκριση του υπεύθυνου «IT», εκτός από τους φορητούς υπολογιστές, για τους οποίους είναι υπεύθυνοι οι χρήστες τους.

Για «hardware» που βρίσκεται σε μέρος που είναι τρωτό ή περιέχει δεδομένα προσωπικού χαρακτήρα πρέπει να γίνεται χρήση μέτρων φυσικής ασφάλειας όπως κλείδωμα πορτών.

Προστασία Υλικού από Φθορά Λόγω Ατυχήματος

Πρέπει να γίνεται προσεκτική χρήση φαγητών και ποτών κοντά σε «hardware». Ποτά και φαγητά δεν επιτρέπονται στο «server room».

Η θέση όλου του «hardware» πρέπει να είναι σύμφωνη με τα πρότυπα υγείας και ασφάλειας συμπεριλαμβανόμενης και της σταθερότητας των γραφείων και των ελεύθερων καλωδίων.

Όλοι οι προσωπικοί υπολογιστές και εκτυπωτές πρέπει να είναι απενεργοποιημένοι όταν δεν χρησιμοποιούνται για παρατεταμένες περιόδους, όπως τη νύχτα ή τα σαββατοκύριακα, εξαιρείται ο βασικός εξοπλισμός του «server room».

Μαγνητικά μέσα δεν πρέπει να τοποθετούνται δίπλα σε εκτυπωτές λέιζερ, φωτοτυπικά μηχανήματα ή τηλέφωνα, επειδή μπορεί να προκληθεί φθορά των αποθηκευμένων δεδομένων.

Δισκέτες, CD/DVD, USB πρέπει να ταυτοποιούνται και να φυλάσσονται σε κουτιά ή γραφεία με κλειδαριά.

Δεν πρέπει να εμποδίζονται οι αεραγωγοί των υπολογιστών.

Προστασία των Δεδομένων από Βλάβη Υλικού (hardware)

Αντίγραφα ασφαλείας των δεδομένων και των προγραμμάτων του συστήματος, πρέπει να λαμβάνονται σε τακτική βάση, όπως καθορίζεται από τον υπεύθυνο του πληροφοριακού συστήματος.

Τα δεδομένα δεν πρέπει να κρατούνται σε τοπικό επίπεδο στους υπολογιστές, καθώς αυτό δεν περιλαμβάνεται στην αυτόματη νυχτερινή δημιουργία αντιγράφων ασφαλείας των εξυπηρετητών του δικτύου. Τα δεδομένα πρέπει να αποθηκεύονται σε φακέλους στους εξυπηρετητές του δικτύου.

Τα αντίγραφα ασφαλείας πρέπει να φυλάσσονται με ασφάλεια εκτός του χώρου του κεντρικού «server».

Οι διαδικασίες ανάκτησης των δεδομένων από τα αντίγραφα ασφαλείας πρέπει να ελέγχονται σε τακτική βάση, όπως καθορίζεται από τους υπεύθυνους συντήρησης του πληροφοριακού συστήματος.

Προστασία των Δεδομένων από μη Εξουσιοδοτημένη Πρόσβαση

Πρέπει να εφαρμόζονται έλεγχοι των κωδικών. Οι κωδικοί πρόσβασης πρέπει να είναι τουλάχιστον πέντε χαρακτήρες, να περιλαμβάνουν γράμματα και αριθμούς, να είναι διαφορετικοί από αυτούς που έχουν ήδη χρησιμοποιηθεί, να έχουν δημιουργηθεί από τους χρήστες.

Οι κωδικοί πρόσβασης πρέπει να αλλάζουν τουλάχιστον μία φορά κάθε σαράντα μέρες.

Οι λεπτομέρειες για τους κωδικούς πρόσβασης καταγράφονται από τους υπεύθυνους του πληροφοριακού συστήματος και διατηρούνται σε ασφαλές μέρος.

Οι αναφορές που περιέχουν ευαίσθητες πληροφορίες και οι οποίες απαιτείται να διατεθούν πρέπει μετά τη χρήση να τοποθετούνται σε ειδικούς κάδους για κατατεμαχισμό.

Τα αντίγραφα ασφαλείας και τα αντίγραφα των δεδομένων πρέπει να αποθηκεύονται με ασφάλεια εκτός του χώρου του κεντρικού «server».

Όλα τα μέσα αποθήκευσης, συμπεριλαμβανομένων των αντιγράφων ασφαλείας πρέπει να έχουν ιδιαίτερη σήμανση για να αποφευχθεί οποιαδήποτε σύγχυση ως προς το περιεχόμενό τους.

Έλεγχος Λογισμικού

Όλο το λογισμικό πρέπει να αγοραστεί μέσω του τμήματος «IT» και δεν πρέπει να εγκατασταθεί κανένα λογισμικό συμπεριλαμβανομένου λογισμικού χωρίς άδεια από το τμήμα «IT».

Πρέπει να διατηρείται μητρώο (register) των λογισμικών από τους υπεύθυνους «IT».

Το λογισμικό δεν επιτρέπεται να αντιγράφεται, δεδομένου ότι αυτό συνιστά παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας και ως εκ τούτου είναι παράνομο – εκτός αν έχει ρητά επιτραπεί από την άδεια χρήσης, η οποία περιλαμβάνει την εγκατάσταση του λογισμικού από ένα σετ δίσκων(CDs) επάνω σε κάποιο αριθμό υπολογιστών.

Όλοι οι δίσκοι που περιλαμβάνουν το λογισμικό του συστήματος πρέπει να φυλάσσονται με ασφάλεια στο «IT» «server room». Αυτά είναι τα μόνα αποδεικτικά στοιχεία για τη νόμιμη άδεια χρήσης του λογισμικού, και μπορεί να απαιτηθεί να παρουσιαστούν ως αποδεικτικά στοιχεία στην Αρχή Προστασίας Πνευματικών Δικαιωμάτων.

Προστασία Προσωπικών Δεδομένων

Ο οργανισμός έχει την υποχρέωση να τηρεί τις διατάξεις του νόμου 2472/1997, για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Το ανθρώπινο δυναμικό έχει το δικαίωμα σεβασμού της ιδιωτικής του ζωής και συνεπώς προσδοκά ότι οι πληροφορίες που το αφορούν πρέπει να αντιμετωπίζονται ως εμπιστευτικές.

Όλοι οι εργαζόμενοι και εξωτερικοί συνεργάτες του οργανισμού έχουν έννομο καθήκον μέριμνας για την προστασία των προσωπικών πληροφοριών.

Όλα τα τμήματα/μονάδες του οργανισμού, πρέπει να έχουν μια ενεργό πολιτική για την ενημέρωση των υποκειμένων σχετικά με το είδος των δεδομένων και των σκοπών για τους οποίους αυτές οι πληροφορίες, συλλέγονται.

Διαδικασίες (αυτοματοποιημένες ή μη) για την αποθήκευση, διάθεση και χειρισμό των πληροφοριών, πρέπει να προστατεύουν την εμπιστευτικότητα. Πρέπει να ληφθεί μέριμνα για την αποφυγή της ακούσιας παραβίασης της εμπιστοσύνης.

Η παραβίαση της εμπιστευτικότητας είναι ένα σοβαρό ζήτημα που μπορεί να οδηγήσει σε πειθαρχικές κυρώσεις.

Όλες οι αιτήσεις για λήψη δεδομένων πρέπει να διαβιβάζονται στον υπεύθυνο του πληροφοριακού συστήματος ή τον υπεύθυνο για την προστασία των δεδομένων.

Προστασία από Απομακρυσμένη Πρόσβαση

Ασύρματη Πρόσβαση

Όπου υπάρχει απομακρυσμένη πρόσβαση του δικτύου μέσω ασύρματων συνδέσεων το δίκτυο πρέπει να ρυθμιστεί ώστε να μη διαφημίζει την ύπαρξη του, η ισχύ του σημείου πρόσβασης πρέπει να οριστεί στη χαμηλότερη τιμή, που διασφαλίζεται η λειτουργία του, να χρησιμοποιείται το «WPA2» ως πρότυπο ασφάλειας της σύνδεσης.

Ασφαλής Πρόσβαση μέσω VPN

Η πρόσβαση του δικτύου από απομακρυσμένους χρήστες πρέπει να γίνεται μόνο μέσω «IPSec VPN» ή «SSL VPN» συνδέσεις. Αυτό κρίνεται απαραίτητο για την ασφαλή σύνδεση της απομακρυσμένης συσκευής με το δίκτυο.

Πρόληψη από την Απώλεια Δεδομένων

Όλοι οι φορητοί υπολογιστές πρέπει να έχουν τις ακόλουθες ρυθμίσεις ασφάλειας για την αποφυγή της κλοπής δεδομένων.

- Όλα τα δεδομένα του οργανισμού στο φορητό υπολογιστή πρέπει να είναι κρυπτογραφημένα χρησιμοποιώντας το κατάλληλο λογισμικό κρυπτογράφησης.
- Θα επιτρέπεται απομακρυσμένη πρόσβαση σε εμπιστευτικά έγγραφα του οργανισμού, όχι όμως η λήψη αυτών.

Προστασία Απομακρυσμένων Συσκευών

Για την αποφυγή κινδύνων του δικτύου του οργανισμού πρέπει να εγκατασταθεί λογισμικό ασφαλείας στις συσκευές.

- Λογισμικό «firewall» πρέπει να εγκατασταθεί στις συσκευές για αποφυγή κινδύνων «trojans» και «back door».
- Το λογισμικό «antivirus» πρέπει να ρυθμιστεί έτσι ώστε να πραγματοποιείται αυτόματη λήψη ενημερώσεων.

Αυθεντικοποίηση

Η αυθεντικοποίηση των απομακρυσμένων συσκευών που συνδέονται στο δίκτυο, πρέπει να γίνει με τη χρήση ψηφιακών πιστοποιητικών.

Σχέδιο Συνέχισης Λειτουργίας

Η πολιτική ασφάλειας πρέπει να περιλαμβάνει οδηγίες που αφορούν τις απαιτούμενες ενέργειες μετά την πραγματοποίηση ενός σημαντικού περιστατικού παραβίασης της ασφάλειας, ώστε οι λειτουργίες του οργανισμού να εξακολουθήσουν να πραγματοποιούνται με κάποιους εναλλακτικούς τρόπους, έως ότου αντιμετωπιστεί το πρόβλημα ασφάλειας του πληροφοριακού συστήματος. Για παράδειγμα πρέπει να υπάρχει εφεδρικός «Web Server».

Διαδικασίες Διαχείρισης της Πολιτική Ασφάλειας

Ένα σημαντικό κομμάτι της πολιτικής ασφάλειας περιγράφει και προσδιορίζει τις λοιπές δραστηριότητες που πρέπει να συνοδεύουν την εφαρμογή της, ώστε να είναι αποτελεσματική η διαχείριση της ασφάλειας του πληροφοριακού συστήματος. Αυτές οι διαδικασίες περιλαμβάνουν:

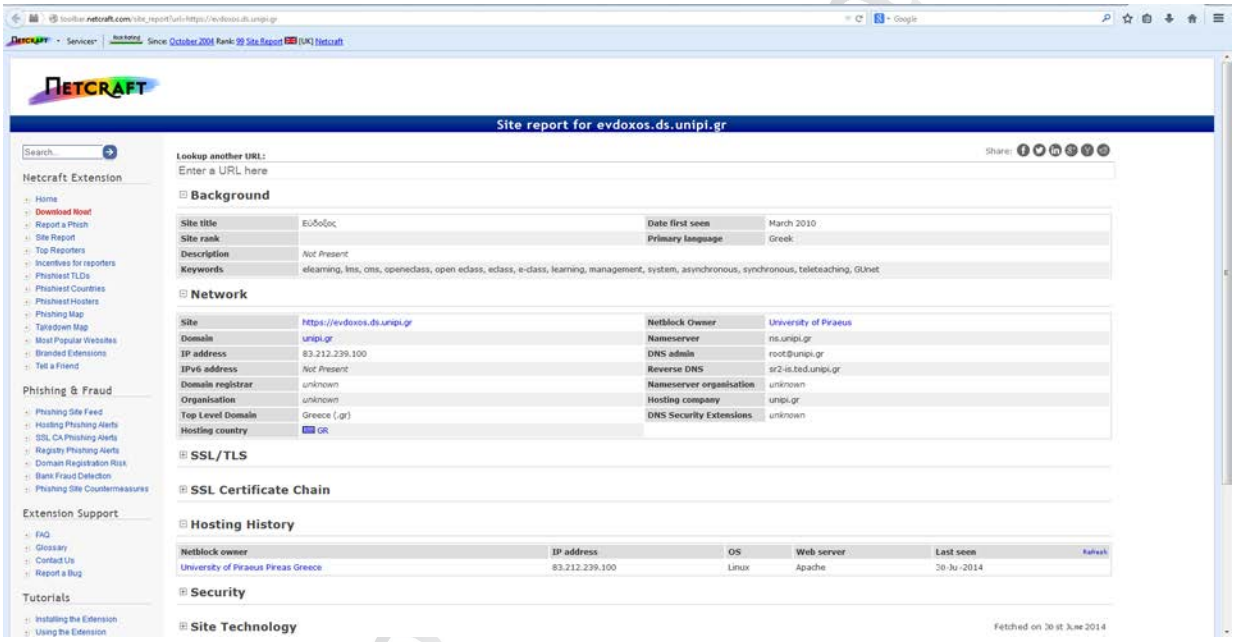
- **Την αξιολόγηση και αναθεώρηση της πολιτικής**. Η πολιτική ασφάλεια πρέπει να αξιολογείται και να αναθεωρείται, τόσο ως προς το περιεχόμενο όσο και ως προς τις διαδικασίες εφαρμογής της.

- **Τον έλεγχο και τη συμμόρφωση με την πολιτική ασφάλειας**. Στην πολιτική ασφάλειας πρέπει να καθορίζονται οι διαδικασίες με τις οποίες ελέγχεται (auditing) η εφαρμογή της πολιτικής από τους χρήστες του πληροφοριακού συστήματος, καθώς και οι διαδικασίες για το χειρισμό των περιστατικών μη συμμόρφωσης με αυτή.

Κεφάλαιο 5: Ανίχνευση Ευπαθειών στο Πληροφοριακό Σύστημα «ΕΥΔΟΞΟΣ»

Η ανίχνευση ευπαθειών σε ένα πληροφοριακό σύστημα αποτελεί ένα ισχυρό και αποτελεσματικό εργαλείο εναντίον όλων όσων θέλουν να το βλάψουν.

Για την ανίχνευση ευπαθειών στο πληροφοριακό σύστημα «ΕΥΔΟΞΟΣ» (*https://evdoxos.ds.unipi.gr/*), στην αρχή ο «pentester» συλλέγει όσες δημόσια διαθέσιμες πληροφορίες είναι δυνατόν να εντοπιστούν σχετικά με το στόχο, μέσω της ιστοσελίδας «*netcraft.com*». Η ιστοσελίδα αυτή σαρώνει (crawl) σε τακτά χρονικά διαστήματα τον παγκόσμιο ιστό, συλλέγει δεδομένα (όπως τύπος του «server», έκδοση του λειτουργικού συστήματος) από τα διάφορα μηχανήματα που συναντά και τα αρχειοθετεί. Στην Εικόνα 18 παρουσιάζονται οι πληροφορίες που συνέλεξε η ιστοσελίδα «netcraft.com» από το στόχο «*https://evdoxos.ds.unipi.gr/*».

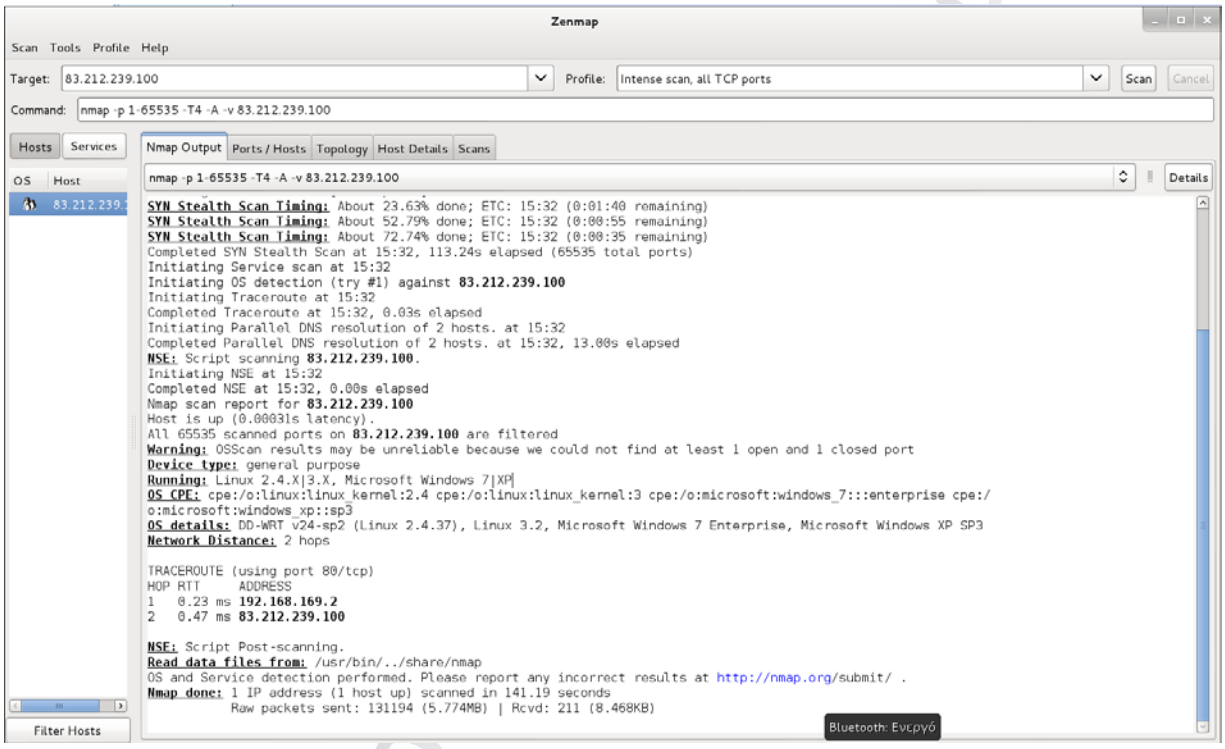


Εικόνα 18: netcraft

Στην συνέχεια, ο «pentester» για να βρει περισσότερες πληροφορίες για το λειτουργικό σύστημα χρησιμοποιεί την εφαρμογή «Zenmap» (Εικόνα 19).

Το «Zenmap» χρησιμοποιεί ακατέργαστα πακέτα προς όλες τις διαθέσιμες «IP», για να μπορέσει να εντοπίσει αν υπάρχουν διαθέσιμοι ενεργοί εξυπηρετητές, τι υπηρεσίες έχουν αυτοί οι εξυπηρετητές, τι λειτουργικό σύστημα διαθέτουν, τι τύπο τοίχου προστασίας ή φίλτρων χρησιμοποιούν καθώς και πολλά ακόμα τέτοια χαρακτηριστικά. Το «Zenmap» χρησιμοποιείται πάρα πολύ από διαχειριστές συστήματος για να δουν από τα πιο απλά χαρακτηριστικά ενός εξυπηρετητή, όπως είναι η ώρα που βρίσκεται «on-line», ως τα πιο σύνθετα που είναι ο έλεγχος ασφάλειας. Η έξοδος του «Zenmap» είναι μια λίστα από στόχους που έχουν ελεγχθεί, που περιλαμβάνει αρκετά χαρακτηριστικά ανάλογα με τις αρχικές παραμέτρους που έχουν τεθεί. Το ποιο ενδιαφέρον χαρακτηριστικό σε αυτές τις λίστες είναι το «*port table*», το όποιο δείχνει όλες τις διαθέσιμες πόρτες που απάντησαν στον έλεγχο μαζί με το πρωτόκολλο που χρησιμοποιούν, την υπηρεσία που φιλοξενούν καθώς και τη κατάσταση στην οποία βρίσκονται. Η κατάσταση αυτή μπορεί να είναι «*open*», «*closed*», «*filtered*» ή «*unfiltered*».

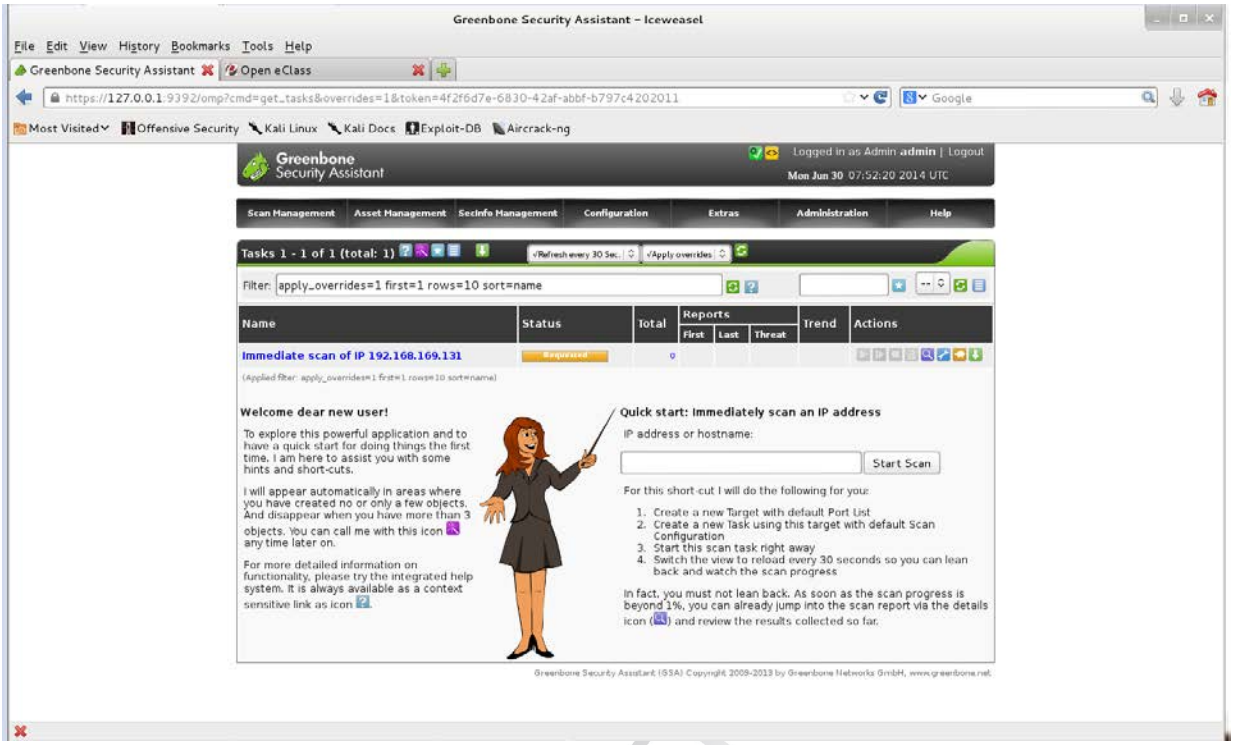
- **Open**. Σημαίνει ότι μια εφαρμογή στο μηχάνημα – στόχο ακούει στην πόρτα αυτή και είναι έτοιμη για σύνδεση.
- **Closed**. Σημαίνει ότι δεν υπάρχει κάποια εφαρμογή στο μηχάνημα – στόχο που να απαντάει στον έλεγχο.
- **Filtered**. Σημαίνει ότι ένα τοίχος προστασίας ή κάποιο φίλτρο μπλοκάρει τη σύνδεση, έτσι το πρόγραμμα «Zenmap» δεν μπορεί να διευκρινίσει αν η πόρτα αυτή είναι «open» ή «closed».
- **Unfiltered**. Σημαίνει ότι μια εφαρμογή στο μηχάνημα – στόχο ακούει στην πόρτα αυτή, αλλά το πρόγραμμα «Zenmap» για άγνωστο λόγο δεν μπορεί να προσδιορίσει αν είναι «open» ή «closed».



Εικόνα 19: Zenmap

Κατόπιν, για λόγους ασφαλείας η ανίχνευση ευπαθειών συνεχίζεται σε εικονικό περιβάλλον. Ο «pentester» εγκαθιστά α) τα λειτουργικά συστήματα «Kali Linux» και «CentOS 6.5» στο προηγμένο λογισμικό εικονικής μηχανής «VMware Workstation», σε περιβάλλον Windows (Παράρτημα Α, Παράτημα Γ), β) την εφαρμογή «OpenVAS» στο λειτουργικό σύστημα «Kali Linux» (Παράρτημα Β), γ) τα λογισμικά MySQL 5.5.x, Apache HTTP Server 2.2.x, PHP 5.5.x και phpMyAdmin 4.2.x στο λειτουργικό σύστημα «CentOS 6.5» (Παράτημα Δ), δ) το λογισμικό «Open eClass 2.10», στο λειτουργικό σύστημα «CentOS 6.5».

Αμέσως μετά, ο «pentester» σαρώνει το στόχο (Open eClass) με την εφαρμογή «OpenVAS» (Εικόνα 20).



Εικόνα 20: Σάρωση του Λογισμικού «Open eClass» με την Εφαρμογή «OpenVAS»

Μετά την σάρωση, εντοπίζονται ευπάθειες υψηλής, μέσης και χαμηλής επικινδυνότητας. Οι ευπάθειες, μέσης και χαμηλής επικινδυνότητας δεν παρουσιάζουν ιδιαίτερο ενδιαφέρον. Σαν υψηλού κινδύνου τρωτότητα το «OpenVAS» αναφέρει την πιθανότητα ευπάθειας σε επιθέσεις «***http TRACE XSS attack***» (Παράτημα Ε). Πιο συγκεκριμένα το «OpenVAS» αναφέρει ότι, ο απομακρυσμένος «server» υποστηρίζει τις μεθόδους «*TRACE*» ή/και «*TRACK*».

Οι μέθοδοι «HTTP TRACE» ή/και «HTTP TRACK» είναι «HTTP» μέθοδοι που χρησιμοποιούνται για τη αποσφαλμάτωση των «web server» συνδέσεων. Οι «servers» που υποστηρίζουν αυτές τις μεθόδους, υφίστανται «*cross-site-scripting*» (XSS) επιθέσεις όταν συνδυάζονται και με άλλες αδυναμίες των φυλλομετρητών. Οι επιθέσεις αυτές ονομάζονται «cross-site-tracing» (XST) επιθέσεις.

Στις «XST» επιθέσεις, ο εισβολέας εκμεταλλεύεται το γεγονός ότι ο απομακρυσμένος «server» υποστηρίζει τις μεθόδους «TRACE» ή/και «TRACK», έτσι ώστε να ξεγελάσει τους νόμιμους χρήστες, με σκοπό αυτοί να του δώσουν τα διαπιστευτήριά τους.

Η λύση που προτείνεται είναι να απενεργοποιηθούν οι παραπάνω μέθοδοι με την προσθήκη των ακόλουθων γραμμών σε κάθε «virtual host» στο αρχείο διαμόρφωσης:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Κεφάλαιο 6: Συμπεράσματα - Προτάσεις

Οι *υπηρεσίες ιστού* (web services) είναι μια τεχνολογία, που επιτρέπει στις εφαρμογές να επικοινωνούν μεταξύ τους ανεξαρτήτως πλατφόρμας και γλώσσας προγραμματισμού, μέσω προτύπων XML μηνυμάτων. Μια υπηρεσία ιστού χαρακτηρίζεται από τα πρότυπα «*SOAP*», «*WSDL*» και«*UDDI*», που στο σύνολό τους υλοποιούν μια βασική λειτουργία «*αίτησης και απόκρισης*».

Η «XML» είναι ένας πολύτιμος μηχανισμός για την ανταλλαγή δεδομένων μέσω του διαδικτύου. Το «SOAP» είναι ένα πρωτόκολλο για αποστολή μηνυμάτων XML και διευκολύνει τη διαδικασία ενδοεπικοινωνίας με τρόπους που δεν ήταν δυνατοί πιο πριν. Η «WSDL» περιγράφει τα περιεχόμενα των μηνυμάτων, ορίζει πού είναι διαθέσιμη μία υπηρεσία ιστού και ποιά πρωτόκολλα επικοινωνίας χρησιμοποιούνται για να επικοινωνήσει ο χρήστης με αυτή την υπηρεσία. Το «UDDI» είναι μια κεντρική υπηρεσία καταλόγου, όπου υπηρεσίες ιστού μπορούν να καταχωρηθούν και να προσδιοριστούν σε έναν παροχέα υπηρεσιών.

Εξαιτίας των κακόβουλων επιθέσεων που πραγματοποιούνται σε αυτές τις υπηρεσίες, και επειδή πρέπει να εξασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικοποίηση και η εξουσιοδότηση αυτών των υπηρεσιών αναπτύχθηκαν πρότυπα ασφάλειας.

Πρότυπα ασφάλειας υπάρχουν για την εμπιστευτικότητα (XML κρυπτογράφηση), για επικύρωση της προέλευσης των μηνυμάτων (XML ψηφιακές υπογραφές), για διαχείριση δημόσιου κλειδιού (XKMS), για πιστοποίηση και εξουσιοδότηση (SAML) και για τη δήλωση πολιτικών εξουσιοδότησης (XACML).

Ένα πληροφοριακό σύστημα είναι ένας οργανωμένος συνδυασμός ανθρώπων, υλικού, λογισμικού, δικτύων επικοινωνίας, και πηγών δεδομένων, το οποίο συλλέγει, μετασχηματίζει, και διαχέει πληροφορίες σε έναν οργανισμό.

Η πολιτική ασφάλειας των πληροφοριακών συστημάτων αποτελεί το βασικό εργαλείο για τη διαχείριση της ασφάλειας αυτών. Στην πολιτική ασφάλειας καθορίζονται οι στόχοι της ασφάλειας καθώς και ο τρόπος με τον οποίο οι στόχοι αυτοί θα υλοποιηθούν. Βασικό συστατικό στοιχείο κάθε πολιτικής ασφάλειας πληροφοριακού συστήματος είναι η περιγραφή των κανόνων και των διαδικασιών που πρέπει να ακολουθούνται για την προστασία των πληροφοριακών συστημάτων, καθώς και ο καθορισμός των συγκεκριμένων ρόλων και αρμοδιοτήτων που απαιτούνται για την υλοποίηση της πολιτικής ασφάλειας. Η εφαρμογή μιας πολιτικής ασφάλειας σε έναν οργανισμό έχει δεσμευτικό χαρακτήρα για όλα τα μέλη του οργανισμού.

Η ανίχνευση ευπαθειών σε ένα πληροφοριακό σύστημα αποτελεί ένα ισχυρό και αποτελεσματικό εργαλείο εναντίον όλων όσων θέλουν να το βλάψουν. Η προστασία του υπό εξέταση πληροφοριακού συστήματος και η διασφάλιση των βασικών αρχών ασφάλειας του εκάστοτε οργανισμού, ο οποίος κατέχει το εν λόγω σύστημα προκύπτει με την μέθοδο «Penetration Testing».

Μελλοντικά, θα μπορούσαν να πραγματοποιηθούν διάφορες επεκτάσεις της παρούσας εργασίας. Ενδεικτικά, προτείνεται η υλοποίηση μιας υπηρεσίας ιστού, μεταξύ του πληροφοριακού συστήματος «ΕΥΔΟΞΟΣ» (*https://evdoxos.ds.unipi.gr/*) και της υπηρεσίας πληροφόρησης φοιτητών του Πανεπιστημίου Πειραιώς (*https://students.unipi.gr/*), η οποία θα δέχεται το Α.Μ του φοιτητή και θα επιστρέφει την βαθμολογία του. Η υλοποίηση της συγκεκριμένης υπηρεσίας ιστού θα πρέπει να κάνει χρήση του προτύπου ασφαλείας «SAML», προκειμένου να τηρηθούν οι απαιτήσεις ασφάλειας.

Βιβλιογραφικές Αναφορές

Actional Corporation (2004). *The Web Services Security Threat.* Available from: «http://www.metz.supelec.fr/metz/personnel/galtier/PagesPerso/Enseignement/3A/SOA/Articles/web_service_security_threat.pdf».

Chappell, D. & Jewell, T. (2002). *Java Web Services*. O'Reilly & Associates publications.

Chitnis, M., Tiwari, P., Ananthamurthy, L. (2002). *Introducing Web Services Part 2: Architecture*. Available from: «http://www.developer.com/services/article.php/1495091/Introduction-to-Web-Services---Part-2-Architecture.htm».

Micro Focus (2013). *Simple Object Access Protocol (SOAP)*. Available from: «http://documentation.microfocus.com/help/index.jsp?topic=%2Fcom.microfocus.silkperformer.doc%2FGUID-FEFE9379-8382-48C7-984D-55D98D6BFD37.html».

Newcomer, E. (2002). *Understanding Web Services XML, WSDL, SOAP, and UDDI*. Addison -Wesley publications.

Refsnes Data (2013a). *Introduction to XML*. Available from: «http://www.w3schools.com/xml/xml_whatis.asp».

Refsnes Data (2013b). *SOAP Syntax*. Available from: «http://www.w3schools.com/soap/soap_syntax.asp».

Refsnes Data (2013c). *SOAP Example*. Available from: «http://www.w3schools.com/soap/soap_example.asp».

Refsnes Data (2013d). *XML Schema Tutorial*. Available from: «http://www.w3schools.com/schema/default.asp».

Shah, S. (2007). Advanced *web services hacking, Attacks & Defense*. Available from: «http://www.slideshare.net/shreeraj/advanced-web-services-hacking».

Singhal, A., Winogradm T., Scarfone, K. (2007). *Guide to Secure Web Services*. National Institute of Standards and Technology Special Publication, pp 800-895. Available from: «http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf».

Vasudevan, V. (2001). *A Web Services Primer*. Available from: «http://www.xml.com/pub/a/ws/2001/04/04/webservices/#uddi_toc».

Δημητρίου, Θ. (2007). *Web Services και Soap*, εργασία του τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας, Επιβλέπων: Καθηγητής Μαργαρίτης Κ.

Ηλιακόπουλος, Ι. (2009). *Αρχιτεκτονική ασφαλείας εφαρμογών και υπηρεσιών web services*. Διπλωματική Εργασία, Επιβλέπων Καθηγητής: Σερπάνος Δ., Σχολή: Ηλεκτρολόγων Μηχανικών και Τεχνολογίας, Τομέας: Ηλεκτρονικής και Υπολογιστών, Πολυτεχνική Σχολή Πάτρας.

Καρύδα, Μ. (2004). Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων. Στο Σ. Κάτσικα, Δ. Γκρίτζαλη & Σ. Γκρίτζαλη (Επιμ.), *Ασφάλεια Πληροφοριακών Συστημάτων* (σελ. 377-406). Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

Κεμάλης, Κ. και Μακροβασίλης Α. (2005). *Ασφάλεια σε Υπηρεσίες Ιστού*, εργασία του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου, Επιβλέπων: Λέκτορας Τζουραμάνης Θ.

Πολέμη, Ν. και Καλιοντζόγλου, Α. (2008). *Πρακτικά θέματα Ασφάλειας Πληροφοριακών Συστημάτων και Εφαρμογών*, Εκδόσεις νέων Τεχνολογιών, Αθήνα.

Παράρτημα

Α. Εγκατάσταση του Λειτουργικού Συστήματος «Kali Linux» στο Προηγμένο Λογισμικό Εικονικής Μηχανής VMware Workstation σε Περιβάλλον Windows

Για να κατεβάσει ο οποιοσδήποτε χρήστης το λειτουργικό σύστημα «*Kali Linux*», πηγαίνει στην ηλεκτρονική διεύθυνση «http://www.kali.org/downloads/» και κατεβάζει την τελευταία έκδοση του λειτουργικού, σύμφωνα με την αρχιτεκτονική του υπολογιστή (i386 ή amd64 ή armel ή armhf), στον οποίο πρόκειται να εγκατασταθεί. Το αρχείο που κατεβαίνει είναι της μορφής «.iso» και ο χρήστης είτε το «καίει» σε ένα DVD είτε το αφήνει ως έχει.

Η εικονικοποίηση (virtualization) είναι μια τεχνολογία λογισμικού, που επιτρέπει να τρέχουν ταυτοχρόνως πολλά λειτουργικά συστήματα στην ίδια φυσική μηχανή. Μια εικονική μηχανή είναι ένα απομονωμένο τμήμα λογισμικού, δεν περιέχει κανένα τμήμα υλικού (hardware) και μπορεί να τρέχει το εκάστοτε λειτουργικό σύστημα, όπως ένας φυσικός υπολογιστής. Οι εικονικές μηχανές μοιράζονται τους πόρους του υλικού, χωρίς να παρεμβάλλεται η μια με την άλλη, έτσι ώστε να τρέχουν ταυτόχρονα διάφορα λειτουργικά συστήματα και διάφορες εφαρμογές σε ένα ενιαίο υπολογιστή.

Ένα από τα καλύτερα προγράμματα εικονικοποίησης είναι το «*VMware Workstation*». Για να κατεβάσει ο οποιοσδήποτε χρήστης το λογισμικό «*VMware Workstation*», πηγαίνει στην ηλεκτρονική διεύθυνση «http://www.vmware.com/products/workstation/index.html» και κατεβάζει την τελευταία «*trial*» έκδοση του προγράμματος ή προχωράει στην αγορά του. Στην συνέχεια, ο χρήστης εκτελεί το αρχείο «*VMware-workstation-x.exe*» και προβαίνει στην εγκατάσταση του προγράμματος «*VMware Workstation*». Μόλις ολοκληρωθεί με επιτυχία η εγκατάσταση του προγράμματος, ο χρήστης επανεκκινεί τον υπολογιστή του. Κατόπιν, ανοίγει το πρόγραμμα «*VMware Workstation*», εμφανίζεται ή αρχική οθόνη της Εικόνα 21 και ακολουθεί τα επόμενα βήματα.

Στο βήμα 1 (Εικόνα 22), επιλέγει «*Create a New Virtual Machine*», προκειμένου να δημιουργήσει μια νέα εικονική μηχανή στον υπολογιστή του.

Στο βήμα 2 (Εικόνα 23), επιλέγει το είδος της διαμόρφωσης εγκατάστασης που θα ακολουθήσει ο βοηθός εγκατάστασης του προγράμματος και ενεργοποιεί το κουμπί «*Next*».

Στο βήμα 3 (Εικόνα 24), επιλέγει τον τρόπο με τον οποίο θα εγκαταστήσει το λειτουργικό σύστημα «*Kali Linux*» και ενεργοποιεί το κουμπί «*Next*».

Στο βήμα 4 (Εικόνα 25), επιλέγει το λειτουργικό σύστημα και την έκδοση αυτού. Επειδή, το λειτουργικό σύστημα «*Kali Linux*» είναι βασισμένο στο λειτουργικό σύστημα «Debian 6», ο χρήστης στη περιοχή «*Version*» επιλέγει είτε «*Debian 6*» είτε «*Debian 6 64-bit*» ανάλογα με την έκδοση (32bit ή 64bit) του λειτουργικού συστήματος που θέλει να εγκαταστήσει. Στην συνέχεια, ενεργοποιεί το κουμπί «*Next*».

Στο βήμα 5 (Εικόνα 26), εισάγει το όνομα της εικονικής μηχανής και εφόσον το επιθυμεί αλλάζει το μονοπάτι του φακέλου μέσα στον οποίο θα εγκατασταθεί η εικονική μηχανή. Αμέσως μετά, ενεργοποιεί το κουμπί «*Next*».

Στο βήμα 6 (Εικόνα 27), εισάγει το μέγεθος χωρητικότητας που θα έχει ο εικονικός δίσκος και επιλέγει «*Store virtual disk as a single file*», για να μην μειωθεί η απόδοση του υπολογιστή. Κατόπιν, ενεργοποιεί το κουμπί «*Next*».

Στο βήμα 7 (Εικόνα 28), εφόσον το επιθυμεί, επιλέγει «*Customize Hardware*» για να ρυθμίσει τους πόρους (CPU, RAM, hard disk, κάρτα δικτύου) του εικονικού υλικού και έπειτα, ενεργοποιεί το κουμπί «*Close*». Στην συνέχεια, ενεργοποιεί το κουμπί «*Finish*».

Στο βήμα 8 (Εικόνα 29), επιλέγει «*Power On*» (VM>Power>Power On), για να ξεκινήσει η διαδικασία εγκατάστασης του λειτουργικού συστήματος «*Kali Linux*». Επειδή, στο βήμα 3 δεν έχει επιλέξει το μέσο που βρίσκεται το λειτουργικό σύστημα, εμφανίζεται η οθόνη της Εικόνα 30. Στην συνέχεια, ακολουθεί την διαδρομή «*VM>Removable Devices>CD/DVD (IDE)>Settings*» (Εικόνα 31), για να επιλέξει το μέσο που βρίσκεται το λειτουργικό σύστημα. Στην Εικόνα 32 είτε επιλέγει «*Use physical drive*», εφόσον έχει τοποθετήσει στο «cd/dvd rom» του φυσικού υπολογιστή το DVD με το λειτουργικό σύστημα που θέλει να εγκαταστήσει, είτε «*Use ISO image file*», εφόσον το λειτουργικό σύστημα που θέλει να εγκαταστήσει βρίσκεται σε αρχείο της μορφής «*.iso*». Στην δεύτερη περίπτωση, ενεργοποιεί το κουμπί «*Browse*» (Εικόνα 33) και επιλέγει το μονοπάτι, στο οποίο βρίσκεται αποθηκευμένο το αρχείο της μορφή «*.iso*», με το λειτουργικό σύστημα «*Kali Linux*» (Εικόνα 34). Κατόπιν, ενεργοποιεί το κουμπί «*Άνοιγμα*» και αμέσως μετά, ενεργοποιεί το κουμπί «*OK*» (Εικόνα 35). Στην συνέχεια, ακολουθεί την διαδρομή «*VM>Removable Devices>CD/DVD (IDE)>Connect*» (Εικόνα 36), προκειμένου να συνδεθεί το «cd/dvd rom» με την εικονική μηχανή. Τέλος, ο χρήστης κάνει επανεκκίνηση (VM>Power>Reset) (Εικόνα 37). Μετά την επανεκκίνηση, φορτώνεται το λειτουργικό σύστημα «*Kali Linux*» στην εικονική μηχανή, ξεκινάει η εγκατάσταση του και εμφανίζεται το μενού εκκίνησης του (Εικόνα 38).

Στο βήμα 9 (Εικόνα 39), επιλέγει «*Graphical Install*», με το πλήκτρο «*κάτω βελάκι*», έτσι ώστε η εγκατάσταση να γίνει με την βοήθεια γραφικού περιβάλλοντος και κατόπιν πατάει το πλήκτρο «*Enter*».

Στο βήμα 10 (Εικόνα 40,Εικόνα 41), επιλέγει την γλώσσα που θα χρησιμοποιήσει για την διαδικασία εγκατάστασης του προγράμματος. Επίσης, η γλώσσα αυτή, θα είναι η προεπιλεγμένη γλώσσα του λειτουργικού συστήματος, μετά την εγκατάσταση του. Αμέσως μετά, ενεργοποιεί το κουμπί «*Continue*».

Στο βήμα 11 (Εικόνα 42), επιλέγει την τοποθεσία διαμονής του και ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 12 (Εικόνα 43), εφόσον το επιθυμεί, προσθέτει την γλώσσα εισόδου πληκτρολογίου της επιλογής του και ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 13 (Εικόνα 44), επιλέγει την συντόμευση που επιθυμεί, προκειμένου να επιτευχθεί η εναλλαγή μεταξύ τοπικής και Λατινικής διάταξης πληκτρολογίου και ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 14 (Εικόνα 45), εισάγει το όνομα που επιθυμεί να έχει ο εικονικός υπολογιστής και ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 15 (Εικόνα 46), εφόσον το επιθυμεί, εισάγει το όνομα του τομέα δικτύου (domain name) και ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 16 (Εικόνα 47), εισάγει κωδικό πρόσβασης για τον χρήστη «*root*» και ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 17 (Εικόνα 48), επιλέγει την μέθοδο διαμέρισης δίσκου που επιθυμεί και ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 18 (Εικόνα 49), επιλέγει τον δίσκο που θέλει να διαμερίσει και ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 19 (Εικόνα 50), επιλέγει το σχήμα διαμέρισης και ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 20 (Εικόνα 51), εφόσον συμφωνεί με την επισκόπηση των κατατμήσεων, επιλέγει «*Ολοκλήρωση της διαμέρισης και αποθήκευση των αλλαγών στον δίσκο*» και ενεργοποιεί το κουμπί «*Συνέχεια*», ειδάλλως προβαίνει στις τροποποιήσεις που επιθυμεί.

Στο βήμα 21 (Εικόνα 52), επιλέγει «*Ναι*», έτσι ώστε να διαμορφωθούν οι κατατμήσεις (root, swap) και να αποθηκευτούν αυτές οι αλλαγές στους δίσκους. Ύστερα, ενεργοποιεί το κουμπί «*Συνέχεια*».

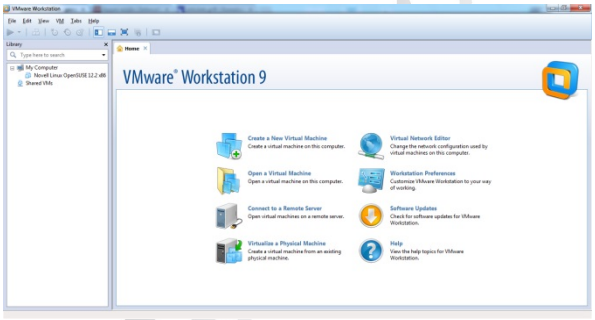
Στο βήμα 22 (Εικόνα 53), επιλέγει «*Ναι*», έτσι ώστε να χρησιμοποιηθεί ένας δικτυακός καθρέφτης, συμπληρωματικά ως προς το λογισμικό που περιλαμβάνεται στο DVD εγκατάστασης, προκειμένου να κάνει διαθέσιμες τυχόν νεώτερες εκδόσεις του. Στην συνέχεια, ενεργοποιεί το κουμπί «*Συνέχεια*». Αμέσως μετά, εφόσον είναι απαραίτητη η χρήση «*HTTP διαμεσολαβητή*» (HTTP proxy), για πρόσβαση στο διαδίκτυο εισάγει τις κατάλληλες ρυθμίσεις, ειδάλλως αφήνει το πεδίο κενό (Εικόνα 54). Κατόπιν, ενεργοποιεί το κουμπί «*Συνέχεια*».

Στο βήμα 23 (Εικόνα 55), επιλέγει «*Ναι*», έτσι ώστε να εγκατασταθεί ο «*boot loader*» «*Grub*» στο «*master boot record*» (βασική εγγραφή εκκίνησης) και ενεργοποιεί το κουμπί «*Συνέχεια*». Ο «boot loader» (φορτωτής εκκίνησης) είναι το πρώτο πρόγραμμα λογισμικού, που εκτελείται όταν ξεκινάει ένας υπολογιστής.

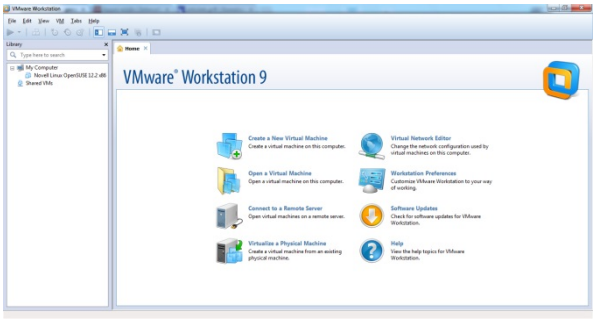
Στο βήμα 24 (Εικόνα 56), εφόσον η εγκατάσταση ολοκληρώθηκε με επιτυχία, ενεργοποιεί το κουμπί «*Συνέχεια*», για να γίνει επανεκκίνηση του εικονικού υπολογιστή.

Στο βήμα 25 (Εικόνα 57), εμφανίζεται ο «*boot loader*» «*Grub*» και ο χρήστης επιλέγει «*Debian GNU/Linux, with Linux 3.14-kali1-686-pae*». Αμέσως μετά, πατάει το πλήκτρο «*Enter*».

Στο τελευταίο βήμα (Εικόνα 58), για να εισέλθει στο λειτουργικό σύστημα «*Kali Linux*», πατάει το πλήκτρο «*Enter*» και εισάγει για Όνομα χρήστη την τιμή «root». Κατόπιν, πατάει ξανά το πλήκτρο «*Enter*» και εισάγει για κωδικό πρόσβασης τον κωδικό που έχει ορίσει για το χρήστη «*root*» στο βήμα 16 (Εικόνα 47).

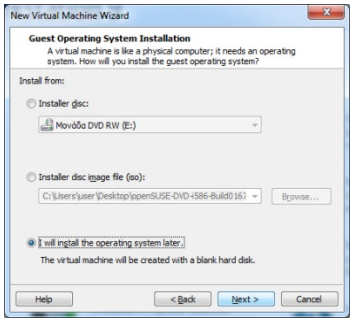


Εικόνα 21: VMware Workstation

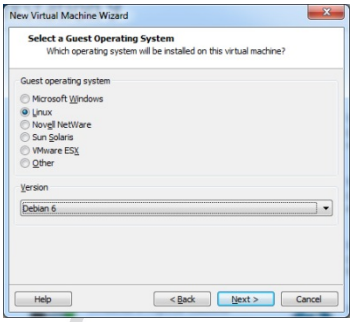


Εικόνα 22: Βήμα 1ο

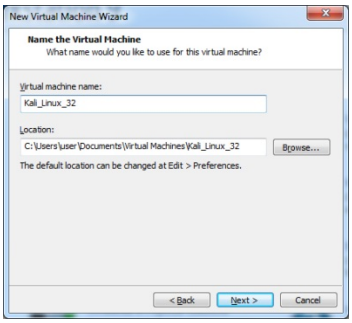
Εικόνα 23: Βήμα 2ο



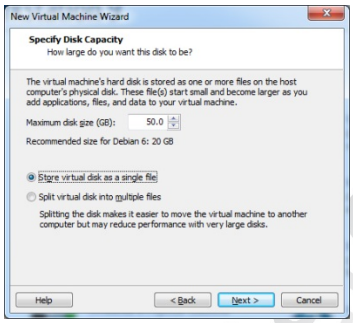
Εικόνα 24: Βήμα 3ο



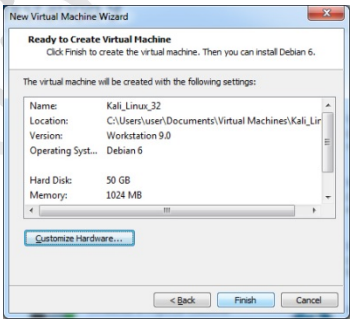
Εικόνα 25: Βήμα 4ο



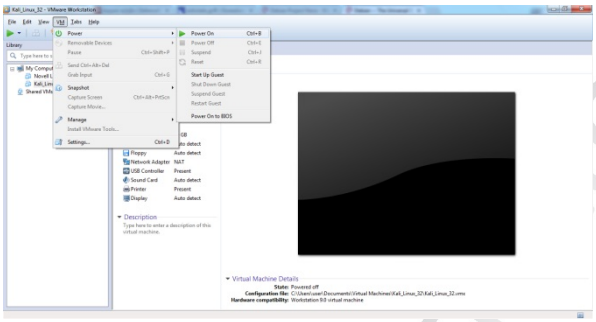
Εικόνα 26: Βήμα 5ο



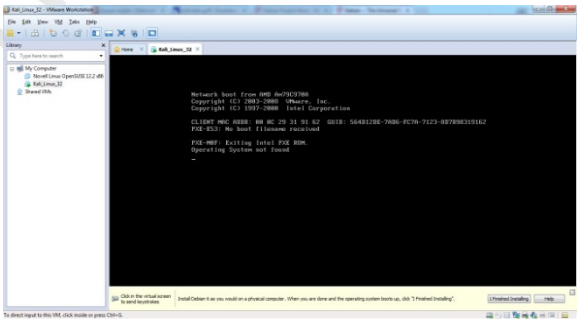
Εικόνα 27: Βήμα 6ο



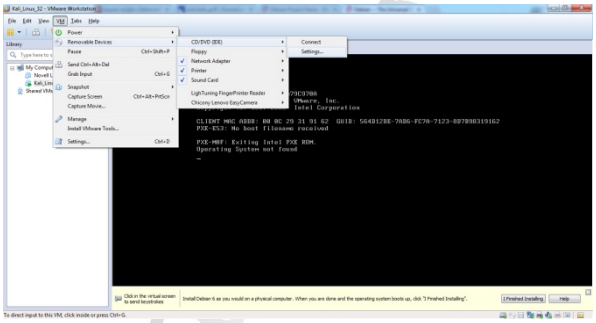
Εικόνα 28: Βήμα 7ο



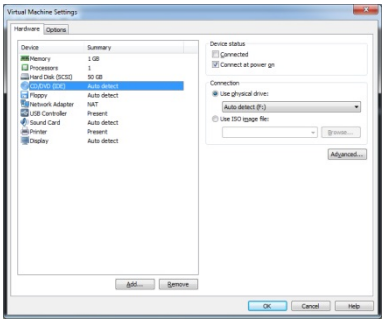
Εικόνα 29: Βήμα 8ο



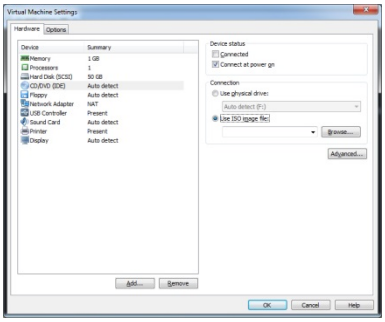
Εικόνα 30: Βήμα 8ο



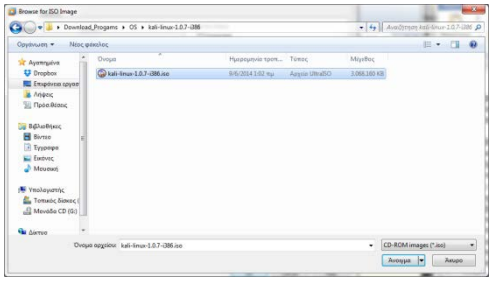
Εικόνα 31: Βήμα 8ο



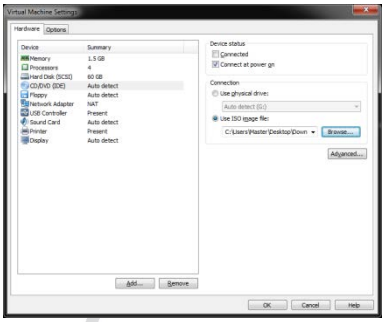
Εικόνα 32: Βήμα 8ο



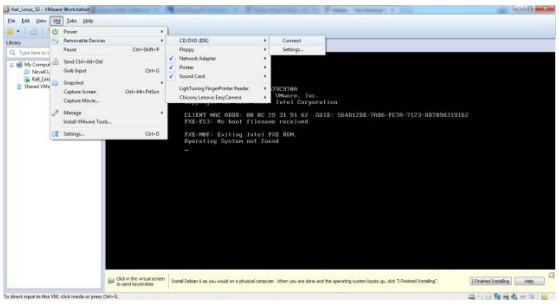
Εικόνα 33: Βήμα 8ο



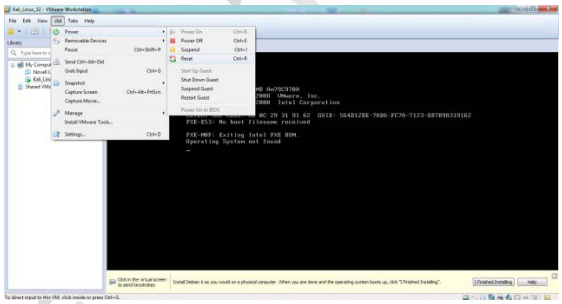
Εικόνα 34: Βήμα 8ο



Εικόνα 35: Βήμα 8ο



Εικόνα 36: Βήμα 8ο

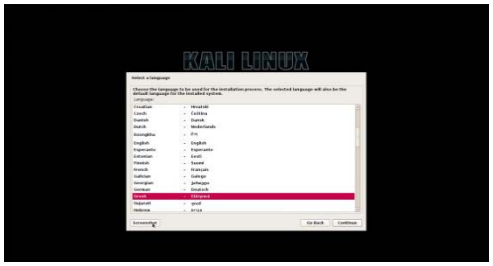


Εικόνα 37: Βήμα 8ο

Εικόνα 38: Μενού Εκκίνησης του Λειτουργικού Συστήματος «Kali Linux»

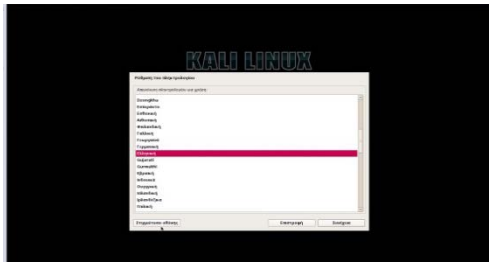
Εικόνα 39: Βήμα 9ο

Εικόνα 40: Βήμα 10ο



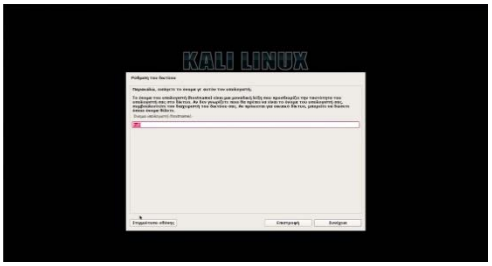
Εικόνα 41: Βήμα 10ο

Εικόνα 42: Βήμα 11ο



Εικόνα 43: Βήμα 12ο

Εικόνα 44: Βήμα 13ο

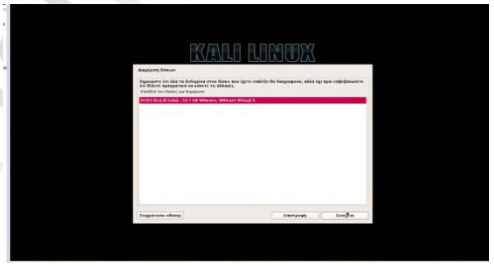


Εικόνα 45: Βήμα 14ο

Εικόνα 46: Βήμα 15ο

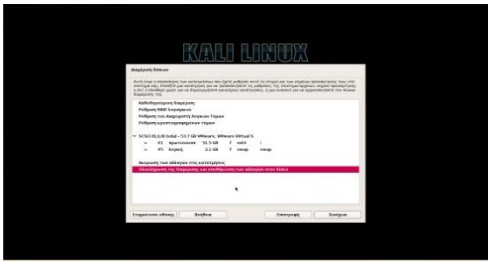
Εικόνα 47: Βήμα 16ο

Εικόνα 48: Βήμα 17ο



Εικόνα 49: Βήμα 18ο

Εικόνα 50: Βήμα 19ο



Εικόνα 51: Βήμα 20ο

Εικόνα 52: Βήμα 21ο

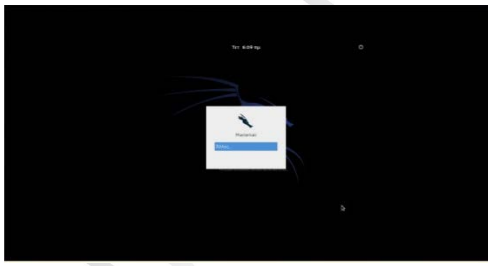
Εικόνα 53: Βήμα 22ο

Εικόνα 54: Βήμα 22ο

Εικόνα 55: Βήμα 23ο

Εικόνα 56: Βήμα 24ο

Εικόνα 57: Βήμα 25ο



Εικόνα 58: Βήμα 26ο

Σημείωση 1: Για να εγκαταστήσει ο οποιοσδήποτε χρήστης το λογισμικό «Adobe *flash player*» στο λειτουργικό σύστημα «*Kali Linux*», πηγαίνει στην ηλεκτρονική διεύθυνση «http://get.adobe.com/flashplayer/» και ελέγχει, το να είναι συμβατή η έκδοση του λογισμικού «Adobe *flash player*» με την αρχιτεκτονική (i386 ή amd64 ή armel ή armhf) και τον φυλλομετρητή (browser) του λειτουργικού συστήματος «*Kali Linux*», που έχει εγκατασταθεί στον εικονικό υπολογιστή. Αν δεν είναι συμβατή, τότε επιλέγει «*Different operating system or browser*» και προβαίνει στις κατάλληλες ρυθμίσεις. Στην συνέχεια, επιλέγει την τελευταία «*.tar.gz for other linux*» έκδοση. Κατόπιν, ενεργοποιεί το κουμπί «*Download* now». Στο νέο παράθυρο που εμφανίζεται, αποθηκεύει το αρχείο «*install_flash_player_11_linux.x.tar.gz*» (το «*x*» συμβολίζει την αρχιτεκτονική) στον φάκελο «*root*». Στην συνέχεια, ανοίγει ένα τερματικό και πληκτρολογεί την εντολή «*tar xzvf install_flash_player_11_linux.x.tar.gz*». Αμέσως μετά, πατάει το πλήκτρο «*Enter*», πληκτρολογεί την εντολή «*cp libflashplayer.so /usr/lib/mozilla/plugins/*» ή «*mv libflashplayer.so /usr/lib/mozilla/plugins/*» και πατάει ξανά το πλήκτρο «*Enter*». Τέλος, ο χρήστης προβαίνει στην επανεκκίνηση του εικονικού υπολογιστή.

Σημείωση 2: Προκειμένου να ενημερωθεί το λειτουργικό σύστημα «*Kali Linux*» και οι διάφορες εφαρμογές του, ο χρήστης ανοίγει ένα τερματικό και εκτελεί την εντολή «*apt-get update*», για να ανανεώσει την λίστα των διαθέσιμων πακέτων. Στην συνέχεια, εκτελεί την εντολή «*apt-get upgrade*», για να αναβαθμίσει τα όσα πακέτα μπορούν να

αναβαθμιστούν, χωρίς να γίνει εγκατάσταση ή αφαίρεση κάποιου άλλου πακέτου. Αμέσως μετά, εκτελεί την εντολή «*apt-get dist-upgrade*», για να αναβαθμίσει τα πακέτα εκείνα τα οποία απαιτούν την εγκατάσταση ή αφαίρεση κάποιου άλλου πακέτου, για να αναβαθμιστούν. Τέλος, ο χρήστης προβαίνει στην επανεκκίνηση του εικονικού υπολογιστή.

Σημείωση 3: Για να εγκαταστήσει ο οποιοσδήποτε χρήστης το λογισμικό «*VMware Tools*» στο λειτουργικό σύστημα «*Kali Linux*», στην αρχή ανοίγει ένα τερματικό και εκτελεί τις παρακάτω εντολές, προκειμένου να εγκαταστήσει κάποια πακέτα, που απαιτούνται από το πρόγραμμα εγκατάστασης του λογισμικού «*Vmware Tools*».

```
echo cups enabled >> /usr/sbin/update-rc.d
echo vmware-tools enabled >> /usr/sbin/update-rc.d
apt-get install gcc make linux-headers-$(uname -r)
ln-s /usr/src/linux-headers-$(uname -
r)/include/generated/uapi/linux/version.h /usr/src/linux-headers-$(uname-
r)/include/linux/
```

Στην συνέχεια, ακολουθεί την διαδρομή «*VM>Install Vmware Tools*» (Εικόνα 59), για να τοποθετήσει στο «cd/dvd rom» του εικονικού υπολογιστή το αρχείο της μορφής «.iso», που περιέχει το πρόγραμμα εγκατάστασης του λογισμικού «*VMware Tools*».

Εικόνα 59: Εγκατάσταση VMware Tools

Κατόπιν, ανοίγει ένα τερματικό και εκτελεί τις παρακάτω εντολές, προκειμένου να αντιγράψει το πρόγραμμα εγκατάστασης του λογισμικού «*VMware Tools*» στο φάκελο «/tmp/».

```
mkdir /mnt/vmware
mount /dev/cdrom /mnt/vmware/
cp –rf /mnt/vmware/VMwareTools*/tmp/
```

Αμέσως μετά, ο χρήστης, με τις παρακάτω εντολές εισέρχεται στο φάκελο «/tmp/», εξάγει το συμπιεσμένο αρχείο και εκτελεί το πρόγραμμα εγκατάστασης του λογισμικού «*VMware Tools*».

```
cd /tmp/
tar zxpf VMwareTools-*.tar.gz
cd vmware-tools-distrib/
./vmware-install.pl
```

Τέλος, ακολουθεί τις προτροπές, που εμφανίζονται κατά την διάρκεια της εγκατάστασης, έως ότου ολοκληρωθεί με επιτυχία η εγκατάσταση του λογισμικού «*VMware Tools*».

Επειδή, η κίνηση του ποντικιού μπορεί να είναι αργή και βραδυκίνητη, ο χρήστης εκτελεί τις παρακάτω εντολές, προκειμένου να εγκαταστήσει το πακέτο «*xserver-xorg-input-vmmouse*». Ύστερα, προβαίνει στην επανεκκίνηση του εικονικού υπολογιστή.

```
apt-get install xserver-xorg-input-vmmouse
reboot
```

Β. Εγκατάσταση της Εφαρμογής «OpenVAS» στο Λειτουργικό Σύστημα «Kali Linux»

Η εφαρμογή «OpenVAS» (Open Vulnerability Assessment System – Σύστημα Ανοιχτού Κώδικα Αξιολόγησης Ευπαθειών) είναι ένα σύνολο εργαλείων και υπηρεσιών (services), οι οποίες επικοινωνούν μεταξύ τους πάντα κρυπτογραφημένα, μέσω διαφόρων πρωτοκόλλων.

Η ανίχνευση ευπαθειών πραγματοποιείται με τη βοήθεια των λεγόμενων «*NVTs*» (Network Vulnerability Tests – Έλεγχοι Ευπάθειας Δικτύου), τα οποία ενημερώνονται τακτικά και στην ουσία υποβάλλουν τα υπό εξέταση συστήματα σε διάφορες δοκιμασίες κι ελέγχους, με στόχο την αποκάλυψη αδυναμιών σε ρυθμίσεις, σε υπηρεσίες κ.ο.κ.

Στην περίπτωση που ο οποιοσδήποτε χρήστης επιθυμεί να χρησιμοποιήσει την εφαρμογή «OpenVAS», συνδέεται σε αυτήν μέσω ενός φυλλομετρητή και ξεκινά ελέγχους ή/και παίρνει αναφορές.

Στην συνέχεια, παρατίθενται οι υπηρεσίες που αποτελούν το «OpenVAS», μερικά βασικά του εργαλεία και διάφοροι πελάτες (clients) του.

- **OpenVAS Scanner** (openvassd). Η υπηρεσία αυτή ξεκινάει με την συλλογή «NVTs» και στην συνέχεια, ψάχνει για πάσης φύσεως αδυναμίες στα μηχανήματα που της ζητείται να ελέγξει. Η επικοινωνία με τον «OpenVAS Scanner» γίνεται μέσω του πρωτοκόλλου «*OpenVAS Transfer Protocol*» (OTP) και είναι κρυπτογραφημένη κατά «*SSL*». Ο «OpenVAS Scanner», εξ ορισμού, ακούει για αιτήσεις πελατών από την θύρα (port) 9391.

- **OpenVAS Manager** (*openvasmd*). Τα αποτελέσματα του «OpenVAS Scanner» τα παίρνει και τα διαχειρίζεται ο «OpenVAS Manager», ο οποίος τα αποθηκεύει σε μια σχεσιακή βάση δεδομένων της «SQLite». Στην ίδια βάση αποθηκεύονται και οι ρυθμίσεις των χρηστών του συστήματος. Ο «OpenVAS Manager» είναι αυτός που μιλά απευθείας με τον «OpenVAS Scanner», μέσω «OTP», και είναι σε θέση να ζητά την εκτέλεση εργασιών ανίχνευσης, καθώς και τον τερματισμό, την παύση ή/και την επανεκκίνησή τους.

  Επιπλέον, ο «OpenVAS Manager» μέσω του πρωτοκόλλου «*OpenVAS Manager Protocol*» (OMP), επικοινωνεί με διάφορους πελάτες (clients) όπως ο «Greenbone Security Assistant» και το «omp» για τη γραμμή εντολών. Η επικοινωνία είναι κρυπτογραφημένη κατά «*SSL*».

  Ο «OpenVAS Manager», εξ ορισμού, ακούει για αιτήσεις πελατών από την θύρα (port) 9390.

- **OpenVAS Adminitrator** (*openvasad*). Ο «OpenVAS Administrator» διαχειρίζεται τους χρήστες καθώς και τις τροφοδοτήσεις (feeds) που δέχεται η εφαρμογή «OpenVAS». Η επικοινωνία με τον «OpenVAS Administrator» γίνεται μέσω του πρωτοκόλλου «*OpenVAS Administrator Protocol*» (OAP) και είναι κρυπτογραφημένη κατά «*SSL*».

  Τις πληροφορίες για τους χρήστες αλλά και για τα «feeds», ο Administrator τις αποθηκεύει στην ίδια σχεσιακή βάση δεδομένων «SQLite» που χρησιμοποιεί κι ο «OpenVAS Manager».

  Ο «OpenVAS Administrator», εξ ορισμού, ακούει για αιτήσεις πελατών από την θύρα (port) 9393.

- **Greenbone Security Assistant** (*GSA, gsad*). Ο «GSA» είναι ένας «OMP client», που παρέχει στο χρήστη της εφαρμογής «OpenVAS» ένα εύχρηστο «web panel».

Ο χρήστης έρχεται σε επαφή με το εύχρηστο «web panel» του «GSA», μέσω ενός φυλλομετρητή. Το «web panel» για να τρέξει χρησιμοποιεί ένα μικρό «web server» (micro-httpd), το οποίο είναι ενσωματωμένο στον «GSA». Η μετάφραση των απαντήσεων του «OMP» σε «HTML» γίνεται με χρήστη «XSLT».

Ο «GSA», εξ ορισμού, ακούει για αιτήσεις πελατών από την θύρα (port) 9392.

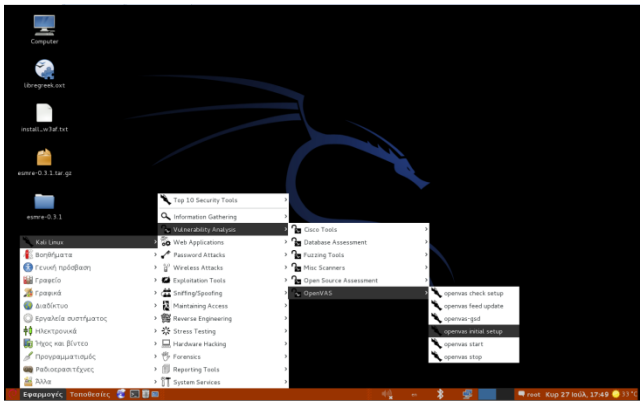
Για να εγκαταστήσει ο οποιοσδήποτε χρήστης την εφαρμογή «OpenVAS» στο λειτουργικό σύστημα «*Kali Linux*», ακολουθεί τα επόμενα βήματα.

Στο βήμα 1, συνδέεται στο λειτουργικό σύστημα «*Kali Linux*» ως χρήστης «*root*», ακολουθεί την διαδρομή «*Applications> Kali Linux> Vulnerability Analysis> OpenVAS*» και ενεργοποιεί την επιλογή «*openvas initial setup*» (Εικόνα 60). Στην συνέχεια, εκτελείται το «script» της αρχικής εγκατάστασης του «OpenVAS» (Εικόνα 61). Το «script» αυτό, μεταξύ άλλων εργασιών κατεβάζει ένα αρχείο με όλα τα «NVTs», φτιάχνει πιστοποιητικά για την Αρχή Πιστοποίησης, τον «OpenVAS Scanner» και τους «clients», ενεργοποιεί την υπηρεσία openvassd (η οποία φορτώνει τα plugins, δηλαδή τα NVTs), δημιουργεί έναν χρήστη για το «OpenVAS» με όνομα «admin» και δικαιώματα διαχειριστή, ενώ ζητά από το χρήστη να ορίσει ένα κωδικό πρόσβασης γι' αυτόν. Κατόπιν, ο χρήστης ορίζει ένα κωδικό πρόσβασης για τον χρήστη «admin» του «OpenVAS» και πατάει το πλήκτρο «*Enter*». Αμέσως μετά (Εικόνα 62), ολοκληρώνεται η εκτέλεση του «script» της αρχικής εγκατάστασης του «OpenVAS».

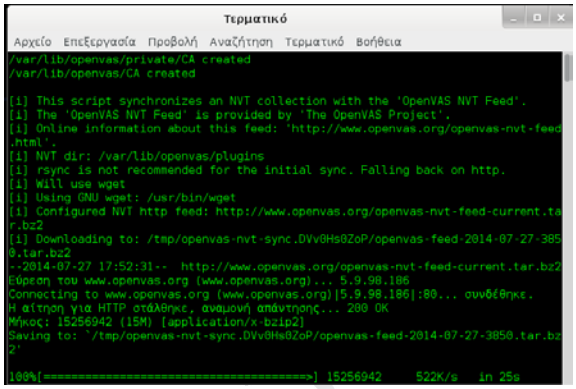
Στο βήμα 2, ανοίγει ένα τερματικό και εκτελεί την εντολή «*openvas-check-setup*», προκειμένου να ελέγξει την εγκατάσταση του «OpenVAS» και να πληροφορηθεί για τα όποια προβλήματα έχουν προκύψει. Μετά την εκτέλεση της παραπάνω εντολής, ο χρήστης πληροφορείται με μήνυμα λάθους, για την βάση «SCAP» που απουσιάζει (Εικόνα 63). Στην συνέχεια, ακολουθεί την διαδρομή «*Applications> Kali Linux> Vulnerability Analysis> OpenVAS*» και ενεργοποιεί την επιλογή «*openvas feed update*». Κατόπιν, απαντάει καταφατικά στην ερώτηση περί «migration» (Εικόνα 64) και περιμένει μέχρι να τελειώσει το «script» τις εργασίες που τρέχει.

Στο βήμα 3, ανοίγει ένα τερματικό και εκτελεί ξανά την εντολή «*openvas-check-setup*», προκειμένου να ελέγξει για άλλη μια φορά την εγκατάσταση του «OpenVAS». Το «script» που τρέχει ενημερώνει το χρήστη ότι η εγκατάσταση του «OpenVAS» είναι εντάξει και τον προειδοποιεί για κάποια πακέτα που απουσιάζουν. Στην συνέχεια, ο χρήστης για να τα εγκαταστήσει εκτελεί την εντολή «*apt-get -y install rpm alien nsis*» σε ένα τερματικό.

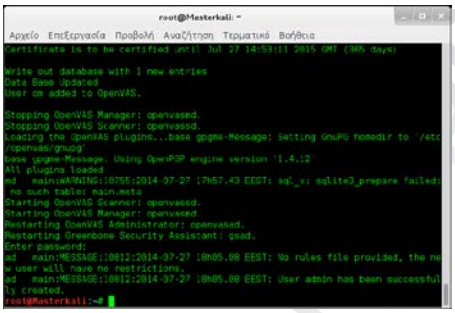
Στο βήμα 4, ανοίγει το φυλλομετρητή «Iceweasel» και στο «url» πληκτρολογεί την διεύθυνση «*https://127.0.0.1:9392*». Μετά την προειδοποίηση περί μη έμπιστης σύνδεσης, ο χρήστης κάνει διαδοχικά κλικ στα «*I Understand the Risks*», «*Add Exception*» και «*Confirm Security Exception*». Στη σελίδα «login.html» (Εικόνα 65) του «Greenbone Security Assistant», ο χρήστης εισάγει για «*username*» την τιμή «admin» και για «*password*» το κωδικό πρόσβασης που έχει ορίσει στο βήμα 1 και εισέρχεται στην αρχική σελίδα της εφαρμογής «OpenVAS».



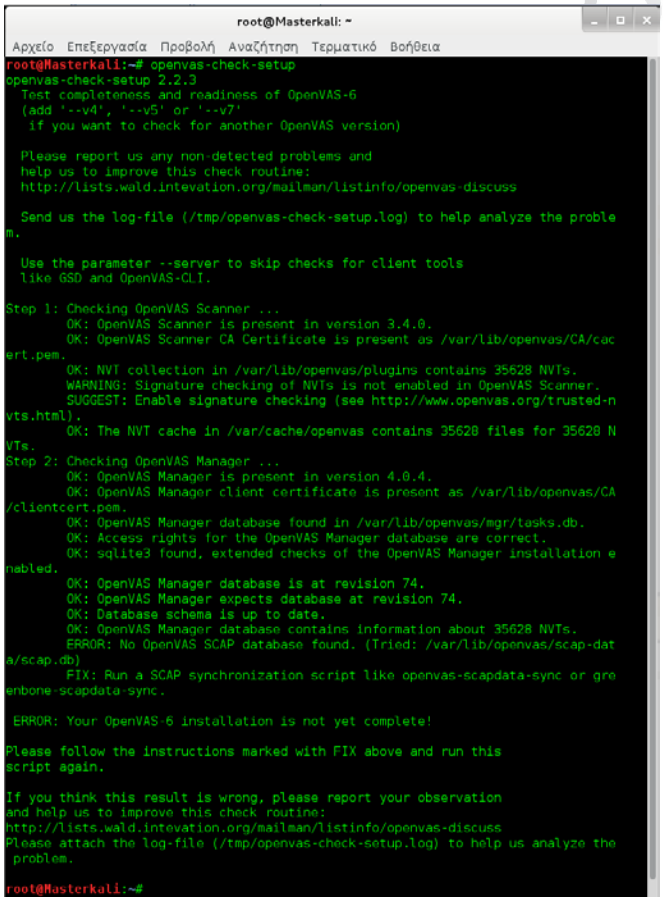
Εικόνα 60: Επιλογή Αρχικής Εγκατάστασης του OpenVAS



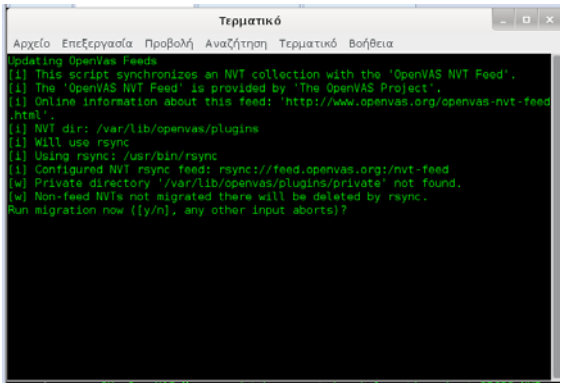
Εικόνα 61: Εκτέλεση του script της Αρχικής Εγκατάστασης του OpenVAS



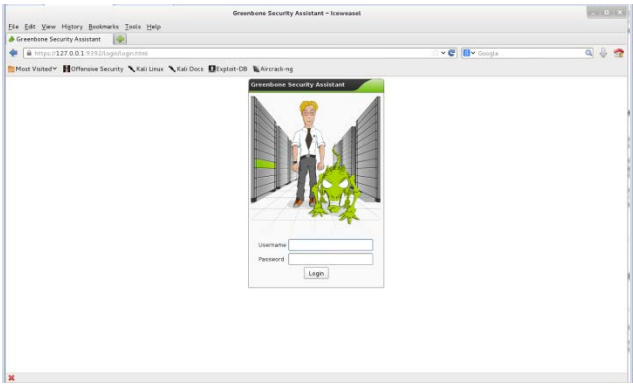
Εικόνα 62: Ολοκλήρωση Εκτέλεσης του script



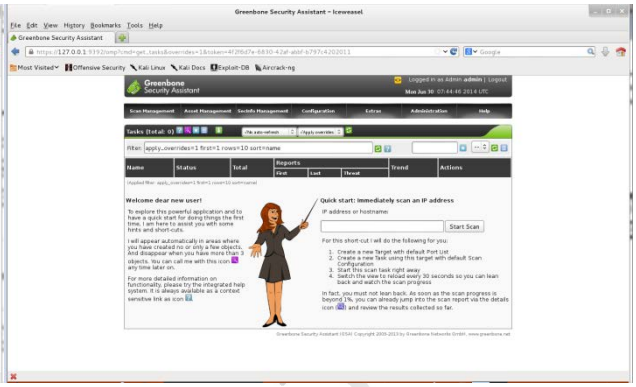
Εικόνα 63: Έλεγχος της Εγκατάστασης του OpenVAS



Εικόνα 64: Run Migration



Εικόνα 65: OpenVAS: login.html



Εικόνα 66: Αρχική Σελίδα του OpenVAS

Σημείωση: Ο χρήστης δημιουργεί στην «Επιφάνεια Εργασίας» η οπουδήποτε αλλού επιθυμεί, το «script» «*OpenVAS.sh*». Στην συνέχεια, ανοίγει ένα τερματικό και εκτελεί την εντολή «*chmod 700 ./Desktop/OpenVAS.sh*», για να ορίσει τα κατάλληλα «permissions» στο αρχείο «*OpenVAS.sh*».

Μετά από επανεκκίνηση του λειτουργικού συστήματος «*Kali Linux*», οι σχετικές με το «OpenVAS» υπηρεσίες δεν λειτουργούν. Προκειμένου ο χρήστης να τις ενεργοποιήσει με τη σωστή σειρά αλλά και να ενημερώνεται αυτόματα η συλλογή με τα «NVTs», ανοίγει ένα τερματικό και εκτελεί την εντολή «*./Desktop/OpenVAS.sh*».

Ακολουθεί ο κώδικας του αρχείου «*OpenVAS.sh*».

```
#!/bin/bash
echo
echo Synchronizing local NVT collection, please be patient...
echo
================================================================================
openvas-nvt-sync
echo
echo Starting OpenVAS Scanner service...
echo
================================================================================
openvassd
echo
echo Synchronizing local SCAP database...
echo
================================================================================
openvas-scapdata-sync
echo
echo Synchronizing local CERT database...
echo
================================================================================
openvas-certdata-sync
```

```
echo
echo Rebuilding OpenVAS Manager database...
echo
================================================================================
openvasmd --rebuild

echo
echo Backing up OpenVAS Manager database...
echo
================================================================================
openvasmd --backup

echo
echo Starting OpenVAS Manager service...
echo
================================================================================
openvasmd -p 9390 -a 127.0.0.1

echo
echo Starting OpenVAS Administrator service...
echo
================================================================================
openvasad -p 9393 -a 127.0.0.1

echo
echo Starting Greenbone Security Assistant service...
echo
================================================================================
gsad -p 9392 --listen=127.0.0.1

echo
echo If all went well, you may now browse to https://127.0.0.1:9392
echo and start enjoying OpenVAS via the GSA web interface
echo
================================================================================
```

Γ. Εγκατάσταση του Λειτουργικού Συστήματος «CentOS» στο Προηγμένο Λογισμικό Εικονικής Μηχανής VMware Workstation σε Περιβάλλον Windows

Για να κατεβάσει ο οποιοσδήποτε χρήστης το λειτουργικό σύστημα «*CentOS*», πηγαίνει στην ηλεκτρονική διεύθυνση «http://www.centos.org/» και κατεβάζει την τελευταία «*netinstall*» έκδοση του λειτουργικού, σύμφωνα με την αρχιτεκτονική του υπολογιστή (i386 ή amd64), στον οποίο πρόκειται να εγκατασταθεί. Το αρχείο που κατεβαίνει είναι της μορφής «.iso» και ο χρήστης είτε το «καίει» σε ένα DVD είτε το αφήνει ως έχει. Κατόπιν, ανοίγει το πρόγραμμα «*VMware Workstation*» και ακολουθεί τα επόμενα βήματα.

Από το βήμα 1 (Εικόνα 67) έως το βήμα 8 (Εικόνα 80), ακολουθεί την ίδια διαδικασία, που εφήρμοσε κατά την εγκατάσταση του λειτουργικού συστήματος «Kali Linux» στο προηγμένο λογισμικό εικονικής μηχανής «VMware Workstation» σε περιβάλλον «Windows», στα αντίστοιχα βήματα, προσέχοντας στο βήμα 4 (Εικόνα 70), στη περιοχή «*Version*», να επιλέξει είτε «*CentOS*» είτε «*CentOS 64-bit*» ανάλογα με την έκδοση (32bit ή 64bit) του λειτουργικού συστήματος που θέλει να εγκαταστήσει.

Στο βήμα 9 (Εικόνα 81)», με το πλήκτρο «*κάτω βελάκι*», επιλέγει «*Install or upgrade an existing system*», έτσι ώστε να ξεκινήσει η εγκατάσταση του λειτουργικού συστήματος «*CentOS 6.5*» και κατόπιν, πατάει το πλήκτρο «*Enter*».

Στο βήμα 10 (Εικόνα 82), με το πλήκτρο «*δεξί βελάκι*», επιλέγει «*Skip*», έτσι ώστε να ξεκινήσει η εγκατάσταση του λειτουργικού συστήματος «CentOS 6.5», χωρίς να γίνει έλεγχος ορθής λειτουργίας του εποπτικού μέσου, στο οποίο είναι εγγεγραμμένο το πρόγραμμα εγκατάστασης του λειτουργικού, εξαιτίας του ότι, η εγκατάσταση θα γίνει μέσω διαδικτύου. Ύστερα, πατάει το πλήκτρο «*Enter*».

Στο βήμα 11 (Εικόνα 83), με τα πλήκτρα «*πάνω ή κάτω βελάκι*», επιλέγει την γλώσσα που θα χρησιμοποιήσει για την διαδικασία εγκατάστασης του προγράμματος. Επίσης, η γλώσσα αυτή, θα είναι η προεπιλεγμένη γλώσσα του λειτουργικού συστήματος, μετά την εγκατάσταση του. Αμέσως μετά, με την βοήθεια του πλήκτρου «Tab», ενεργοποιεί το κουμπί «*OK*».

Στο βήμα 12 (Εικόνα 84), με τα πλήκτρα «*πάνω ή κάτω βελάκι*», επιλέγει την γλώσσα εισόδου πληκτρολογίου που επιθυμεί και με την βοήθεια του πλήκτρου «Tab», ενεργοποιεί το κουμπί «*OK*».

Στο βήμα 13 (Εικόνα 85), με τα πλήκτρα «*πάνω ή κάτω βελάκι*», επιλέγει την μέθοδο εγκατάστασης του λειτουργικού συστήματος (`url`) και κατόπιν, με την βοήθεια του πλήκτρου «Tab», ενεργοποιεί το κουμπί «*OK*».

Στο βήμα 14 (Εικόνα 86), διαμορφώνει τις «IP» διευθύνσεις και ύστερα, με την βοήθεια του πλήκτρου «Tab» ενεργοποιεί το κουμπί «*OK*».

Στο βήμα 15 (Εικόνα 87, Εικόνα 88), εισάγει την πλήρη ηλεκτρονική διεύθυνση, που περιέχει την «εικόνα» εγκατάστασης του λειτουργικού συστήματος «CentOS 6.5» και αμέσως μετά, ενεργοποιεί το κουμπί «*OK*» Η ηλεκτρονική διεύθυνση για την 32bit έκδοση του λειτουργικού είναι η «http://ftp.ntua.gr/pub/linux/centos/6.5/os/i386/images/install.img», ενώ για την 64bit είναι η «http://ftp.ntua.gr/pub/linux/centos/6.5/os/x86_64/images/install.img».

Στο βήμα 16 (Εικόνα 89), περιμένει να τελειώσει η ανάκτηση της «εικόνας» εγκατάστασης του λειτουργικού συστήματος «CentOS 6.5».

Στο βήμα 17 (Εικόνα 90), στο γραφικό περιβάλλον εγκατάστασης του λειτουργικού συστήματος, ενεργοποιεί το κουμπί «*Επόμενο*».

Στο βήμα 18 (Εικόνα 91), επιλέγει τον τύπο των αποθηκευτικών συσκευών, στις οποίες θα εγκατασταθεί το λειτουργικό σύστημα και ενεργοποιεί το κουμπί «*Επόμενο*». Στην συνέχεια, στο προειδοποιητικό μήνυμα «Προειδοποίηση συσκευής αποθήκευσης», επιλέγει «*Yes, discard any data*» (Εικόνα 92).

Στο βήμα 19 (Εικόνα 93), εισάγει το όνομα συστήματος που επιθυμεί να έχει ο εικονικός υπολογιστής και ενεργοποιεί το κουμπί «*Επόμενο*».

Στο βήμα 20 (Εικόνα 94), επιλέγει την τοποθεσία διαμονής του και ενεργοποιεί το κουμπί «*Επόμενο*».

Στο βήμα 21 (Εικόνα 95), εισάγει κωδικό πρόσβασης για τον χρήστη «*root*» και ενεργοποιεί το κουμπί «*Επόμενο*».

Στο βήμα 22 (Εικόνα 96), επιλέγει τον τύπο εγκατάστασης που επιθυμεί, τσεκάρει το «checkbox» «*Επισκόπηση και τροποποίηση διάταξης κατάτμησης*» και ενεργοποιεί το κουμπί «*Επόμενο*». Αμέσως μετά, εφόσον συμφωνεί με την προτεινόμενη κατάτμηση του εικονικού δίσκου ενεργοποιεί το κουμπί «*Επόμενο*», ειδάλλως επιλέγει τον τόμο που επιθυμεί να τροποποιήσει, ενεργοποιεί το κουμπί «*Επεξεργασία*» ή το κουμπί «*Διαγραφή*», ανάλογα με την ενέργεια που θέλει να εκτελέσει, προβαίνει στις σχετικές ενέργειες και στην συνέχεια ενεργοποιεί το κουμπί «*Επόμενο*» (Εικόνα 97). Έπειτα, στο προειδοποιητικό μήνυμα «Προειδοποίηση διαμόρφωσης», επιλέγει «*Διαμόρφωση*» (Εικόνα 98), προκειμένου να διαμορφωθούν οι κατατμήσεις (root, home, swap) του εικονικού δίσκου, στον οποίον θα εγκατασταθεί το λειτουργικό σύστημα. Στην συνέχεια, στο προειδοποιητικό μήνυμα «Εγγραφή ρύθμισης δίσκων στο δίσκο», επιλέγει «*Εγγραφή αλλαγών στο δίσκο*» (Εικόνα 99) και ύστερα, πραγματοποιείται η διαμόρφωση (Εικόνα 100).

Στο βήμα 23 (Εικόνα 101), ενεργοποιεί το κουμπί «*Επόμενο*», προκειμένου να εγκατασταθεί ο «*boot loader*» στο «*/dev/sda*».

Στο βήμα 24 (Εικόνα 102), επιλέγει το πακέτο του λειτουργικού συστήματος «CentOS 6.5» που επιθυμεί να εγκαταστήσει, τσεκάρει το «radiobutton» «Προσαρμογή τώρα», για να προσαρμόσει περαιτέρω το πακέτο εγκατάστασης (Εικόνα 103) και ύστερα, ενεργοποιεί το κουμπί «*Επόμενο*».

Στο βήμα 25 (Εικόνα 104), γίνεται εκκίνηση της εγκατάστασης.

Στο βήμα 26 (Εικόνα 105), εφόσον η εγκατάσταση ολοκληρώθηκε με επιτυχία, ενεργοποιεί το κουμπί «*Επανεκκίνηση*».

Στο βήμα 27 (Εικόνα 106), ενεργοποιεί το κουμπί «*Μπροστά*».

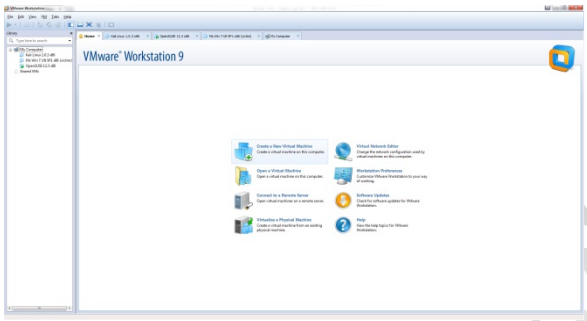
Στο βήμα 28 (Εικόνα 107), τσεκάρει το «radiobutton» «*Yes, I agree to the License Agreement*», για να αποδεχθεί τους όρους της άδειας χρήσης και ενεργοποιεί το κουμπί «*Μπροστά*».

Στο βήμα 29 (Εικόνα 108), δημιουργεί έναν νέο χρήστη και εφόσον εισαγάγει το όνομα και τον κωδικό πρόσβασης, ενεργοποιεί το κουμπί «*Μπροστά*».

Στο βήμα 30 (Εικόνα 109), ρυθμίζει την ημερομηνία και την ώρα του συστήματος και αμέσως μετά, ενεργοποιεί το κουμπί «*Τέλος*».

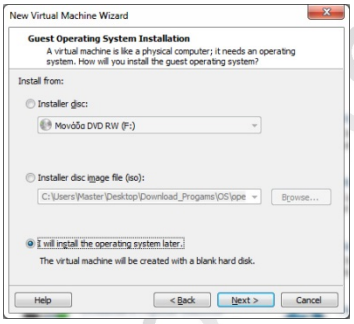
Στο βήμα 31 (Εικόνα 110), για να εισέλθει στο λειτουργικό σύστημα «CentOS 6.5», είτε επιλέγει το νέο χρήστη που δημιούργησε στο βήμα 29 (Εικόνα 108), πατάει το πλήκτρο

«*Enter*» και εισάγει για κωδικό πρόσβασης τον κωδικό που έχει ορίσει για το χρήστη αυτόν, είτε επιλέγει «Άλλος», πατάει το πλήκτρο «*Enter*», εισάγει για Όνομα χρήστη την τιμή «root», πατάει ξανά το πλήκτρο «*Enter*» και εισάγει για κωδικό πρόσβασης τον κωδικό που έχει ορίσει για το χρήστη «*root*» στο βήμα 21 (Εικόνα 95).

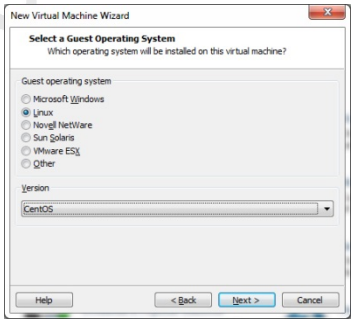


Εικόνα 67: Βήμα 1ο

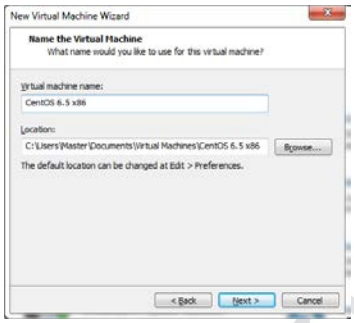
Εικόνα 68: Βήμα 2ο



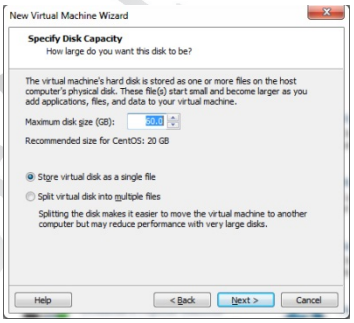
Εικόνα 69: Βήμα 3ο



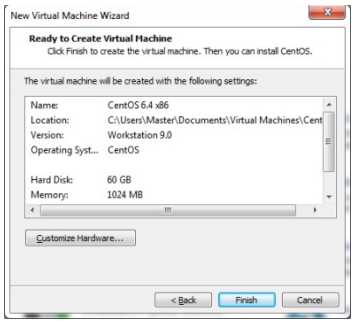
Εικόνα 70: Βήμα 4ο



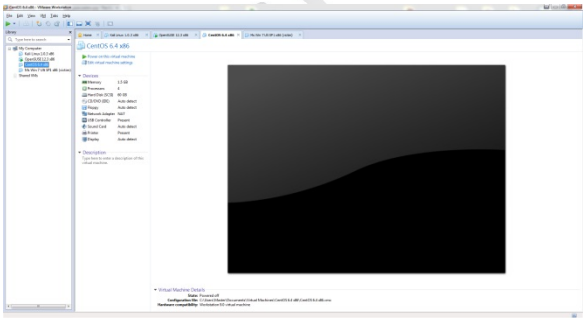
Εικόνα 71: Βήμα 5ο



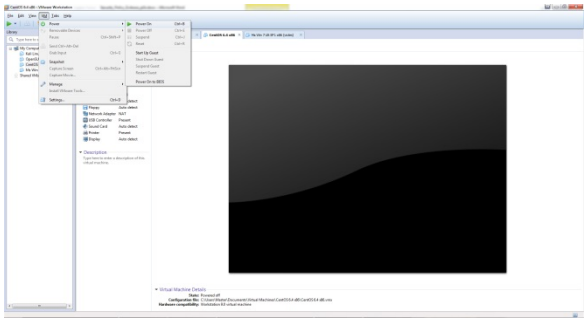
Εικόνα 72: Βήμα 6ο



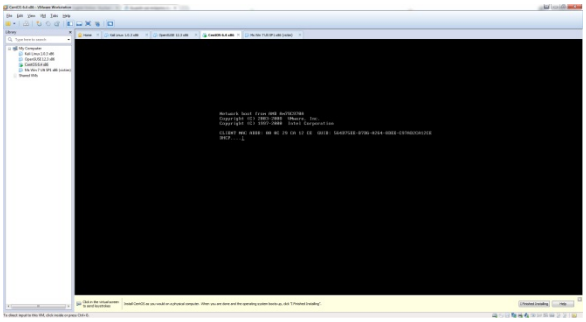
Εικόνα 73: Βήμα 7ο



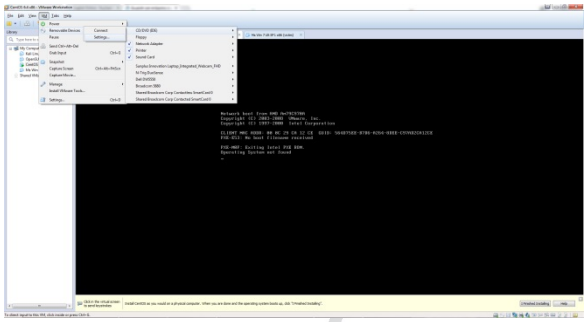
Εικόνα 74: Βήμα 8ο



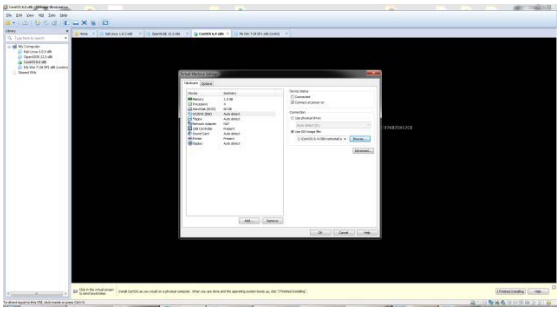
Εικόνα 75: Βήμα 8ο



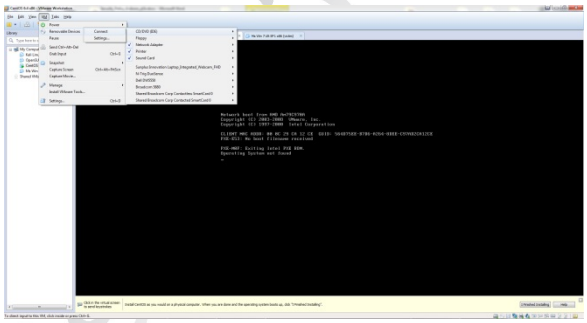
Εικόνα 76: Βήμα 8ο



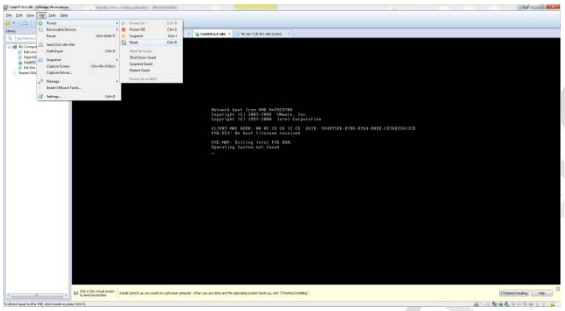
Εικόνα 77: Βήμα 8ο



Εικόνα 78: Βήμα 8ο



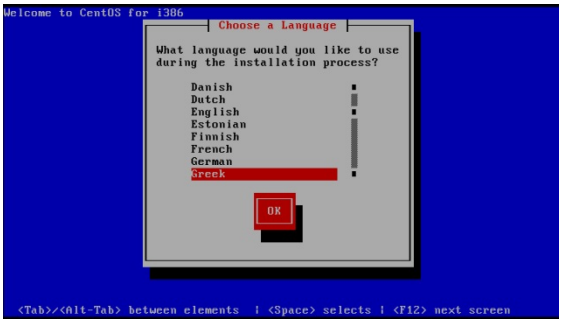
Εικόνα 79: Βήμα 8ο



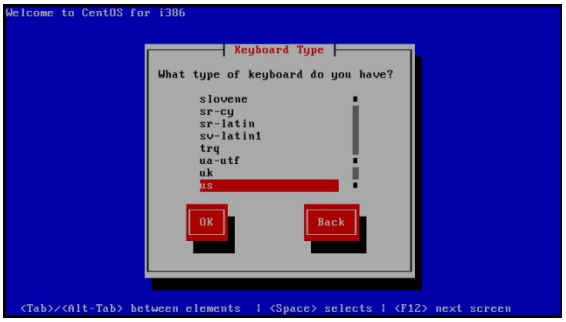
Εικόνα 80: Βήμα 8ο

Εικόνα 81: Βήμα 9ο

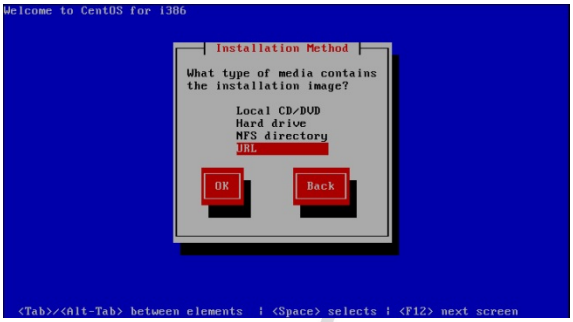
Εικόνα 82: Βήμα 10ο



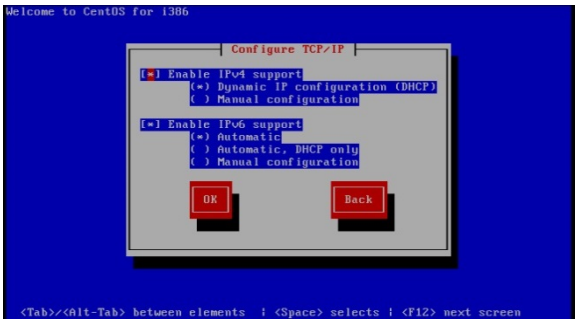
Εικόνα 83: Βήμα 11ο



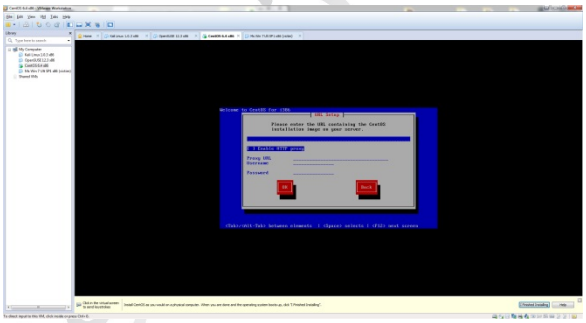
Εικόνα 84: Βήμα 12ο



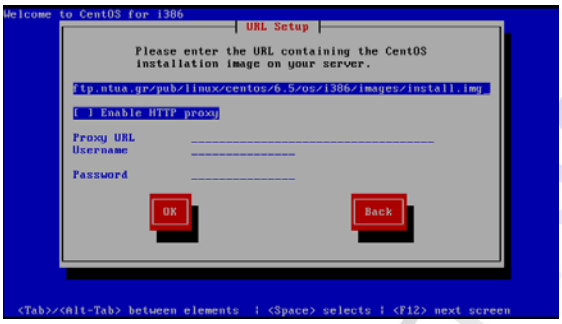
Εικόνα 85: Βήμα 13ο



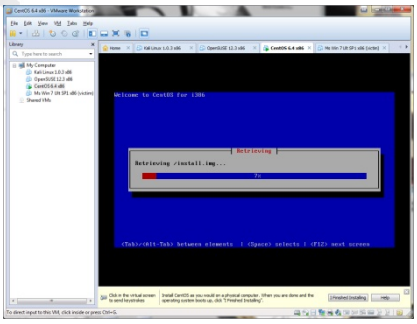
Εικόνα 86: Βήμα 14ο



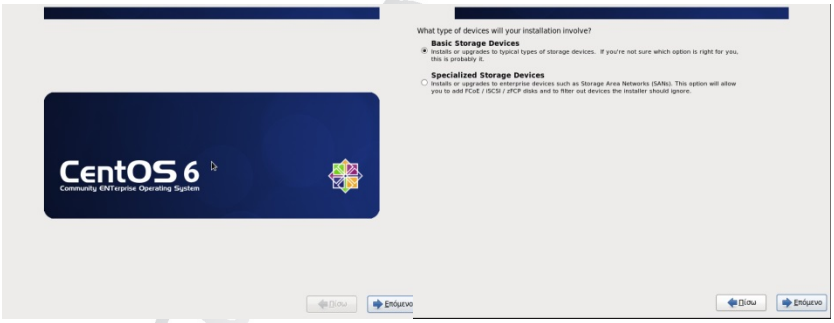
Εικόνα 87: Βήμα 15ο



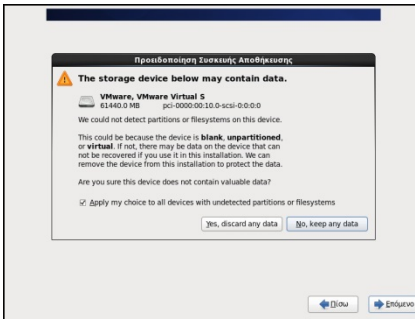
Εικόνα 88: Βήμα 15ο



Εικόνα 89: Βήμα 16ο

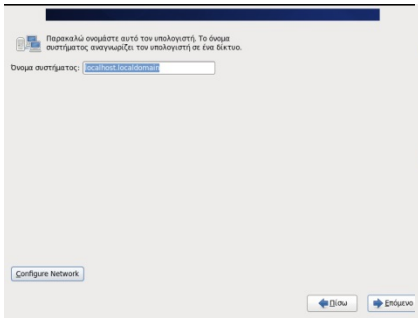


Εικόνα 90: Βήμα 17ο

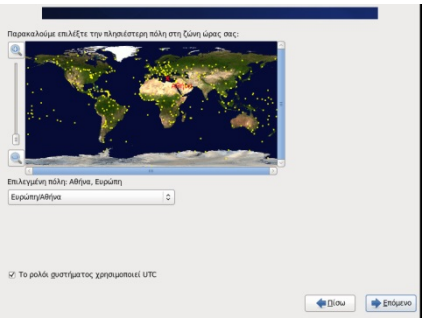


Εικόνα 91: Βήμα 18ο

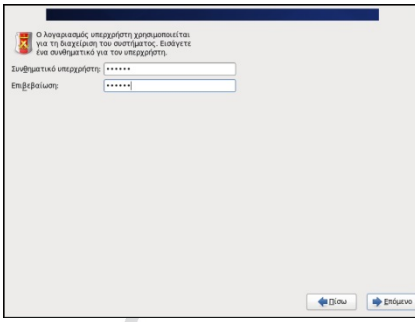
Εικόνα 92: Βήμα 18ο



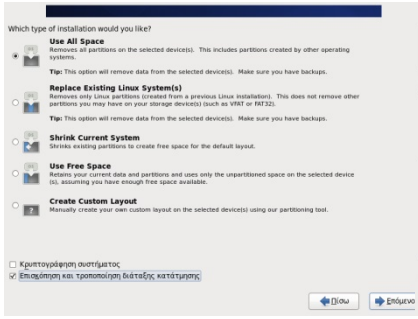
Εικόνα 93: Βήμα 19ο



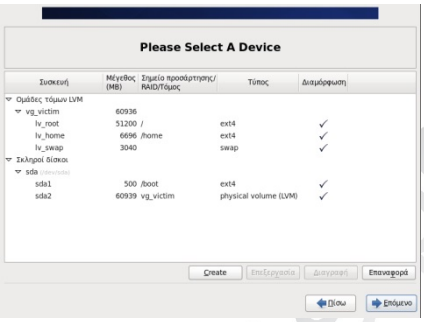
Εικόνα 94: Βήμα 20ο



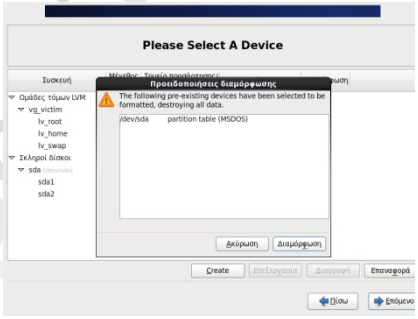
Εικόνα 95: Βήμα 21ο



Εικόνα 96: Βήμα 22ο

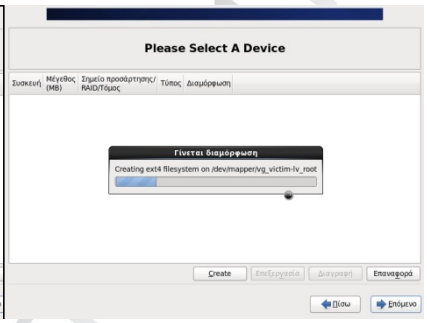


Εικόνα 97: Βήμα 22ο

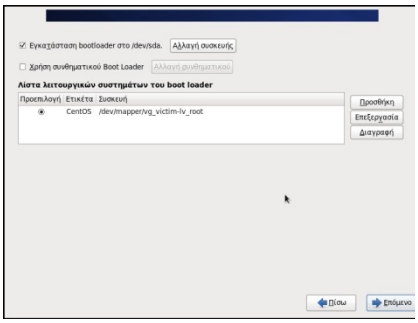


Εικόνα 98: Βήμα 22ο

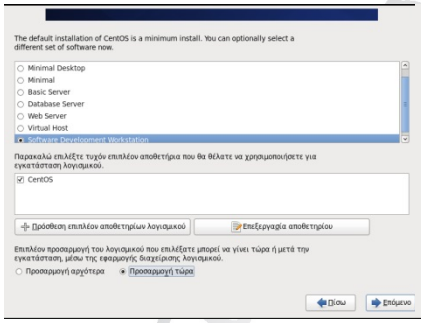
Εικόνα 99: Βήμα 22ο



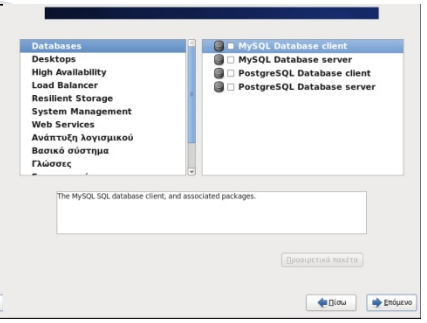
Εικόνα 100: Βήμα 22ο



Εικόνα 101: Βήμα 23ο

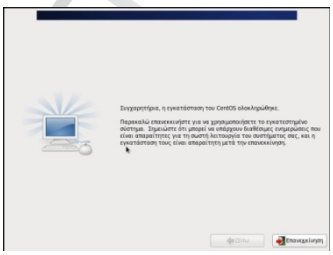


Εικόνα 102: Βήμα 24ο

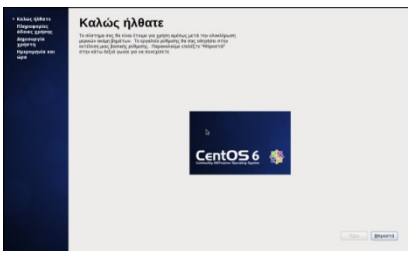


Εικόνα 103: Βήμα 24ο

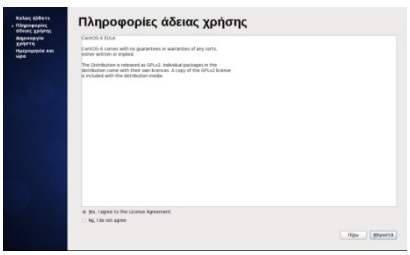
Εικόνα 104: Βήμα 25ο



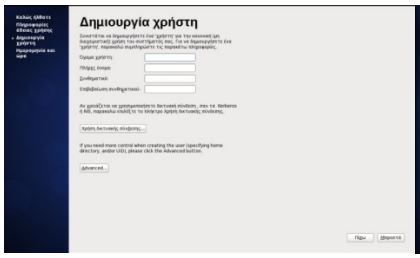
Εικόνα 105: Βήμα 26ο



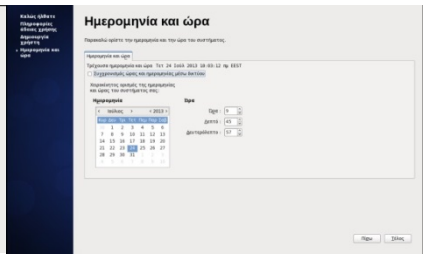
Εικόνα 106: Βήμα 27ο



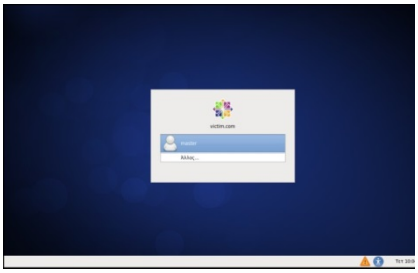
Εικόνα 107: Βήμα 28ο



Εικόνα 108: Βήμα 29ο



Εικόνα 109: Βήμα 30ο



Εικόνα 110: Βήμα 31ο

Σημείωση 1: Για να εγκαταστήσει ο οποιοσδήποτε χρήστης το λογισμικό «Adobe *flash player*» στο λειτουργικό σύστημα «*CentOS 6.5*», συνδέεται σε αυτό, ως χρήστης «*root*» και ακολουθεί την ίδια διαδικασία, που εφήρμοσε κατά την εγκατάσταση του λογισμικού «Adobe *flash player*» στο λειτουργικό σύστημα «Kali Linux».

Σημείωση 2: Προκειμένου να ενημερωθεί το λειτουργικό σύστημα «*CentOS 6.5*» και οι διάφορες εφαρμογές του, ο χρήστης συνδέεται σε αυτό, ως χρήστης «*root*», ανοίγει ένα τερματικό και εκτελεί την εντολή «*yum update*».

Σημείωση 3: Για να εγκαταστήσει ο οποιοσδήποτε χρήστης το λογισμικό «*VMware Tools*» στο λειτουργικό σύστημα «*CentOS 6.5*», συνδέεται σε αυτό, ως χρήστης «root», ακολουθεί την διαδρομή «*VM>Install Vmware Tools*», για να τοποθετήσει στο «cd/dvd rom» του εικονικού υπολογιστή το αρχείο της μορφής «.iso», που περιέχει το πρόγραμμα εγκατάστασης του λογισμικού «*VMware Tools*», ανοίγει ένα τερματικό και εκτελεί τις παρακάτω εντολές, προκειμένου να αντιγράψει το πρόγραμμα εγκατάστασης του λογισμικού «*VMware Tools*» στο φάκελο «/tmp/».

```
mkdir /mnt/vmware
mount /dev/cdrom /mnt/vmware/
cp –rf /mnt/vmware/VMwareTools*/tmp/
```

Αμέσως μετά, ο χρήστης, με τις παρακάτω εντολές εισέρχεται στο φάκελο «/tmp/», εξάγει το συμπιεσμένο αρχείο και εκτελεί το πρόγραμμα εγκατάστασης του λογισμικού «*VMware Tools*».

```
cd /tmp/
tar zxpf VMwareTools-*.tar.gz
cd vmware-tools-distrib/
./vmware-install.pl
```

Τέλος, ακολουθεί τις προτροπές, που εμφανίζονται κατά την διάρκεια της εγκατάστασης, έως ότου ολοκληρωθεί με επιτυχία η εγκατάσταση του λογισμικού «*VMware Tools*».

Δ. Εγκατάσταση των Λογισμικών MySQL 5.5.x, Apache HTTP Server 2.2.x, PHP 5.5.x και phpMyAdmin 4.2.x στο Λειτουργικό Σύστημα «CentOS 6.5»

Στην αρχή, ο χρήστης συνδέεται στο λειτουργικό σύστημα «CentOS 6.5» ως χρήστης «root», ανοίγει ένα τερματικό και εκτελεί τις παρακάτω εντολές, προκειμένου να διαγράψει οποιαδήποτε παλιότερη έκδοση των λογισμικών προγραμμάτων «MySQL», «Apache», «PHP», «phpMyAdmin» είναι εγκατεστημένη.

```
MySQL: yum remove mysql mysql-server
Apache: yum remove httpd
PHP: yum remove php
phpMyAdmin: yum remove phpMyAdmin
```

Αμέσως μετά προβαίνει στην επανεκκίνηση του εικονικού υπολογιστή. Στην συνέχεια, συνδέεται στο λειτουργικό σύστημα «CentOS 6.5» ως χρήστης «root», ανοίγει ένα τερματικό και εκτελεί τις παρακάτω εντολές, προκειμένου να εγκαταστήσει επιπρόσθετα πακέτα (Extra Packages for Enterprise Linux -EPEL), καθώς και το αποθετήριο Remi (Remi Repo), έτσι ώστε να είναι διαθέσιμες οι νεώτερες εκδόσεις των λογισμικών προγραμμάτων «MySQL», «Apache», «PHP», «phpMyAdmin».

```
32bit:
rpm -Uvh http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
rpm -Uvh http://rpms.famillecollet.com/enterprise/remi-release-6.rpm

64bit:
rpm -Uvh http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
rpm -Uvh http://rpms.famillecollet.com/enterprise/remi-release-6.rpm
```

Κατόπιν, εκτελεί την παρακάτω εντολή, στο ήδη ανοικτό τερματικό, για να εγκαταστήσει τα λογισμικά MySQL, Apache, PHP και phpMyAdmin.

```
yum --enablerepo=remi,remi-php55 install httpd mysql mysql-server php php-common phpMyAdmin
```

Ο χρήστης, εφόσον το επιθυμεί, εκτελεί μία ή περισσότερες από τις ακόλουθες εντολές, για να δει ή/και για να εκμαιεύσει περισσότερες πληροφορίες ή/και για να εγκαταστήσει τις χρήσιμες βιβλιοθήκες και τις αυτόνομες αλγοριθμικές δομές (modules) της «PHP» που είναι διαθέσιμες.

```
yum search php-
yum info name of the module
yum install name of the module name of the module name of the module …
```

Στην συνέχεια, εκτελεί την παρακάτω εντολή, στο ήδη ανοικτό τερματικό, για να εγκαταστήσει συγκεκριμένες βιβλιοθήκες και αυτόνομες αλγοριθμικές δομές της «PHP».

```
yum --enablerepo=remi,remi-php55 install php-pecl-apc php-cli php-pear php-pdo php-mysqlnd php-pgsql php-pecl-mongo php-sqlite php-pecl-memcache php-pecl-memcached php-gd php-mbstring php-mcrypt php-xml
```

Κατόπιν, ανοίγει το αρχείο «*httpd.conf*», του φακέλου «*/etc/httpd/conf/*», με την βοήθεια ενός κειμενογράφου. Εφόσον ο «Apache HTTP Server» πρόκειται να εγκατασταθεί στον υπολογιστή του χρήστη, ο χρήστης βρίσκει την γραμμή «*#ServerName www.example.com:80*», πατάει «*Enter*» και εισάγει την γραμμή «*ServerName localhost*». Επίσης, αλλάζει την γραμμή «*DirectoryIndex index.html index.html.var*» σε «*DirectoryIndex index.html index.html.var index.htm index.shtml index.php index.php4 index.php3 index.cgi*». Ύστερα, βρίσκει την γραμμή «*AddOutputFilter INCLUDES .shtml*», πατάει «*Enter*» και εισάγει την γραμμή «*AddHandler application/x-httpd-php .php .phtml .html .htm*», διασφαλίζοντας ότι ο μηχανισμός εκτέλεσης της PHP, θα διερμηνεύει τα αρχεία με επεκτάσεις «.php», «.phtml», «.html» και «.htm». Εάν κάποιος χρήστης, επιθυμεί να προβεί σε κλείδωμα φακέλων ή/και αρχείων, με εισαγωγή «*ονόματος χρήστη*» και «*κωδικού*» (.htaccess), τότε αλλάζει τη γραμμή «*AllowOverride None*» σε «*AllowOverride All*».Στην περίπτωση που ο χρήστης θέλει να εκκινήσει την υπηρεσία «*httpd*», πληκτρολογεί την εντολή «*service httpd start*», ενώ εάν θέλει να την σταματήσει, πληκτρολογεί την εντολή «*/etc/init.d/httpd stop*». Εφόσον επιθυμεί να επανεκκινήσει την υπηρεσία, πληκτρολογεί την εντολή «*service httpd restart*». Εάν θελήσει να ενημερωθεί για την κατάσταση της υπηρεσίας, πληκτρολογεί «*/etc/init.d/httpd status*». Όλα τα αρχεία που κάνει «host» ο «server» θα πρέπει να αποθηκεύονται στο φάκελο «*/var/www/html/*». Προτείνεται, ο χρήστης για δική του ευκολία, να δημιουργήσει ένα νέο φάκελο (π.χ. με την ονομασία «*websites*»), μέσα στο φάκελο «*html*» για να αποθηκεύει εκεί όλα τα αρχεία του, καθώς και να δημιουργήσει έναν σύνδεσμο προς το φάκελο «*html*» και να τον τοποθετήσει στην επιφάνεια εργασίας.

Επιπρόσθετα, ανοίγει το αρχείο «*php.ini*», του φακέλου «*/etc/*», με την βοήθεια ενός κειμενογράφου. Αλλάζει την γραμμή «*error_reporting = E_ALL & ~E_DEPRECATED & ~E_STRICT*» σε «*error_reporting = E_ALL & ~E_NOTICE & ~E_STRICT & ~E_DEPRECATED*». Αλλάζει την γραμμή «*display_errors = Off*» σε «*display_errors = On*». Εντοπίζει την γραμμή «*report_memleaks = On*», για να βεβαιωθεί ότι η τιμή «*report_memleaks*» είναι «*On*». Στη περίπτωση, που η τιμή «*report_memleaks*» είναι «*Off*», δεν θα εμφανίζονται τα «*memory leaks*». Πατάει «*Enter*», μετά από την γραμμή «*;date.timezone =*» και εισάγει την γραμμή «*date.timezone = Europe/Athens*», εφόσον βρίσκεται στην Ελλάδα, ειδάλλως πηγαίνει στην ηλεκτρονική διεύθυνση «http://php.net/manual/en/timezones.php» και αναζητά από την πλήρη λίστα των χρονικών ζωνών την ήπειρο και την χώρα όπου διαμένει.

Ύστερα, ανοίγει το αρχείο «*config.inc.php*», του φακέλου «*/etc/phpMyAdmin*», με την βοήθεια ενός κειμενογράφου. Τροποποιεί την παράμετρο «*$cfg['Servers'][$i]['host']*». Η παράμετρος αυτή καθορίζει το μέρος που ο «MySQL Server» λειτούργει. Εάν ο «MySQL Server» λειτουργεί στον ίδιο υπολογιστή, όπου λειτουργεί ο «Web Server» Apache με την PHP, θα πρέπει ο χρήστης να ορίσει την παράμετρο αυτή να είναι «localhost» («*$cfg['Servers'][$i]['host'] = 'localhost';*»). Επίσης, τροποποιεί και την παράμετρο «*$cfg['Servers'][$i]['auth_type']*». Η παράμετρος αυτή καθορίζει τον τρόπο, με το οποίο ο χρήστης εισέρχεται και έχει πρόσβαση στον «MySQL Server». Οι πιθανές τιμές της παραμέτρου είναι «*http*», «*cookie*», «*config*». Αν ο χρήστης επιλέξει την τιμή «*http*», τότε οι παράμετροι «*$cfg['blowfish_secret']*» και «*$cfg['Servers'][$i]['auth_type']*» παίρνουν τις εξής τιμές: «*$cfg['blowfish_secret'] = '';*» και «*$cfg['Servers'][$i]['auth_type'] = 'http';*». Αυτή η μέθοδος αυθεντικοποίησης είναι η βασική μέθοδος αυθεντικοποίησης «HTTP», είναι περισσότερο ασφαλής, και είναι καλό να χρησιμοποιείται. Αν ο χρήστης επιλέξει την τιμή «cookie», τότε οι παράμετροι «$cfg['blowfish_secret']» και «$cfg['Servers'][$i]['auth_type']» παίρνουν τις εξής τιμές: «$cfg['blowfish_secret'] = 'anyrandomtextyouwant';» και

«$cfg['Servers'][$i]['auth_type'] = 'cookie';». Αν ο χρήστης επιλέξει την τιμή «config», τότε οι παράμετροι «$cfg['blowfish_secret']», «$cfg['Servers'][$i]['auth_type']», «$cfg['Servers'][$i]['user']» και «$cfg['Servers'][$i]['password']» παίρνουν τις εξής τιμές: «$cfg['blowfish_secret'] = '';», «$cfg['Servers'][$i]['auth_type'] = 'config';», «$cfg['Servers'][$i]['user'] = 'root';» και «$cfg['Servers'][$i]['password'] = 'password_MySQL';».

Στην συνέχεια, ο χρήστης επανεκκινεί τον υπολογιστή του και αμέσως μετά, συνδέεται στο λειτουργικό σύστημα «CentOS 6.5» ως χρήστης «root», ανοίγει ένα τερματικό και εκτελεί τις παρακάτω εντολές, προκειμένου να ενεργοποιήσει τις υπηρεσίες «MySQL» και «Apache».

```
chkconfig --levels 235 mysqld on
chkconfig --levels 235 httpd on
```

Κατόπιν, εκτελεί τις ακόλουθες εντολές, για να εκκινήσει τις υπηρεσίες MySQL και Apache.

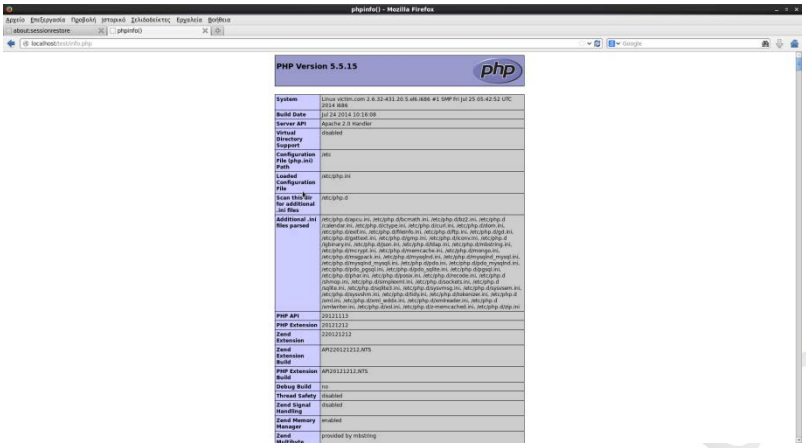
```
/etc/init.d/mysqld start
service httpd start
```

Στην συνέχεια, εκτελεί την εντολή «*mysqladmin -u root password 'mypassword'*», για να εισάγει κωδικό πρόσβασης για το χρήστη «*root*», του «MySQL Server».

Έπειτα, για να ελέγξει την σωστή εγκατάσταση της «MySQL» και να επιβεβαιώσει την ορθή λειτουργία της, εκτελεί την εντολή «*mysql -u root -p*». Στην συνέχεια, πληκτρολογεί τον κωδικό πρόσβασης που έχει ορίσει για το χρήστη «*root*» του «MySQL Server». Εφόσον, εισάγει το σωστό κωδικό, τότε εμφανίζεται η αρχική οθόνη της επιτυχημένης σύνδεσης. Με την προτροπή «*mysql>*» η «MySQL», δείχνει ότι είναι έτοιμη να δεχθεί εντολές. Για παράδειγμα, με την εντολή «*show databases;*», εμφανίζονται τα ονόματα των εγκατεστημένων βάσεων δεδομένων.

Εφόσον, επιθυμεί να παραμετροποιήσει τις ρυθμίσεις του «MySQL Server», είτε ανοίγει το αρχείο «*my.cnf*», του φακέλου «*/etc/*», με την βοήθεια ενός κειμενογράφου, είτε πληκτρολογεί την εντολή «*mysql_secure_installation*» και προβαίνει στις ρυθμίσεις που επιθυμεί. Επίσης, το μονοπάτι του φακέλου στον οποίο αποθηκεύονται οι Βάσεις Δεδομένων είναι το «*/var/lib/mysql*».

Αμέσως μετά, προβαίνει στην επανεκκίνηση του εικονικού υπολογιστή. Στην συνέχεια, μέσα στον φάκελο «*html*», δημιουργεί το αρχείο «*info.php*» (δεξί κλικ> Δημιουργία εγγράφου> Κενό αρχείο), του οποίου το περιεχόμενο είναι «*<?php phpinfo(); ?>*». Έπειτα, ο χρήστης ανοίγει έναν φυλλομετρητή και στο «url» πληκτρολογεί την διεύθυνση «*localhost/info.php*». Αν η «PHP» έχει εγκατασταθεί σωστά, ο χρήστης βλέπει μια σελίδα με πληροφορίες για τις εκδόσεις «PHP», «Apache» κ.α. που χρησιμοποιεί (Εικόνα 111).

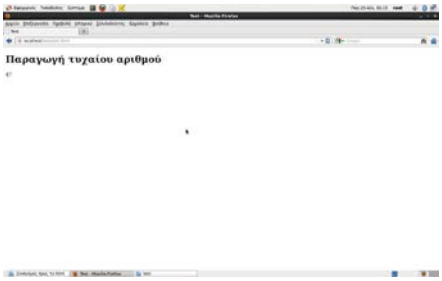


Εικόνα 111: Επιτυχημένη Εγκατάσταση της PHP

Για να βεβαιωθεί ο χρήστης, ότι ο μηχανισμός εκτέλεσης της «PHP», διερμηνεύει τα αρχεία με επεκτάσεις . «.php», «.phtml», «.html» και «.htm», δημιουργεί το αρχείο «*test.html*», μέσα στον φάκελο «*html*». Ακολουθεί ο κώδικας του αρχείου.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">


    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8"
/>
        <title>Test</title>
    </head>


    <body>
      <h1>Παραγωγή τυχαίου αριθμού</h1>


        <?php
            echo(mt_rand(0,100));
        ?>
    </body>


</html>
```

Στην συνέχεια ο χρήστης ανοίγει έναν φυλλομετρητή και στο «url» πληκτρολογεί την διεύθυνση «*localhost/test.html*». Αν η «PHP» και ο «Apache» έχουν εγκατασταθεί σωστά, τότε ο χρήστης βλέπει το αποτέλεσμα της Εικόνα 112.

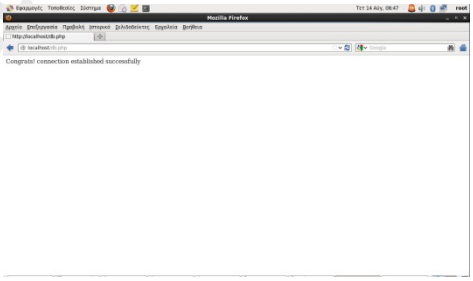


Εικόνα 112: Παραγωγή Τυχαίου Αριθμού με την Χρήση PHP

Για να βεβαιωθεί ο χρήστης, ότι υπάρχει πλήρη συνεργασία μεταξύ της «MySQL» και της «PHP», δημιουργεί το αρχείο «*db.php*», μέσα στον φάκελο «html». Ακολουθεί ο κώδικας του αρχείου.

```
<?php
      $con = mysql_connect("localhost","root","my_password");
      if (!$con)
      {
         die('Could not connect: ' . mysql_error());
      }
      else
      {
         echo "Congrats! connection established successfully";
      }
      mysql_close($con);
?>
```

Στην συνέχεια ο χρήστης ανοίγει έναν φυλλομετρητή και στο «url» πληκτρολογεί την διεύθυνση «*localhost/db.php*». Αν η «PHP» και η «MySQL» συνεργάζονται σωστά, τότε ο χρήστης βλέπει το αποτέλεσμα της Εικόνα 113.



Εικόνα 113: Επιτυχημένη Σύνδεση στην Βάση Δεδομένων

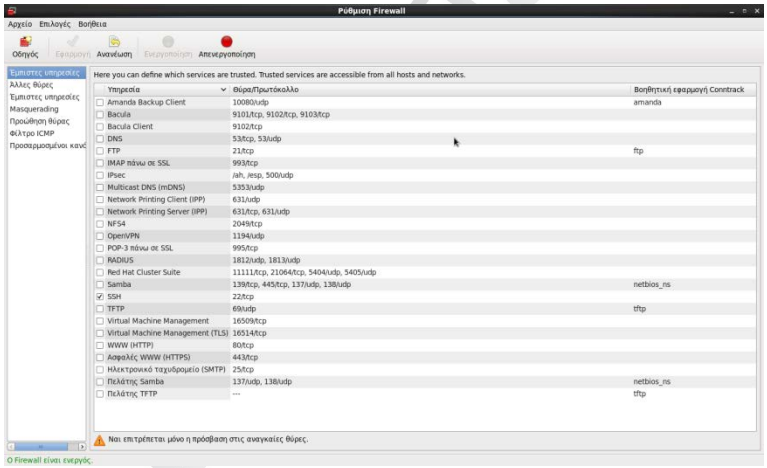
Τέλος, ο χρήστης ανοίγει ένα τερματικό και εκτελεί την εντολή «*yum update*», για να ενημερωθεί το λειτουργικό σύστημα «*CentOS 6.5*» και οι διάφορες εφαρμογές του.

Εφόσον, ο χρήστης, επιθυμεί να διαχειριστεί τις Βάσεις Δεδομένων, με το εργαλείο «phpMyAdmin», πληκτρολογεί την διεύθυνση «*http://localhost/phpMyAdmin*», στο «url» ενός φυλλομετρητή και στη προτροπή πιστοποίησης που θα εμφανιστεί, εισάγει για «*username*» την τιμή «root» και για «*password*» το κωδικό πρόσβασης που έχει εισαγάγει για το χρήστη «*root*», του «MySQL Server».

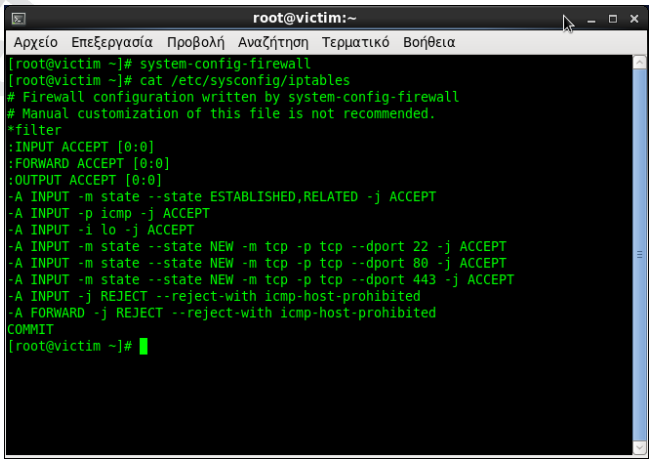
Σημείωση: Προκειμένου ο χρήστης να έχει πρόσβαση στις υπηρεσίες «*HTTP*» και «*HTTPS*» του «Apache HTTP Server» από οποιοδήποτε άλλο λειτουργικό σύστημα, προβαίνει σε άρση αποκλεισμ*ού* των θυρών *80* και *443 αντίστοιχα*, από το ανάχωμα ασφαλείας (firewall) «*iptables*».

Για να επιτευχθεί αυτό, ο χρήστης συνδέεται στο λειτουργικό σύστημα «CentOS 6.5» ως χρήστης «root», ανοίγει ένα τερματικό και εκτελεί την εντολή «*system-config-firewall*», προκειμένου να ρυθμίσει το ανάχωμα ασφαλείας «*iptables*» μέσα από γραφικό περιβάλλον (Εικόνα 114). Στην συνέχεια, επιλέγει τις υπηρεσίες «*HTTP*» και «*HTTPS*» και ενεργοποιεί το κουμπί «*Εφαρμογή*». Κατόπιν, ενεργοποιεί την επιλογή «*Έξοδο*» από την διαδρομή «*Αρχείο> Έξοδος*» και αμέσως μετά, προβαίνει στην επανεκκίνηση του εικονικού υπολογιστή.

Στην συνέχεια, για να επιβεβαιώσει την σωστή ρύθμιση του αναχώματος ασφαλείας, συνδέεται στο λειτουργικό σύστημα «CentOS 6.5» ως χρήστης «root», ανοίγει ένα τερματικό και εκτελεί την εντολή «*cat /etc/sysconfig/iptables*». Εφόσον, εμφανίζονται οι ρυθμίσεις του αναχώματος ασφαλείας «*iptables*» που απεικονίζονται στην Εικόνα 115 (*-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT* και *-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT*), οι υπηρεσίες «*HTTP*» και «*HTTPS*» του «Apache HTTP Server» είναι προσβάσιμες από οποιοδήποτε άλλο λειτουργικό σύστημα.



Εικόνα 114: Ρύθμιση του Αναχώματος Ασφαλείας «iptables»



Εικόνα 115: Προβολή Ρυθμίσεων του «iptables»

Ε. Αναφορά Ευπαθειών του Πληροφοριακού Συστήματος «ΕΥΔΟΞΟΣ»

Scan Report

Jun 30, 2014

Summary

This document reports on the results of an automatic security scan. The scan started at Mon Jun 30 08:40:48 2014 UTC and ended at Mon Jun 30 08:53:05 2014 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.169.131	Severity: High	1	2	2	20	0
Total: 1		1	2	2	20	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 25 results selected by the filtering described above. Before filtering there were 26 results.

2 Results per Host

2.1 192.168.169.131

Host scan start Mon Jun 30 08:40:55 2014 UTC
Host scan end Mon Jun 30 08:53:04 2014 UTC

Service (Port)	Threat Level
http (80/tcp)	High
general/tcp	Medium
ssh (22/tcp)	Medium
http (80/tcp)	Low
http (80/tcp)	Log
general/tcp	Log
ssh (22/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log

2.1.1 High http (80/tcp)

High (CVSS: 5.8)
NVT: http TRACE XSS attack

```
Summary:
Debugging functions are enabled on the remote HTTP server.
Description :
```

...continues on next page ...

... continued from previous page ...

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
An attacker may use this flaw to trick your legitimate web users to give him their credentials.
Solution:
Disable these methods.
Plugin output :
Solution:
Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable

OID of test routine: 1.3.6.1.4.1.25623.1.0.11213

References

CVE: CVE-2004-2320, CVE-2003-1567
BID:9506, 9561, 11604
Other:
URL:http://www.kb.cert.org/vuls/id/867593

[return to 192.168.169.131]

2.1.2 Medium general/tcp

Medium (CVSS: 2.6)
NVT: TCP timestamps

It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 374427
Paket 2: 375575

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

References

... continues on next page ...

... continued from previous page ...

Other:
URL:http://www.ietf.org/rfc/rfc1323.txt

[return to 192.168.169.131]

2.1.3 Medium ssh (22/tcp)

Medium (CVSS: 3.5)
NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability

According to its banner, the version of OpenSSH installed on the remote host is older than 5.7:
ssh-2.0-openssh_5.3
Summary:
The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.
OpenSSH before 5.7 is affected;
Solution:
Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103503

References
CVE: CVE-2012-0814
BID:51702
Other:
URL:http://www.securityfocus.com/bid/51702
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445
URL:http://packages.debian.org/squeeze/openssh-server
URL:https://downloads.avaya.com/css/P8/documents/100161262

[return to 192.168.169.131]

2.1.4 Low http (80/tcp)

Low (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.169.131
+ Target Hostname:    192.168.169.131
+ Target Port:        80
+ Start Time:         2014-06-30 08:42:05 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS)
+ Retrieved x-powered-by header: PHP/5.5.15
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: http://192.168.169.131/openeclass/
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.7). Apach
↪e 2.0.65 (final release) and 2.2.26 are also current.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
↪ST
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /test/info.php: PHP is installed, and a test script which runs php
↪info() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 20
↪99088, size: 5108, mtime: Tue Aug 28 10:48:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7354 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2014-06-30 08:42:20 (GMT0) (15 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.14260

Low (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

```
Here is the wapiti report:
Vulnerabilities report -- Wapiti
  http://wapiti.sourceforge.net/
This report has been generated by Wapiti Web Application Scanner
--- End of report ---
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80110

[return to 192.168.169.131]

2.1.5 Log http (80/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: HTTP Server type and version

```
The remote web server type is :
Apache/2.2.15 (CentOS)
Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

```
This are the directories/files found with brute force:
http://192.168.169.131:80/
http://192.168.169.131:80/cgi-bin/
http://192.168.169.131:80/error/
http://192.168.169.131:80/icons/
http://192.168.169.131:80/index.php
http://192.168.169.131:80/phpMyAdmin
http://192.168.169.131:80/phpMyAdmin/
http://192.168.169.131:80/phpmyadmin
http://192.168.169.131:80/phpmyadmin/
http://192.168.169.131:80/test/
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103079

Log (CVSS: 0.0)
NVT: Services

A web server is running on this port

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

Log (CVSS: 0.0)
NVT: Web mirroring

```
The following CGI have been discovered :
Syntax : cginame (arguments [default value])
/openeclass/template/classic/img/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/template/ocean/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/template/modern/img/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/index.php (localize [] )
/openeclass/modules/auth/registration.php (localize [] )
/openeclass/modules/auth/opencourses.php (fc [1] )
/openeclass/info/contact.php (localize [] )
/openeclass/info/copyright.php (localize [] )
/openeclass/modules/auth/altsearch.php (is_submit [ÎÏ?Î¿Î²Î¿ÎÎ®] localize [] u
↪name [] auth [] passwd [] )
/openeclass/include/securimage/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/manuals/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/modules/auth/methods/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/manuals/manual.php (localize [] )
/openeclass/template/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/main/perso/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/info/about.php (localize [] )
/openeclass/modules/auth/mail_verify.php (localize [] )
/openeclass/modules/auth/lostpass.php (send_link [Î[U+0091]Ï?Î¿Ï[U+0083]Ï[U+0084]ÎÎ¿ÎÎ®] localiz
↪userName [] email [] )
/openeclass/modules/search/search.php (submit [] search_terms [] )
/openeclass/modules/auth/altnewuser.php (localize [] uname [] auth [0] )
/openeclass/modules/auth/newuser.php (am [] submit [Î[U+0095]Î³Î³Ï?Î±Ï[U+0086]Î®] captcha_code
↪ [] password [] nom_form [] password1 [] uname [] localize [] prenom_form [] d
↪epartment [] email [] )
/openeclass/template/ocean/img/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/main/login_form.php (localize [] next [%2Fmain%2Fdisplay_profile.php
↪] )
/openeclass/modules/auth/listfaculte.php (localize [] )
/openeclass/template/classic/{%URL_PATH%}modules/search/{%SEARCH_ACTION%} (searc
↪h_terms [] submit [] )
/openeclass/template/modern/{%URL_PATH%}modules/search/{%SEARCH_ACTION%} (search
↪_terms [] submit [] )
```

... continues on next page ...

... continued from previous page ...

```
/openeclass/template/ocean/{%URL_PATH%}modules/search/{%SEARCH_ACTION%} (search_
↪terms [] submit [] )
/openeclass/template/classic/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/template/modern/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/modules/auth/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/modules/auth/formuser.php (localize [] p [1] )
/openeclass/info/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/ (submit [ 'Î[U+0095]Î¯Ï[U+0083]Î¿Î´Î¿Ï[U+0082]'] pass [] uname [] )
/openeclass/main/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
/openeclass/modules/auth/contactadmin.php (localize [] )
/openeclass/info/license/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
Directory index found at /openeclass/template/classic/
Directory index found at /openeclass/template/
Directory index found at /openeclass/template/classic/img/
Directory index found at /openeclass/main/
PHP script discloses physical path at /openeclass/main/classic.php (/var/www/htm
↪l/openeclass/main/classic.php)
Directory index found at /openeclass/main/perso/
PHP script discloses physical path at /openeclass/modules/auth/opencourses.php (
↪/var/www/html/openeclass/modules/auth/opencourses.php)
Directory index found at /openeclass/modules/auth/
Directory index found at /openeclass/modules/auth/methods/
Directory index found at /openeclass/manuals/
Directory index found at /openeclass/info/
Directory index found at /openeclass/info/license/
Directory index found at /openeclass/template/modern/
Directory index found at /openeclass/template/ocean/
PHP script discloses physical path at /openeclass/modules/auth/methods/casform.p
↪hp (/var/www/html/openeclass/modules/auth/methods/casform.php)
PHP script discloses physical path at /openeclass/modules/auth/methods/dbform.ph
↪p (/var/www/html/openeclass/modules/auth/methods/dbform.php)
PHP script discloses physical path at /openeclass/modules/auth/methods/imapform.
↪php (/var/www/html/openeclass/modules/auth/methods/imapform.php)
PHP script discloses physical path at /openeclass/modules/auth/methods/ldapform.
↪php (/var/www/html/openeclass/modules/auth/methods/ldapform.php)
PHP script discloses physical path at /openeclass/modules/auth/methods/pop3form.
↪php (/var/www/html/openeclass/modules/auth/methods/pop3form.php)
PHP script discloses physical path at /openeclass/modules/auth/methods/shibform.
↪php (/var/www/html/openeclass/modules/auth/methods/shibform.php)
Directory index found at /openeclass/template/modern/img/
Directory index found at /openeclass/template/ocean/img/
Directory index found at /openeclass/include/securimage/
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10662

Log (CVSS: 0.0)
NVT: Directory Scanner

```
The following directories were discovered:
/cgi-bin, /test, /error, /icons
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

References
Other:
OWASP:OWASP-CM-006

Log (CVSS: 0.0)
NVT: PHP Version Detection

```
Detected PHP version: 5.5.15
Location: tcp/80
CPE: cpe:/a:php:php:5.5.15
Concluded from version identification result:
X-Powered-By: PHP/5.5.15
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.800109

Log (CVSS: 0.0)
NVT: Apache Web ServerVersion Detection

```
Detected Apache version: 2.2.15
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.2.15
Concluded from version identification result:
Server: Apache/2.2.15
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900498

[return to 192.168.169.131]

2.1.6 Log general/tcp

Log (CVSS: 0.0)
NVT: OS fingerprinting

```
ICMP based OS fingerprint results: (91% confidence)
Linux Kernel
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

References
Other:
URL:http://www.phrack.org/issues.html?issue=57&id=7#article

Log (CVSS: 0.0)
NVT: Checks for open udp ports

```
Open UDP ports: [None found]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103978

Log (CVSS: 0.0)
NVT: arachni (NASL wrapper)

```
Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you
requested.
Please make sure that Arachni is installed and that arachni is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.110001

Log (CVSS: 0.0)
NVT: Traceroute

```
Here is the route from 192.168.169.136 to 192.168.169.131:
192.168.169.136
```

... continues on next page ...

... continued from previous page ...

192.168.169.131

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Log (CVSS: 0.0)
NVT: Checks for open tcp ports

Open TCP ports: 22, 80

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 192.168.169.131]

2.1.7 Log ssh (22/tcp)

Log
NVT:

Open port.

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0

OID of test routine: 1.3.6.1.4.1.25623.1.0.100259

Log (CVSS: 0.0)
NVT: SSH Server type and version

Detected SSH server version: SSH-2.0-OpenSSH_5.3

... continues on next page ...

... continued from previous page ...

```
Remote SSH supported authentication: password,publickey
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:5.3
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

Log (CVSS: 0.0)
NVT: Services

```
An ssh server is running on this port
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10330

[return to 192.168.169.131]

2.1.8 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
192.168.169.131|cpe:/a:apache:http_server:2.2.15
192.168.169.131|cpe:/a:php:php:5.5.15
192.168.169.131|cpe:/o:linux:kernel
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 192.168.169.131]

2.1.9 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

... continues on next page ...

... continued from previous page ...

traceroute:192.168.169.136,192.168.169.131
TCP ports:22,80
UDP ports:

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 192.168.169.131]

2.1.10 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary:
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103190

References
CVE: CVE-1999-0524
Other:
URL:http://www.ietf.org/rfc/rfc0792.txt

[return to 192.168.169.131]

ΣΤ. Εγκατάσταση των Λογισμικών MySQL 5.6.x, Apache HTTP Server 2.4.x, PHP 5.5.x και phpMyAdmin 4.2.x-all-languages στο Λειτουργικό Σύστημα «Windows»

Στην αρχή ο χρήστης, για δική του ευκολία, καλείται να δημιουργήσει ένα νέο φάκελο στο «*root*» κατάλογο του τοπικού δίσκου, μέσα στο οποίο θα εγκαταστήσει τα λογισμικά «*MySQL 5.6.x*», «*Apache HTTP Server 2.4.x*», «*PHP 5.5.x*» και «*phpMyAdmin 4.2.x – all languages*». Για παράδειγμα, δημιουργεί το φάκελο «`τοπικός δίσκος:\www`».

Στην περίπτωση που δεν είναι εγκατεστημένο στον υπολογιστή του χρήστη το λογισμικό «*Microsoft .NET Framework 4.5.1 (x86 and x64)*» ή νεώτερη έκδοση αυτού, τότε ο χρήστης καλείται να το εγκαταστήσει, κατεβάζοντάς το αυτόνομο πρόγραμμα εγκατάστασης του λογισμικού, από την ηλεκτρονική διεύθυνση «http://www.microsoft.com/en-us/download/default.aspx». Επειδή, το αυτόνομο πρόγραμμα εγκατάστασης δεν περιέχει πακέτα γλωσσών, ο χρήστης, εφόσον επιθυμεί να εγκαταστήσει γλωσσική υποστήριξη, εγκαθιστά το αυτόνομο πακέτο γλώσσας της επιλογής του, κατεβάζοντάς το από την ηλεκτρονική διεύθυνση «http://www.microsoft.com/en-us/download/details.aspx?id=40751».

Επιπλέον, στην περίπτωση που δεν είναι εγκατεστημένο στον υπολογιστή του χρήστη το λογισμικό «*Microsoft Visual Studio 2013*» και εφόσον ο χρήστης πρόκειται να εγκαταστήσει το λογισμικό «*MySQL Community Server*», καλείται να εγκαταστήσει πρώτα το πακέτο αναδιανομής «*Microsoft Visual C++ 2010 SP1 Redistributable Package x86*», κατεβάζοντάς το, από την ηλεκτρονική διεύθυνση «http://www.microsoft.com/en-us/download/». Επίσης, καλείται να εγκαταστήσει και το πακέτο αναδιανομής «*Visual C++ Redistributable for Visual Studio 2012 Update 4*», κατεβάζοντάς την 32bit έκδοση (VSU4\vcredist_x86.exe) αυτού, από την ηλεκτρονική διεύθυνση «http://www.microsoft.com/en-us/download/default.aspx», επειδή πρόκειται να εγκαταστήσει την τελευταία 32bit «*thread safe*» έκδοση του λογισμικού «*PHP*».

Εγκατάσταση του Λογισμικού MySQL

Η MySQL διατίθεται σε δύο βασικές εκδόσεις: α) την έκδοση «*MySQL Enterprise*» , η οποία έχει συνδρομή και όσο αφόρα την διαχείριση και την βελτιστοποίηση της, πραγματοποιείται από επαγγελματίες συμβούλους της MySQL και β) την έκδοση «*MySQL Community Server*», η οποία δεν είναι άλλη από την τελευταία έκδοση της «MySQL Enterprise», με την διαφορά ότι πλέον ο πηγαίος κώδικας είναι ελεύθερα διαθέσιμος, υπό την άδεια GNU General Public License (GPL).

Για να κατεβάσει ο οποιοσδήποτε χρήστης το λογισμικό «*MySQL Community Server*», πηγαίνει στην ηλεκτρονική διεύθυνση «http://www.mysql.com/downloads/mysql/» και κατεβάζει την 32bit έκδοση του «*MySQL Installer for Windows*» της τελευταίας έκδοσης της MySQL (MySQL Community Server 5.6.20>MySQL Installer 5.6 for Windows>Download Windows(x86, 64bit), MySQL Installer MSI> Download Windows(x86, 32bit), MSI Installer (mysql-installer-community-5.6.20.0.msi)). Στην συνέχεια, ο χρήστης εκτελεί το αρχείο «*mysql-installer-community-5.6.x.x.msi*» και ακολουθεί τα επόμενα βήματα.

Στο βήμα 1 (Εικόνα 116) ενεργοποιεί το κουμπί «*Ναι*», για να επιτρέψει στο πρόγραμμα «*mysql-installer-community-5.6.x.x.msi*» να εγκαταστήσει λογισμικό στον υπολογιστή του. Στην συνέχεια, ενεργοποιεί το κουμπί «*Ναι*», για να επιτρέψει στο πρόγραμμα «*WexInstaller.exe*» να πραγματοποιήσει αλλαγές στον υπολογιστή του, έτσι ώστε να εγκατασταθεί το πρόγραμμα εγκατάστασης της MySQL.

Στο βήμα 2 (Εικόνα 117), επιλέγει «*Install MySQL Products*» προκειμένου να εγκαταστήσει και να παραμετροποιήσει τα προϊόντα της MySQL.

Στο βήμα 3 (Εικόνα 118) τσεκάρει το «checkbox» «*I accept the license terms*», για να αποδεχθεί τους όρους της άδειας χρήσης και ενεργοποιεί το κουμπί «*Next*».

Στο βήμα 4 (Εικόνα 119) ενεργοποιεί το κουμπί «*Execute*», προκειμένου το πρόγραμμα εγκατάστασης της MySQL να αναζητήσει μέσω του διαδικτύου τυχόν καινούργιες εκδόσεις των προϊόντων της. Μόλις ολοκληρωθεί η παραπάνω διαδικασία (Εικόνα 120), ενεργοποιεί το κουμπί «*Next*».

Στο βήμα 5 (Εικόνα 121) επιλέγει τον τύπο του «server» που θέλει να εγκαταστήσει και στην συνέχεια ορίζει το μονοπάτι εγκατάστασης της MySQL (π.χ. `τοπικός δίσκος:\www\MySQL` (Εικόνα 122)). Αν επιθυμεί, μπορεί να αλλάξει τον τοπικό δίσκο ή/και το μονοπάτι του φακέλου «data», στον οποίο αποθηκεύονται οι Βάσεις Δεδομένων (π.χ. `τοπικός δίσκος:\www\MySQL\MySQL Server 5.6` (Εικόνα 122)). Στην συνέχεια, ενεργοποιεί το κουμπί «*Next*».

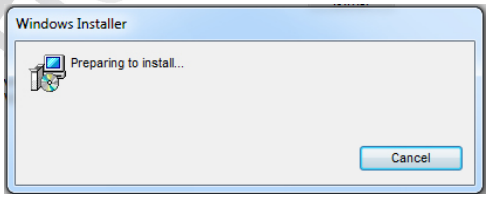
Στο βήμα 6 (Εικόνα 123) ενεργοποιεί το κουμπί «*Execute*», προκειμένου, πριν από την εγκατάσταση των προϊόντων της MySQL, να εγκατασταθούν στον υπολογιστή του, απαραίτητα λογισμικά προγράμματα και αμέσως μετά (Εικόνα 124), ενεργοποιεί το κουμπί «*Next*». Εάν, είναι ήδη εγκατεστημένα τα απαραίτητα λογισμικά προγράμματα, ενεργοποιεί το κουμπί «*Next*» (Εικόνα 124).

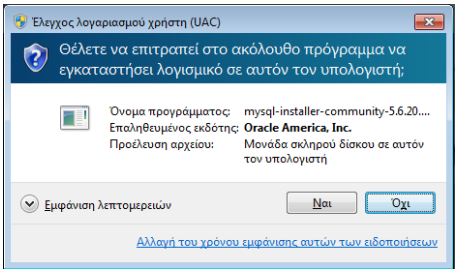
Στο βήμα 7 (Εικόνα 125) ενεργοποιεί το κουμπί «*Execute*», προκειμένου να εγκατασταθούν στον υπολογιστή του τα προϊόντα της MySQL. Αμέσως μετά την εγκατάσταση όλων των προϊόντων της MySQL (Εικόνα 126), ενεργοποιεί το κουμπί «*Next*», για να προχωρήσει στην παραμετροποίηση τους.

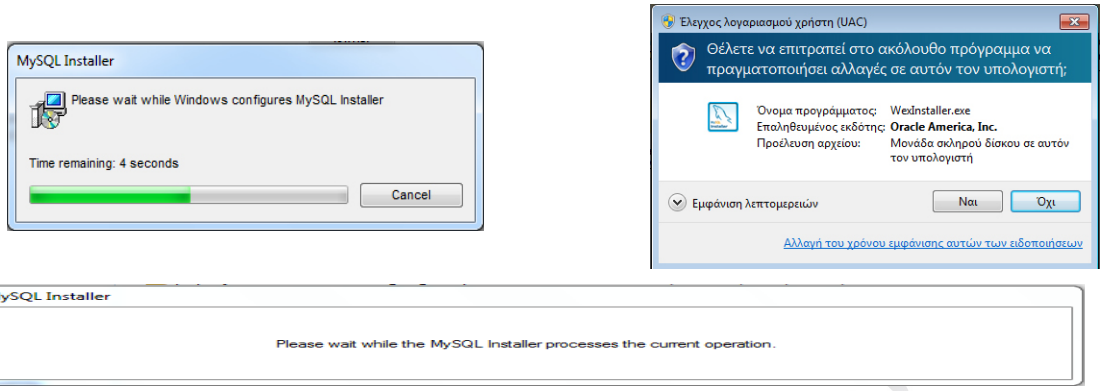
Στο βήμα 8 (Εικόνα 127) ενεργοποιεί το κουμπί «*Next*» για να παραμετροποιήσει τον «MySQL Server». Αμέσως μετά (Εικόνα 128), επιλέγει τον τύπο του server που θέλει να εγκαταστήσει (Εικόνα 129) και εφόσον βεβαιωθεί ότι είναι ήδη τσεκαρισμένα τα «checkbox» «*Enable TCP/IP Networking*» και «*Open Firewall port for network access*», τσεκάρει το «checkbox» «*Show Advanced Options*» (Εικόνα 130). Στην συνέχεια, ενεργοποιεί το κουμπί «*Next*» και κατόπιν (Εικόνα 131), εισάγει κωδικό πρόσβασης για το χρήστη «*root*». Έπειτα, ενεργοποιεί το κουμπί «*Next*» και είτε αλλάζει τις παραμέτρους της υπηρεσίας «MySQL Server» είτε τις αφήνει ως έχουν (Εικόνα 132). Έπειτα, ενεργοποιεί το κουμπί «*Next*» και τέλος (Εικόνα 133), εφόσον επιθυμεί να είναι διαθέσιμα όλα τα logs, τσεκάρει όλα τα «checkbox» και ενεργοποιεί το κουμπί «*Next*».

Στο βήμα 9 (Εικόνα 134) ενεργοποιεί το κουμπί «*Next*», προκειμένου να παραμετροποιηθούν τα παραδείγματα χρήσης και στην συνέχεια (Εικόνα 135), ενεργοποιεί το κουμπί «*Next*».

Στο τελευταίο βήμα (Εικόνα 136) ενεργοποιεί το κουμπί «*Finish*», εφόσον πρώτα έχει ολοκληρωθεί με επιτυχία η διαμόρφωση των παραμέτρων του προγράμματος. Κατόπιν, εμφανίζεται η αρχική οθόνη του MySQL Workbench (Εικόνα 137).

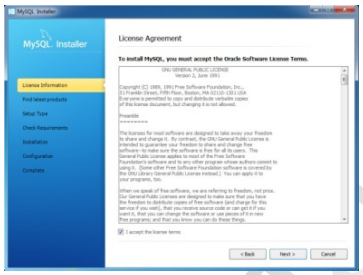




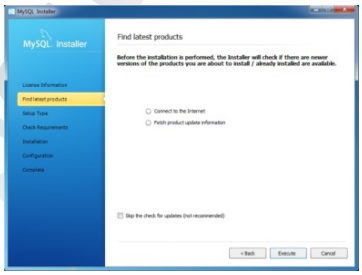


Εικόνα 116: Βήμα 1ο

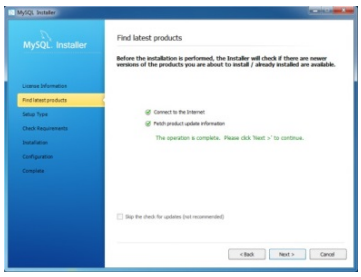
Εικόνα 117: Βήμα 2ο



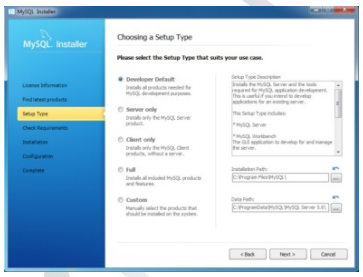
Εικόνα 118: Βήμα 3ο



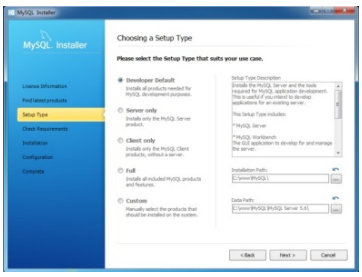
Εικόνα 119: Βήμα 4ο



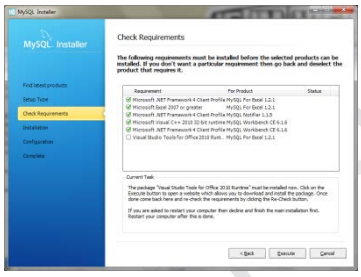
Εικόνα 120: Βήμα 4ο



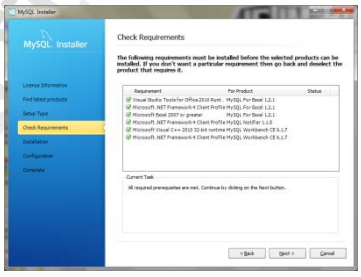
Εικόνα 121: Βήμα 5ο



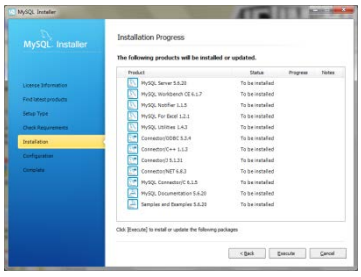
Εικόνα 122: Βήμα 5ο



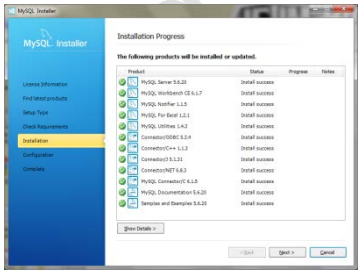
Εικόνα 123: Βήμα 6ο



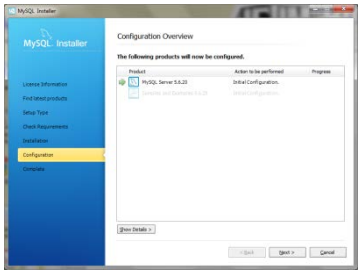
Εικόνα 124: Βήμα 6ο



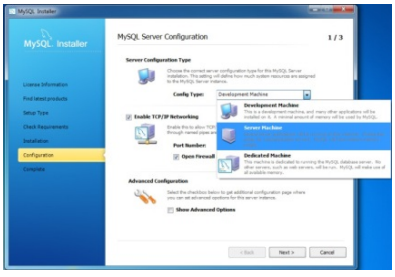
Εικόνα 125: Βήμα 7ο



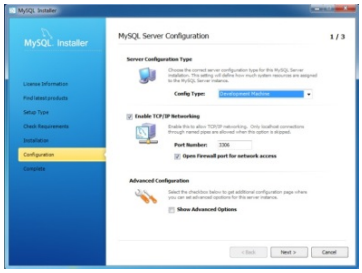
Εικόνα 126: Βήμα 7ο



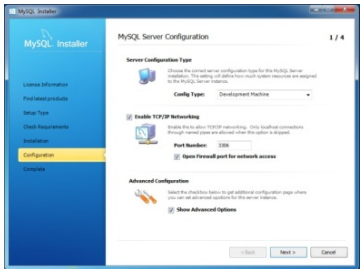
Εικόνα 127: Βήμα 8ο



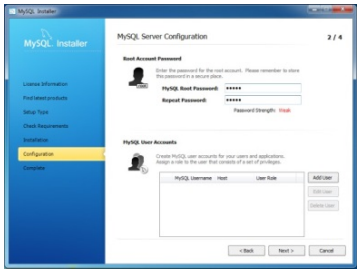
Εικόνα 128: Βήμα 8ο



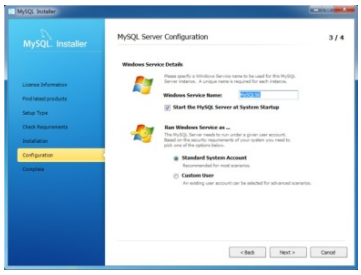
Εικόνα 129: Βήμα 8ο



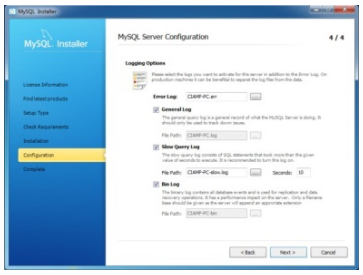
Εικόνα 130: Βήμα 8ο



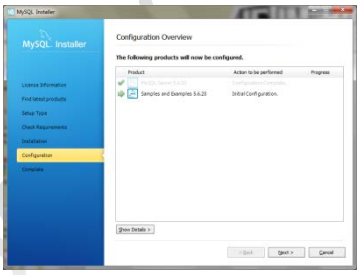
Εικόνα 131: Βήμα 8ο



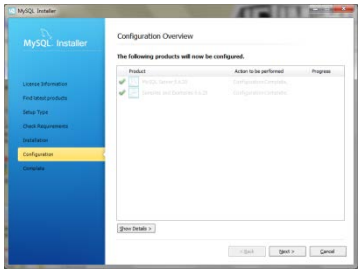
Εικόνα 132: Βήμα 8ο



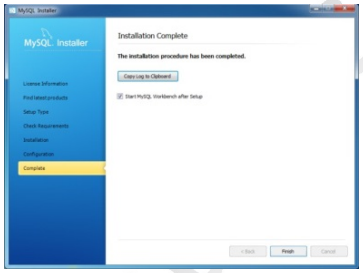
Εικόνα 133: Βήμα 8ο



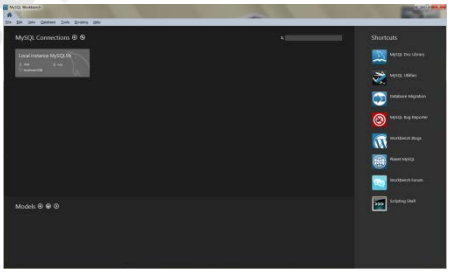
Εικόνα 134: Βήμα 9ο



Εικόνα 135: Βήμα 9ο



Εικόνα 136: Βήμα 10ο

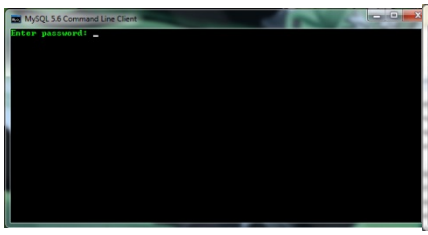


Εικόνα 137: Βήμα 10ο

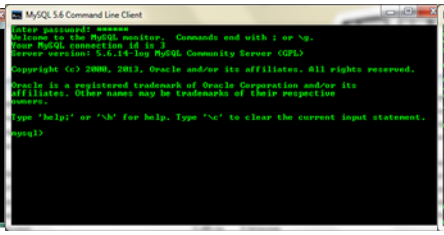
Σημείωση: Κάθε φορά, που ο χρήστης ανοίγει τον υπολογιστή του, η MySQL τρέχει. Αυτό το εξακριβώνει με το να ακολουθήσει το μονοπάτι «*Έναρξη>Πίνακας Ελέγχου>Όλα τα στοιχεία του Πίνακα Ελέγχου>Εργαλεία διαχείρισης>Υπηρεσίες>MySQL56*» και να δεί ότι η υπηρεσία «MySQL56» έχει ξεκινήσει αυτόματα.

Επιπλέον, για να ελέγξει την σωστή εγκατάσταση της MySQL και να επιβεβαιώσει ότι δουλεύει σωστά, το μόνο που πρέπει να κάνει, είναι να χρησιμοποιήσει την «*MySQL Command Line Client*» (Έναρξη>Όλα τα προγράμματα>MySQL>MySQL Server 5.6>MySQL 5.6 Command Line Client). Στην αρχή (Εικόνα 138), ο χρήστης πληκτρολογεί τον κωδικό πρόσβασης που έχει ορίσει για το χρήστη «*root*» στο βήμα 8 (Εικόνα 131) της εγκατάστασης της MySQL. Εφόσον, εισάγει το σωστό κωδικό, τότε εμφανίζεται η αρχική οθόνη της επιτυχημένης σύνδεσης (Εικόνα 139). Με την προτροπή «*mysql>*» η MySQL, δείχνει ότι είναι έτοιμη να δεχθεί εντολές. Για παράδειγμα, με την εντολή «*show databases;*» (Εικόνα 140), εμφανίζονται τα ονόματα των εγκατεστημένων βάσεων δεδομένων.

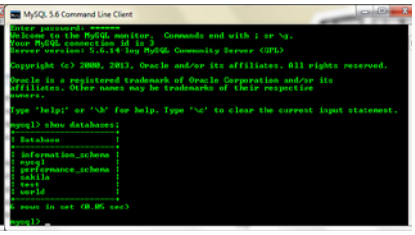
Τέλος, για οποιοδήποτε μελλοντική παραμετροποίηση επιθυμεί να κάνει ο χρήστης είτε παραμετροποιεί το αρχείο «*my.ini*» που βρίσκεται στο φάκελο «*τοπικός δίσκος:\www\MySQL\MySQL Server 5.6*», είτε ανοίγει το πρόγραμμα εγκατάστασης της MySQL (Έναρξη>Όλα τα προγράμματα>MySQL>MySQL Installer>MySQL Installer) και προβαίνει στις ενέργειες που επιθυμεί.



Εικόνα 138: MySQL 5.6 Command Line Client – *Κωδικός*



Εικόνα 139: MySQL 5.6 Command Line Client – *Επιτυχής Σύνδεση*



Εικόνα 140: MySQL 5.6 Command Line Client – *show databases;*

Εγκατάσταση του Λογισμικού Apache HTTP Server

Για να κατεβάσει ο οποιοσδήποτε χρήστης το λογισμικό «*Apache HTTP Server*», εφόσον στην συνέχεια θα εγκαταστήσει το λογισμικό «*PHP VC11 x86*», πηγαίνει στην ηλεκτρονική διεύθυνση «http://www.apachelounge.com/download/» και κατεβάζει την τελευταία 32bit έκδοση του «Apache HTTP Server» (`httpd-2.4.10-win32-VC11.zip`).

Επειδή, το αρχείο που κατεβαίνει είναι σε συμπιεσμένη μορφή, ο χρήστης το εξαγάγει στην «*Επιφάνεια Εργασίας*» και δημιουργείται ο φάκελος «*httpd-2.4.x-win32-VC11*». Στην συνέχεια, ανοίγει το φάκελο «*httpd-2.4.x-win32-VC11*» και αντιγράφει το φάκελο «*Apache24*» στο φάκελο «*τοπικός δίσκος:\www*». Κατόπιν, ανοίγει το φάκελο «*τοπικός δίσκος:\www\Apache24\conf*» και με την βοήθεια ενός κειμενογράφου, ανοίγει το αρχείο «*httpd.conf*» και προβαίνει στις ακόλουθες τροποποιήσεις.

- «*ServerRoot "c:/Apache24"*» → «*ServerRoot "τοπικός δίσκος:/www/Apache24"*»
- «*DocumentRoot "c:/Apache24/htdocs"*» → «*DocumentRoot "τοπικός δίσκος:/www/Apache24/htdocs"*»
- «*<Directory "c:/Apache24/htdocs">*» → «*<Directory "τοπικός δίσκος:/www/Apache24/htdocs">*»
- «*ScriptAlias /cgi-bin/ "c:/Apache24/cgi-bin/"*» → «*ScriptAlias /cgi-bin/ "τοπικός δίσκος:/www/Apache24/cgi-bin/"*»
- «*<Directory "c:/Apache24/cgi-bin">*» → «*<Directory "τοπικός δίσκος:/www/Apache24/cgi-bin">*»

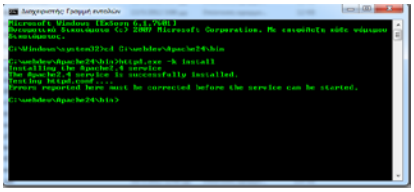
Επιπλέον, εφόσον ο «Apache HTTP Server» πρόκειται να εγκατασταθεί στον υπολογιστή του χρήστη, ο χρήστης βρίσκει την γραμμή «*#ServerName www.example.com:80*», πατάει «*Enter*» και εισάγει την γραμμή «*ServerName localhost*».

Στην περίπτωση, που ο χρήστης θέλει να χρησιμοποιήσει τα «*conf*» αρχεία του φακέλου «*τοπικός δίσκος:\www\Apache24\conf\extra*», θα πρέπει, με την βοήθεια ενός κειμενογράφου, να αλλάξει σε αυτά, το μονοπάτι του φακέλου που βρίσκεται εγκατεστημένος ο Apache.

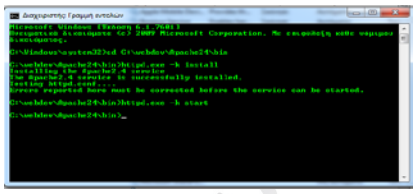
Ο χρήστης προκειμένου να εγκαταστήσει την υπηρεσία Apache, ανοίγει ένα παράθυρο γραμμής εντολών ως *διαχειριστής* (`Έναρξη> Όλα τα προγράμματα> Βοηθήματα> Γραμμή εντολών`) και εκτελεί τις εξής εντολές (Εικόνα 141):

```
cd τοπικός δίσκος:\www\Apache24\bin
httpd.exe -k install
```

Κατόπιν, πληκτρολογεί την εντολή «*httpd.exe -k start*», για να γίνει εκκίνηση της υπηρεσίας Apache (Εικόνα 142). Στην περίπτωση που θέλει να σταματήσει την υπηρεσία, πληκτρολογεί την εντολή «*httpd.exe -k stop*». Εφόσον επιθυμεί να επανεκκινήσει την υπηρεσία, πληκτρολογεί την εντολή «*httpd.exe -k restart*». Εάν θελήσει να απεγκαταστήσει, την υπηρεσία πληκτρολογεί «*httpd.exe -k uninstall*».



Εικόνα 141: Εγκατάσταση της Υπηρεσίας Apache



Εικόνα 142: Εκκίνηση της Υπηρεσίας Apache

Για να ελέγξει ο χρήστης την λειτουργία του «Apache HTTP Server» μέσα από γραφικό περιβάλλον, πηγαίνει στο φάκελο «*τοπικός δίσκος:\www\Apache24\bin*» και αντιγράφει το αρχείο «*ApacheMonitor.exe*» στο φάκελο «*Εκκίνηση*» (Έναρξη> Όλα τα προγράμματα> Εκκίνηση, ύστερα δεξί κλικ> Άνοιγμα και μετά επικόλληση αρχείου). Στην συνέχεια, κάνει διπλό κλικ στο αρχείο «*ApacheMonitor.exe*» και τότε κάτω δεξιά στην γραμμή εργασιών και αριστερά από την εμφανιζόμενη ώρα και ημερομηνία, εμφανίζεται το εικονίδιο της Εικόνα 143. Το συγκεκριμένο εικονίδιο δηλώνει αν ο «Apache HTTP Server» λειτούργει ή όχι. Στις εικόνες Εικόνα 144 και Εικόνα 145 παρατηρούμε την διαδικασία, μέσα από γραφικό περιβάλλον, που ακολουθεί ο χρήστης προκειμένου να εκκινήσει την υπηρεσία Apache.

Εικόνα 143: Εικονίδιο του Apache HTTP Server, που Δηλώνει την μη Λειτουργία της Υπηρεσίας

Εικόνα 144: Διαδικασία Έναρξης της Υπηρεσίας Apache2.4

Εικόνα 145: Λειτουργία του Apache HTTP Server

Ο χρήστης σε αυτό το σημείο προχωράει στην εγκατάσταση του λογισμικού «*PHP*». Μόλις τελειώσει η εγκατάσταση της PHP, σταματάει την λειτουργία του «Apache HTTP Server» (κλικ στο εικονίδιο του Apache Server>Apache2.4>Stop), ανοίγει το φάκελο «*τοπικός δίσκος:\www\Apache24\conf*» και με την βοήθεια ενός κειμενογράφου, ανοίγει το αρχείο «*httpd.conf*» για να προβεί στις ακόλουθες τροποποιήσεις.

Μετά από την γραμμή «*#LoadModule xml2enc_module modules/mod_xml2enc.so*», ο χρήστης πατάει «*Enter*» και εισάγει την γραμμή «*LoadModule php5_module "τοπικός δίσκος:/www/php/php5apache2_4.dll"*», διασφαλίζοντας με αυτό τον τρόπο την ομαλή συνεργασία μεταξύ του Apache και της PHP.

Εάν κάποιος χρήστης, επιθυμεί να προβεί σε κλείδωμα φακέλων ή/και αρχείων, με εισαγωγή «*ονόματος χρήστη*» και «*κωδικού*» (.htaccess), τότε αλλάζει τη γραμμή «*AllowOverride None*» σε «*AllowOverride All*».

Ο χρήστης, αλλάζει την γραμμή «*DirectoryIndex index.html*» σε «*DirectoryIndex index.html index.htm index.shtml index.php index.php4 index.php3 index.cgi*».

Στην συνέχεια, βρίσκει την γραμμή «*#AddOutputFilter INCLUDES .shtml*», πατάει «*Enter*» και εισάγει την γραμμή «*AddHandler application/x-httpd-php .php .phtml .html*

.htm», διασφαλίζοντας ότι ο μηχανισμός εκτέλεσης της PHP, θα διερμηνεύει τα αρχεία με επεκτάσεις «.php», «.phtml», «.html» και «.htm».

Στην τελευταία γραμμή ο χρήστης εισάγει την γραμμή «*PHPIniDir "τοπικός δίσκος:/www/php/"*», προκειμένου να δηλώσει το μονοπάτι του αρχείου «*php.ini*». Τέλος, προβαίνει σε επανεκκίνηση του υπολογιστή του.

Σημείωση: Όλα τα αρχεία που κάνει «host» ο «server» θα πρέπει να αποθηκεύονται στο φάκελο «*τοπικός δίσκος:\www\Apache24\htdocs*». Προτείνεται, ο χρήστης για δική του ευκολία, να δημιουργήσει ένα νέο φάκελο (π.χ. με την ονομασία «*websites*»), μέσα στο φάκελο «*htdocs*» για να αποθηκεύει εκεί όλα τα αρχεία του, καθώς και να δημιουργήσει μια συντόμευση για το φάκελο «*htdocs*» και να την τοποθετήσει στην επιφάνεια εργασίας.

Επιπρόσθετα, ο οποιοσδήποτε χρήστης μπορεί να τοποθετήσει όλα τα αρχεία που δημιουργεί, σε όποιο φάκελο επιθυμεί πέραν από τον προεπιλεγμένο φάκελο «*htdocs*», αρκεί στο αρχείο «*httpd.conf*» και συγκεκριμένα στις γραμμές «*DocumentRoot "τοπικός δίσκος:/www/Apache24/htdocs"*» και «*<Directory "τοπικός δίσκος:/www/Apache24/htdocs">*», να δηλώσει το ακριβές μονοπάτι του φακέλου.

Εγκατάσταση του Λογισμικού PHP

Για να κατεβάσει ο οποιοσδήποτε χρήστης το λογισμικό «*PHP*», πηγαίνει στην ηλεκτρονική διεύθυνση «http://windows.php.net/download/» και κατεβάζει την τελευταία 32bit «*thread safe*» έκδοση της PHP (`php-5.5.15-Win32-VC11-x86.zip`). Οι εκδόσεις VC11 έχουν μεταγλωττιστεί με το «*Visual Studio 2012 compiler*» και έχουν βελτιωθεί τόσο ως προς την απόδοση, όσο και προς τη σταθερότητα. Οι εκδόσεις αυτές, απαιτούν από το χρήστη να έχει εγκαταστήσει στον υπολογιστή του, το πακέτο αναδιανομής «*Visual C++ Redistributable for Visual Studio 2012 Update 4*» ή το λογισμικό «*Microsoft Visual Studio 2012*» ή νεώτερες εκδόσεις αυτών.

Επειδή, το αρχείο που κατεβαίνει είναι σε συμπιεσμένη μορφή, ο χρήστης το εξαγάγει στο φάκελο «*τοπικός δίσκος:\www*». Για περισσότερη ασφάλεια, μετονομάζει το φάκελο «*php-5.5.x-Win32-VC11-x86*» σε «*php*» ή δίνει στο φάκελο κάποιο άλλο όνομα. Στην συνέχεια, ανοίγει το φάκελο «*τοπικός δίσκος:\www\php*», βρίσκει το αρχείο «*php.ini-development*» και το μετονομάζει σε «*php.ini*». Με την βοήθεια ενός κειμενογράφου, προβαίνει στις ακόλουθες τροποποιήσεις του αρχείου, προκειμένου να υπάρχει πλήρη συνεργασία μεταξύ του Apache, της PHP και της MySQL.

Εντοπίζει την περιοχή «*Dynamic Extensions*» και αφαιρεί το ερωτηματικό, που βρίσκεται μπροστά από τις δύο ακόλουθες επεκτάσεις MySQL «*;extension=php_mysql.dll*» «*;extension=php_mysqli.dll*», με σκοπό να επιτευχθεί η συνεργασία μεταξύ της PHP και της MySQL.

Αλλάζει την γραμμή «*error_reporting = E_ALL*» σε «*error_reporting = E_ALL & ~E_NOTICE*», προκειμένου όταν εκτελείται κάποια εντολή PHP, να εμφανίζονται στον φυλλομετρητή όλα τα λάθη εκτός από τις σημειώσεις.

Εντοπίζει την γραμμή «*display_errors = On*», για να βεβαιωθεί ότι η τιμή «*display_errors*» είναι «*On*» καθώς και την γραμμή «*report_memleaks = On*», για να βεβαιωθεί ότι η τιμή «*report_memleaks*» είναι «*On*». Στη περίπτωση, που η τιμή «*report_memleaks*» είναι «*off*», δεν θα εμφανίζονται τα «*memory leaks*».

Βρίσκει την γραμμή «*; extension_dir = "ext*"», πατάει «*Enter*» και εισάγει την γραμμή «*extension_dir = "τοπικός δίσκος:\www\php\ext"*», έτσι ώστε να γνωρίζει η PHP το μονοπάτι του φακέλου «*ext*», στον οποίο βρίσκονται οι επεκτάσεις.

Πατάει «*Enter*», μετά από την γραμμή «*;date.timezone =*» και εισάγει την γραμμή «*date.timezone = Europe/Athens*», εφόσον βρίσκεται στην Ελλάδα, ειδάλλως πηγαίνει στην ηλεκτρονική διεύθυνση «http://php.net/manual/en/timezones.php» και αναζητά από την πλήρη λίστα των χρονικών ζωνών την ήπειρο και την χώρα όπου διαμένει.

Επιπλέον, προαιρετικά και ανάλογα με τις απαιτήσεις του, στην περιοχή «*Dynamic Extensions*», αφαιρεί το ερωτηματικό που βρίσκεται μπροστά από τις ακόλουθες επεκτάσεις MySQL:

«*;extension=php_mbstring.dll*» (multibyte encodings),

«*;extension=php_soap.dll*» (write Web Services, use SOAP),

«*;extension=php_gd2.dll*» (resize images),

«*;extension=php_curl.dll*» (xml writer).

Σε αυτό το σημείο, ο χρήστης προσθέτει το μονοπάτι της PHP, στις μεταβλητές περιβάλλοντος. Με αυτήν την ενέργεια το Λειτουργικό Σύστημα καθώς και ο Apache μπορούν να κοιτάξουν μέσα στο σύστημα, ώστε να βρουν τα «*dll*» τα οποία θα χρειαστούν, προκειμένου να φορτωθεί η PHP. (Έναρξη> Πίνακας Ελέγχου> Σύστημα> Ρυθμίσεις συστήματος για προχωρημένους> Για Προχωρημένους> Μεταβλητές Περιβάλλοντος> Μεταβλητές Συστήματος> Path> Επεξεργασία. Στο πλαίσιο παραθύρου που εμφανίζεται, ο χρήστης προσθέτει στο τέλος του πεδίου «Τιμή Μεταβλητής», την γραμμή «*;τοπικός δίσκος:\www\php*». Στην συνέχεια, ενεργοποιεί το κουμπί «OK» και προβαίνει σε επανεκκίνηση του υπολογιστή του.)

Εγκατάσταση του Λογισμικού phpMyAdmin

Για να κατεβάσει ο οποιοσδήποτε χρήστης το λογισμικό «*phpMyAdmin*», πηγαίνει στην ηλεκτρονική διεύθυνση «http://www.phpmyadmin.net/home_page/downloads.php» και κατεβάζει την τελευταία έκδοση του phpMyAdmin (phpMyAdmin-4.2.7-all-languages.zip).

Επειδή, το αρχείο που κατεβαίνει είναι σε συμπιεσμένη μορφή, ο χρήστης το εξαγάγει στο φάκελο «*τοπικός δίσκος:\www\Apache24\htdocs*». Στην συνέχεια, ανοίγει το φάκελο «*phpMyAdmin-4.2.x-all-languages*» και για περισσότερη ασφάλεια, μετονομάζει το φάκελο «*phpMyAdmin-4.2.x-all-languages*» σε «*phpMyAdmin*» ή δίνει στο φάκελο κάποιο άλλο όνομα. Κατόπιν, αντιγράφει το φάκελο «*phpMyAdmin*» στο φάκελο «*τοπικός δίσκος:\www\Apache24\htdocs*». Αμέσως μετά, ανοίγει το φάκελο «*τοπικός δίσκος:\www\Apache24\htdocs\phpMyAdmin*», βρίσκει το αρχείο «*config.sample.inc.php*» και το μετονομάζει σε «*config.inc.php*». Με την βοήθεια ενός κειμενογράφου, προβαίνει στις ακόλουθες τροποποιήσεις του αρχείου, προκειμένου να λειτουργεί σωστά το phpMyAdmin.

α) Τροποποίηση της παραμέτρου «*$cfg['Servers'][$i]['host']*»

Η παράμετρος αυτή καθορίζει το μέρος που ο «MySQL Server» λειτούργει. Εάν ο «MySQL Server» λειτουργεί στον ίδιο υπολογιστή, όπου λειτουργεί ο «Web Server» Apache με την PHP, θα πρέπει ο χρήστης να ορίσει την παράμετρο αυτή να είναι «localhost» («*$cfg['Servers'][$i]['host'] = 'localhost';*»).

β) Τροποποίηση της παραμέτρου «*$cfg['Servers'][$i]['auth_type']*»

Η παράμετρος αυτή καθορίζει τον τρόπο, με το οποίο ο χρήστης εισέρχεται και έχει πρόσβαση στον «MySQL Server». Οι πιθανές τιμές της παραμέτρου είναι «*http*», «*cookie*», «*config*».

- Αν ο χρήστης επιλέξει την τιμή «*http*», τότε οι παράμετροι «*$cfg['blowfish_secret']*» και «*$cfg['Servers'][$i]['auth_type']*» παίρνουν τις εξής τιμές: «*$cfg['blowfish_secret'] = '';*» και «*$cfg['Servers'][$i]['auth_type'] = 'http';*».

  Αυτή η μέθοδος αυθεντικοποίησης είναι η βασική μέθοδος αυθεντικοποίησης HTTP, είναι περισσότερο ασφαλής, και είναι καλό να χρησιμοποιείται.

- Αν ο χρήστης επιλέξει την τιμή «*cookie*», τότε οι παράμετροι «*$cfg['blowfish_secret']*» και «*$cfg['Servers'][$i]['auth_type']*» παίρνουν τις εξής τιμές: «*$cfg['blowfish_secret'] = 'anyrandomtextyouwant';*» και «*$cfg['Servers'][$i]['auth_type'] = 'cookie';*».

  Αυτή η μέθοδος αυθεντικοποίησης απαιτεί την υποστήριξη cookies από τον φυλλομετρητή και ενεργοποίηση αυτών.

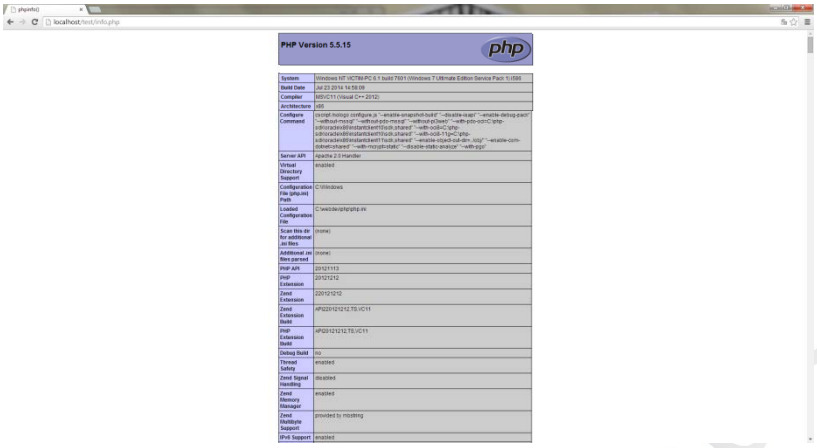
- Αν ο χρήστης επιλέξει την τιμή «*config*», τότε οι παράμετροι «*$cfg['blowfish_secret']*», «*$cfg['Servers'][$i]['auth_type']*», «*$cfg['Servers'][$i]['user']*» και «*$cfg['Servers'][$i]['password']*» παίρνουν τις εξής τιμές: «*$cfg['blowfish_secret'] = '';*», «*$cfg['Servers'][$i]['auth_type'] = 'config';*», «*$cfg['Servers'][$i]['user'] = 'root';*» και «*$cfg['Servers'][$i]['password'] = 'password_MySQL';*».

  Αυτή η μέθοδος αυθεντικοποίησης είναι λιγότερο ασφαλής, επειδή οι κωδικοί που χρησιμοποιούνται προκειμένου να επιτευχθεί η πρόσβαση στο MySQL Server, αποθηκεύονται στις παραμέτρους «*$cfg['Servers'][$i]['user']*» και «*$cfg['Servers'][$i]['password']*» του αρχείου «*config.inc.php*».

Σημείωση: Όταν ο χρήστης, πληκτρολογήσει την διεύθυνση «*http://localhost/phpMyAdmin*», στο «url» ενός φυλλομετρητή, στη προτροπή πιστοποίησης (authorization prompt) που θα εμφανιστεί, θα εισάγει για «*username*» την τιμή «root» και για «*password*» το κωδικό πρόσβασης που έχει πληκτρολογήσει στο βήμα 8 (Εικόνα 131) της εγκατάστασης του λογισμικού MySQL.

Τελευταίο Στάδιο Εγκατάστασης

Μετά την επανεκκίνηση του υπολογιστή, ο χρήστης πηγαίνει στο φάκελο «*τοπικός δίσκος:\www\Apache24\htdocs*», και δημιουργεί το αρχείο «*info.php*» (δεξί κλικ> Δημιουργία> Έγγραφο κειμένου), του οποίου το περιεχόμενο είναι «*<?php phpinfo(); ?>*». Στην συνέχεια, ο χρήστης ανοίγει έναν φυλλομετρητή και στο «url» πληκτρολογεί την διεύθυνση «*localhost/info.php*». Αν η PHP έχει εγκατασταθεί σωστά, ο χρήστης βλέπει μια σελίδα με πληροφορίες για τις εκδόσεις PHP, Apache κ.α. που χρησιμοποιεί (Εικόνα 146).

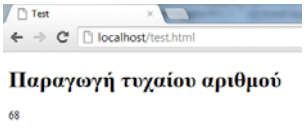


Εικόνα 146: Επιτυχημένη Εγκατάσταση της PHP

Για να βεβαιωθεί ο χρήστης, ότι ο μηχανισμός εκτέλεσης της PHP, διερμηνεύει τα αρχεία με επεκτάσεις «.php», «.phtml», «.html» και «.htm», δημιουργεί το αρχείο «*test.html*». Ακολουθεί ο κώδικας του αρχείου.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">


    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8"
/>
        <title>Test</title>
    </head>


    <body>
      <h1>Παραγωγή τυχαίου αριθμού</h1>


        <?php
            echo(mt_rand(0,100));
        ?>
    </body>


</html>
```

Στην συνέχεια ο χρήστης ανοίγει έναν φυλλομετρητή και στο «url» πληκτρολογεί την διεύθυνση «*localhost/test.html*». Αν η PHP και ο Apache έχουν εγκατασταθεί σωστά, τότε ο χρήστης βλέπει το αποτέλεσμα της Εικόνα 147.

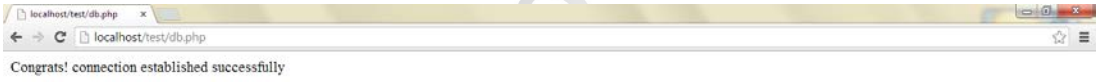


Εικόνα 147: Παραγωγή Τυχαίου Αριθμού με την Χρήση PHP

Για να βεβαιωθεί ο χρήστης, ότι υπάρχει πλήρη συνεργασία μεταξύ της MySQL και της PHP, δημιουργεί το αρχείο «*db.php*». Ακολουθεί ο κώδικας του αρχείου.

```
<?php
      $con = mysql_connect("localhost","root","my_password");
      if (!$con)
      {
         die('Could not connect: ' . mysql_error());
      }
      else
      {
         echo "Congrats! connection established successfully";
      }
      mysql_close($con);
?>
```

Στην συνέχεια ο χρήστης ανοίγει έναν φυλλομετρητή και στο «url» πληκτρολογεί την διεύθυνση «*localhost/db.php*». Αν η PHP και η MySQL συνεργάζονται σωστά, τότε ο χρήστης βλέπει το αποτέλεσμα της Εικόνα 148.



Εικόνα 148: Επιτυχημένη Σύνδεση στην Βάση Δεδομένων

Σημείωση: Όταν ο οποιοσδήποτε χρήστης θελήσει να εισάγει στα πεδία μιας βάσης, εγγραφές με ελληνικούς χαρακτήρες και όταν θέλει να επιστρέφονται σε αυτόν οι εγγραφές με ελληνικούς χαρακτήρες, τότε χρησιμοποιεί την γραμμή κώδικα «*mysql_query("SET NAMES 'utf8'",$con);*» κάτω από την γραμμή κώδικα «*$con=mysql_connect ($dbServer, $dbUser, $dbPass) or exit ("<h3>Cannot connect to database</h3>");*».

Κλείδωμα Φακέλων ή/και Αρχείων με Εισαγωγή «Ονόματος Χρήστη» και «Κωδικού» για Πρόσβαση

Ο οποιοσδήποτε χρήστης, εφόσον επιθυμεί να κλειδώσει φακέλους ή/και αρχεία και για την πρόσβαση σε αυτούς/αυτά να απαιτείται από το σύστημα εισαγωγή ονόματος χρήστη και κωδικού πρόσβασης, στην αρχή δημιουργεί ένα αρχείο, το οποίο περιέχει το όνομα χρήστη και τον κωδικό πρόσβασης.

Για να επιτευχθεί αυτό, ανοίγει ένα παράθυρο γραμμής εντολών ως διαχειριστής (Έναρξη> Όλα τα προγράμματα> Βοηθήματα> Γραμμή εντολών) και εκτελεί την εξής εντολή «*cd τοπικός δίσκος:\www\Apache24\bin*». Στην συνέχεια, με την εντολή «*htpasswd -c τοπικός δίσκος:\password\my_password_file myname*» δημιουργεί το αρχείο, το οποίο περιέχει το όνομα χρήστη και τον κωδικό πρόσβασης («*password*»: ο φάκελος στο οποίο θα βρίσκετε το αρχείο, «*my_password_file*»: το όνομα του αρχείου, «*myname*»: το όνομα

χρήστη που θα περιέχεται στο αρχείο). Στην συνέχεια, και όταν ζητηθεί, ο χρήστης εισάγει τον κωδικό πρόσβασης που θέλει να έχει.

Κατόπιν, προβαίνει στις ακόλουθες ενέργειες ανάλογα με το τι επιθυμεί να πράξει.

- *Διαδικασία κλειδώματος ενός φακέλου ή/και φακέλων*.

  Ο χρήστης, για να εφαρμόσει τη διαδικασία κλειδώματος σε ένα φάκελο, ανοίγει ένα κενό έγγραφο, π.χ. στο notepad, και αντιγράφει σε αυτό, το παρακάτω κώδικα.

```
AuthType Basic
AuthName "Please login first"
AuthUserFile τοπικός δίσκος:/password/my_password_file
<Limit GET POST PUT>
require valid-user
</Limit>
```

  Αποθηκεύει το αρχείο με το όνομα «*.htaccess*», στο «*root*» κατάλογο οποιουδήποτε φακέλου επιθυμεί να κλειδώσει. Ο χρήστης κατά την ονομασία του φακέλου, δεν πρέπει να ξεχάσει την τελεία στην αρχή. Επίσης, αν χρησιμοποιήσει το notepad για τη δημιουργία του αρχείου, τότε κατά την ονομασία του αρχείου, πρέπει να βάλει εισαγωγικά γύρω από το όνομα του (*".htaccess"*).

  Εφόσον, ο χρήστης επιθυμεί να εφαρμόσει τη διαδικασία κλειδώματος σε πολλούς φακέλους, οι οποίοι δεν εμπεριέχονται στον ίδιο φάκελο, αντιγράφει το αρχείο «*.htaccess*» στους «*root*» καταλόγους των φακέλων που επιθυμεί να προστατέψει.

- *Διαδικασία κλειδώματος ενός αρχείου*.

  Ο χρήστης, για να εφαρμόσει τη διαδικασία κλειδώματος σε ένα αρχείο, με την βοήθεια ενός κειμενογράφου, ανοίγει το αρχείο «*.htaccess*» και αντιγράφει σε αυτό, το παρακάτω κώδικα.

```
AuthType Basic
AuthName "Please login first"
AuthUserFile Τοπικός Δίσκος:/password/my_password_file
<Files "mypage.html">
  Require valid-user
</Files>
```

- *Διαδικασία κλειδώματος πολλών αρχείων*.

  Ο χρήστης, για να εφαρμόσει τη διαδικασία κλειδώματος σε πολλά αρχεία, με την βοήθεια ενός κειμενογράφου, ανοίγει το αρχείο «*.htaccess*» και αντιγράφει σε αυτό, το παρακάτω κώδικα.

```
AuthType Basic
AuthName "Please login first"
AuthUserFile Τοπικός Δίσκος:/password/my_password_file
<Files "mypage.html">
  Require valid-user
</Files>
<Files "myotherpage.html">
  Require valid-user
</Files>
```