ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

VULNERABILITY ASSESSMENT ΤΩΝ SERVERS UNIPI.GR & DTPS.UNIPI.GR

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΞΕΝΑΚΗΣ ΧΡΗΣΤΟΣ
ΦΟΙΤΗΤΗΣ: ΦΙΤΣΙΑΛΗΣ ΧΡΗΣΤΟΣ
Α.Μ: ΜΤΕ 0933

ΠΕΡΙΕΧΟΜΕΝΑ

1. SCANNING

Η διαδικασία αυτή αποσκοπεί στην εύρεση συστημάτων τα οποία είναι προσβάσιμα από το διαδίκτυο και δέχονται εισερχόμενη κίνηση από αυτό.

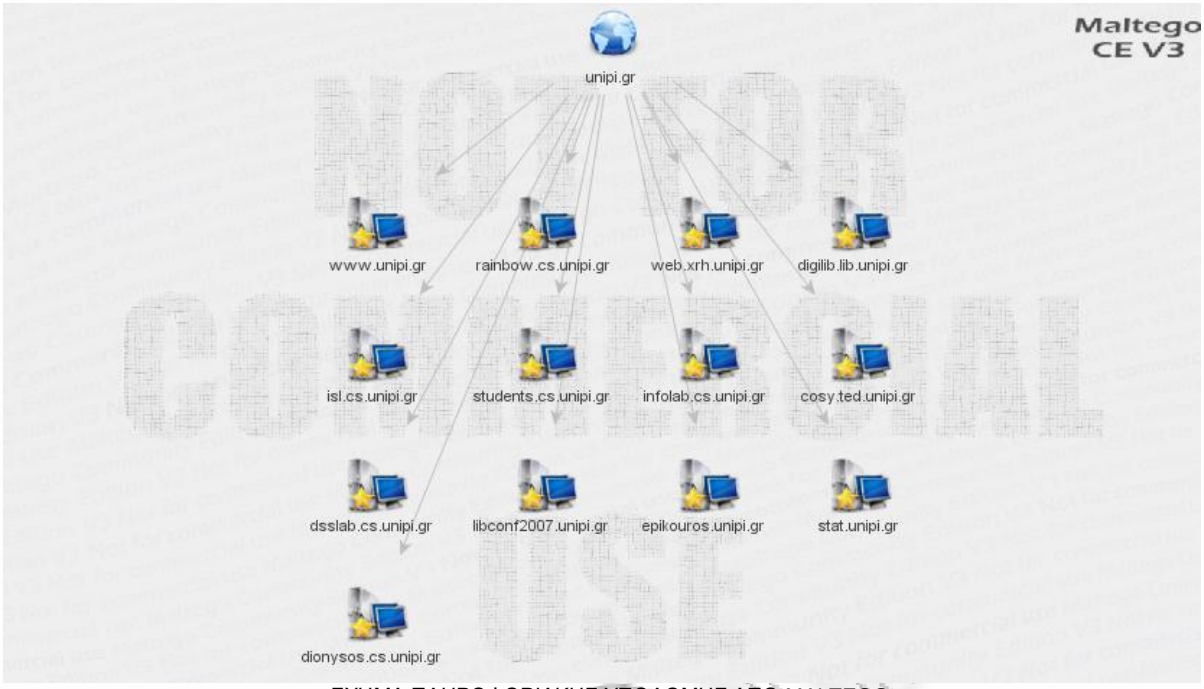
Στη παρούσα αναφορά παραθέτουμε τα αποτελέσματα της μεθοδολογίας που εφαρμόσαμε για να ανακαλύψουμε τη πληροφοριακή υποδομή του πανεπιστημίου Πειραιώς έτσι όπως μπορεί κάποιος να την αντιληφθεί από το εξωτερικό περιβάλλον (Internet). Εφόσον αποδείξαμε οτι το μοναδικό Domain Name που ανήκει ή χρησιμοποιεί το πανεπιστήμιο είναι το unipi.gr, το επόμενο βήμα ήταν να βρούμε την IP διεύθυνση που αντιστοιχεί σε αυτό το domain name. Συνοψίζωντας ακολουθήσαμε τα παρακάτω βήματα:

- Χαρτογράφηση του πανεπιστημίου στον ηλεκτρονικό κόσμο
- Εύρεση dns ονομάτων που ανήκουν στο πανεπιστήμιο
- Αντιστοίχιση dns ονομάτων σε IP διευθύνσεις

Εχουμε από το προηγούμενο βήμα ανακαλύψει ότι η IP διεύθυνση 195.251.229.6 αντιστοιχεί στο domain name unipi.gr. Σε αυτό το σημείο πρέπει να ελέγχθει εάν αυτή η IP διεύθυνση ανήκει στο πανεπιστήμιο Πειραιώς ή εάν το domain unipi.gr φιλοξενείται σε server άλλης εταιρείας. Αρκεί να πληκτρολογήσουμε την IP διεύθυνση σε ένα φυλλομετρητή ώστε να διαπιστώσουμε που θα συνδεθεί το σύστημα. Εκτελώντας τη διαδικασία αυτή διαπιστώνουμε ότι συνδεόμαστε στο site του πανεπιστημίου Πειαραιώς το οποίο σημαίνει ότι το domain unipi.gr φιλοξενείται σε server που διαχειρίζεται το ίδιο το πανεπιστήμιο. Εκτελέσαμε τη διαδικασία αυτή διότι αποτελεί κοινή πρακτική η φιλοξενία ιστοσελίδων σε τρίτους το οποίο καθορίζει σημαντικά τη μεθοδολογία που θα ακολουθηθεί.

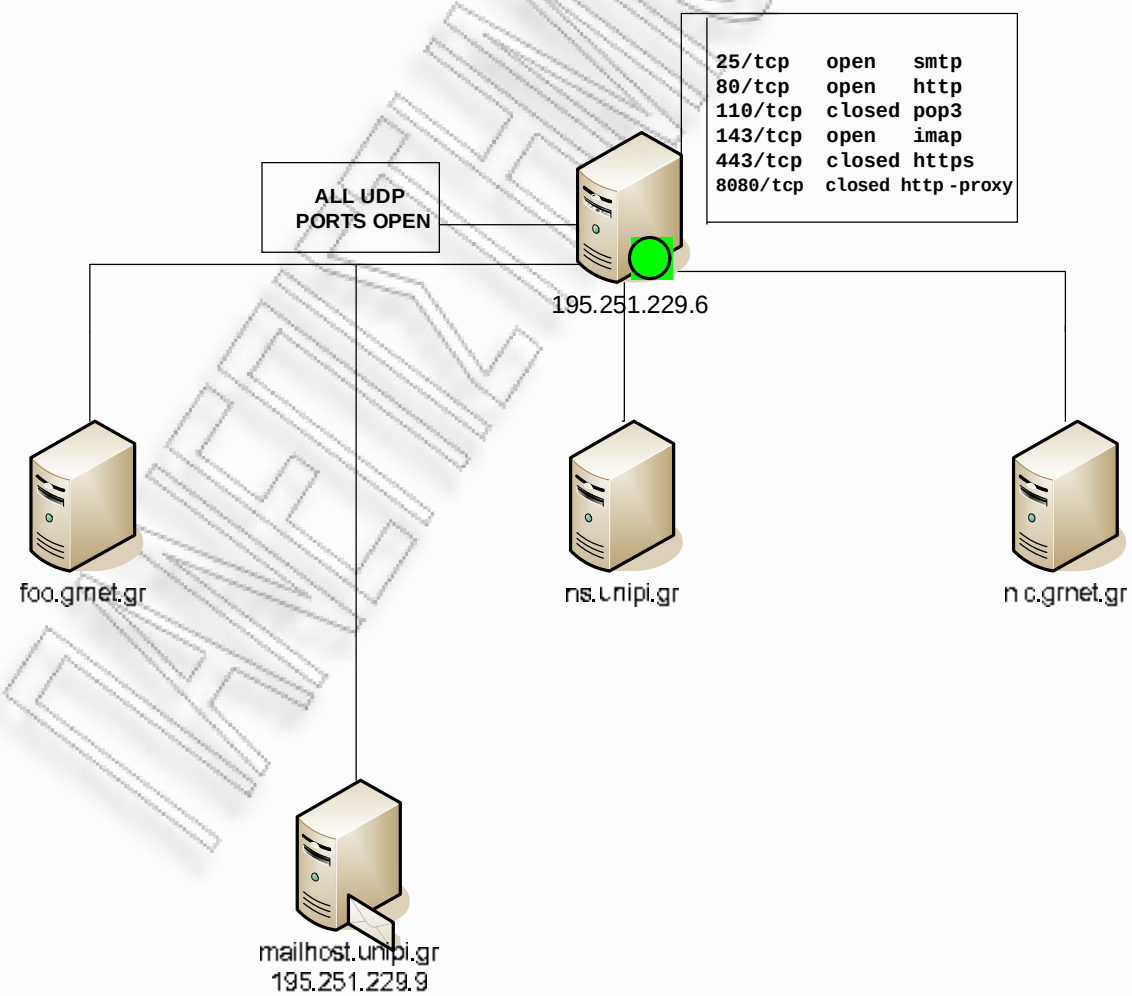
1.1 ΕΥΡΕΣΗ ΠΛΗΡΟΦΟΡΙΑΚΗΣ ΥΠΟΔΟΜΗΣ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ

Εφόσον πλέον έχουμε βρει την IP διεύθυνση που φιλοξενεί την ιστοσελίδα του πανεπιστημίου μπορούμε να προχωρήσουμε στην εύρεση και ανάλυση της πληροφοριακής υποδομής του. Η πληροφοριακή υποδομή φαίνεται σχηματικά παρακάτω.



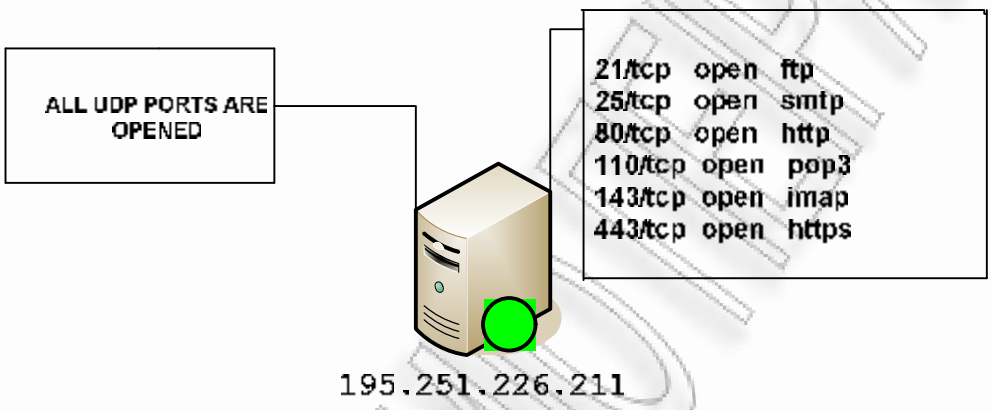
ΣΧΗΜΑ ΠΛΗΡΟΦΟΡΙΑΚΗΣ ΥΠΟΔΟΜΗΣ ΑΠΟ MALTEGO

1.2 ΥΠΗΡΕΣΙΕΣ



Υπηρεσίες που τρέχει ο server unipi.gr

Οπως παρατηρούμε από το παραπάνω σχήμα στο server unipi.gr με IP διεύθυνση 195.251.229.6 φιλοξενείται η ιστοσελίδα του πανεπιστημίου και υπάρχουν κάποια ανοικτά και κάποια κλειστά ports. Στα κλειστά ports δε διέρχεται καθόλου κίνηση και δεν τρέχει καμία υπηρεσία. Ετσι θα αναφερθούμε στα ανοικτά ports και τις υπηρεσίες που τρέχουν. Πιο αναλυτικά στα ports 25, 143 τρέχουν οι υπηρεσίες smtp, imap οι οποίες είναι υπεύθυνες για τη λειτουργία του ηλεκτρονικού ταχυδρομείου και γενικά για τη σωστή αποστολή και λήψη των e-mails. Στη port 80 τρέχει η υπηρεσία http η οποία είναι υπεύθυνη για την εξυπηρέτηση συνδέσεων προς την ιστοσελίδα του πανεπιστήμιου από απομακρυσμένα συστήματα. Τέλος όλες οι udp ports είναι ανοικτές και επιτρέπουν να περάσει κίνηση από αυτές χωρίς να τρέχει κάποια υπηρεσία ωστόσο. Παρακάτω παραθέτουμε σχηματικά τις υπηρεσίες που τρέχουν στο server dtps.unipi.gr.



Υπηρεσίες που τρέχει ο server dtps.unipi.gr

Στο server dtps.unipi.gr με IP διεύθυνση 195.251.229.211 φιλοξενείται το forum του τμήματος ψηφιακών συστημάτων. Πιο αναλυτικά στα ports 25,110,143 τρέχουν οι υπηρεσίες smtp, pop3, imap οι οποίες είναι υπεύθυνες για τη λειτουργία του ηλεκτρονικού ταχυδρομείου και γενικά για τη σωστή αποστολή και λήψη των e-mails. Στη port 21 τρέχει η υπηρεσία ftp η οποία χρησιμοποιείται για τη λήψη ή αποστολή αρχείων σε ftp servers. Στη port 80 τρέχει η υπηρεσία http η οποία αποτελεί τη βασική υπηρεσία ώστε να είναι εφικτές αιτήσεις για σύνδεση σε άλλα συστήματα. Τέλος όλες οι udp ports είναι ανοικτές και επιτρέπουν να περάσει κίνηση από αυτές χωρίς να τρέχει κάποια υπηρεσία ωστόσο.

1.3 ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα συμπεράσματα που προκύπτουν από την εφαρμογή των μεθόδων του συγκεκριμένου βήματος παρουσιάζονται συγκεντρωτικά παρακάτω:

- **Οι ανάγκες της πληροφοριακής υποδομής για ηλεκτρονικό ταχυδρομείο εξυπηρετούνται από τον mail server με ονομασία mailhost.unipi.gr και IP διεύθυνση 195.251.229.9. Η εξυπηρέτηση του συστήματος ονοματοδοσίας πραγματοποιείται από τρεις dns servers όπως φαίνεται από το παραπάνω σχήμα.**

- **Ο server unipi.gr και ο dtps.unipi.gr εξυπηρετούν ένα σύνολο από υπηρεσίες όπως διαδικτυακές συνδέσεις, ηλεκτρονικό ταχυδρομείο καθώς και ftp συνδέσεις.**

2. ENUMERATION

Στο βήμα αυτό γίνεται εντοπισμός ενεργών συνδέσεων στα συστήματα που ανακαλύφθηκαν από το προηγούμενο βήμα, καθώς και πληροφορίες που τα αφορούν όπως λογαριασμούς χρηστών, διαμοιραζόμενους πόρους, λογισμικό με γνωστές αδυναμίες ασφαλείας κτλ.

2.1 Εύρεση λειτουργικών συστημάτων

Στο βήμα αυτό θα προχωρήσουμε στη εύρεση των λειτουργικών συστημάτων τα οποία χρησιμοποιούνται στους προς μελέτη servers (unipi και dtps.unipi). Για το σκοπό αυτό θα κάνουμε χρήση του λογισμικού Nmap το οποίο δίνει τη δυνατότητα μέσω ενεργών συνδέσεων στο προς μελέτη server να ανακαλύψει το τύπο και την έκδοση του λειτουργικού συστήματος με μεγάλη ακρίβεια. Εκτελώντας το λογισμικό Nmap για τους δύο servers που μελετάμε λαμβάνουμε τις παρακάτω εξόδους του προγράμματος πρώτα για το server unipi και μετά για το dtps.unipi.

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-01-07 11:38 EET
Nmap scan report for spider.unipi.gr (195.251.229.6)
Host is up (0.0080s latency).
Not shown: 994 filtered ports
PORT     STATE  SERVICE    VERSION
25/tcp   open   smtp       Cisco PIX sanitized smtpd
80/tcp   open   http       Apache httpd 2.0.54 ((Unix) DAV/2)
110/tcp  closed pop3
143/tcp  open   imap       Courier Imapd (released 2005)
443/tcp  closed https
8080/tcp closed http-proxy
Device type: general purpose|WAP
Running (JUST GUESSING) : OpenBSD 4.X (87%), Sun Solaris 10 (87%), FreeBSD 6.X
(86%), Apple embedded (85%)
Aggressive OS guesses: OpenBSD 4.0 (87%), Sun Solaris 10 (87%), Sun Solaris 10
(SPARC) (87%), OpenBSD 4.3 (86%), FreeBSD 6.3-RELEASE (86%), FreeBSD 6.2-RELEASE
(85%), Apple AirPort Extreme WAP v7.3.2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Device: firewall

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.78 seconds
```

Οπως παρατηρούμε από την έξοδο του Nmap λαμβάνουμε με αρκετά μεγάλη ακρίβεια της τάξης του 88% ότι το λειτουργικό σύστημα που τρέχει στο server unipi είναι το OpenBSD 4.0. Σε γενικές γραμμές παρατηρούμε ότι η έξοδος υποδεικνύει πως το λειτουργικό σύστημα που χρησιμοποιείται είναι κάποιου τύπου Unix και αυτή τη πληροφορία θα χρησιμοποιήσει ένας επιτιθέμενος ώστε να ανακαλύψει αδυναμίες που να μπορεί να εκμεταλλευθεί. Στη πορεία κάνουμε την ίδια διαδικασία για το server dtps.unipi και λαμβάνουμε τη παρακάτω έξοδο. Σημαντική πληροφορία αποτελεί επίσης και ο τύπος του web server που εκτελέιται ώστε να εξυπηρετούνται συνδέσεις στη port 80 ο οποίος στη συγκεκριμένη περίπτωση είναι το Apache 2.0.54.

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-01-07 11:41 EET
Nmap scan report for dtps.unipi.gr (195.251.226.211)
Host is up (0.010s latency).
rDNS record for 195.251.226.211: dtps.ted.unipi.gr
Not shown: 994 filtered ports
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      PureFTPd
25/tcp  open  smtp     Cisco PIX sanitized smtpd
80/tcp  open  http     Apache httpd
110/tcp open  pop3     Courier pop3d
143/tcp open  imap     Courier Imapd (released 2008)
443/tcp open  ssl/http Apache httpd
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: firewall|WAP|general purpose|broadband router
Running (JUST GUESSING) : Check Point embedded (89%), Linux 2.4.X|2.6.X (89%),
Actiontec embedded (88%), OpenBSD 4.X (86%), FreeBSD 6.X (86%)
Aggressive OS guesses: Check Point ZoneAlarm Z100G firewall (89%), Check Point
UTM-1 Edge X firewall (89%), DD-WRT v23 (Linux 2.4.34) (89%), DD-WRT v24 SP2
(Linux 2.4.36) (89%), Linux 2.6.23 (89%), Tomato 1.27 (Linux 2.4.20) (88%),
Actiontec GT701 DSL modem (88%), OpenBSD 4.0 (86%), FreeBSD 6.2-RELEASE (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Device: firewall

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.38 seconds
```

Η συγκεκριμένη περίπτωση παρουσιάζει ιδαίτερο ενδιαφέρον καθώς η έξοδος του προγράμματος φανερώνει πως ο συκγκεριμένος server επιτελεί λειτουργίες firewall και δρομολογητή. Γι' αυτό το λόγο και ως λειτουργικό σύστημα παρουσιάζεται ταυτόχρονα και το OpenBSD 4.0 αλλά και το firewall το οποίο χρησιμοποιείται στο συγκεκριμένο server. Ομοίως όπως και στο server unipi έτσι και εδώ ο web server που χρησιμοποιείται είναι ο Apache.

2.2 Εύρεση banners των υπηρεσιών

Μία ακόμα πληροφορία που μπορούμε να εξάγουμε πολύ εύκολα αποτελεί το banner της υπηρεσίας που τρέχει σε μία συγκεκριμένη port. Το banner αποτελεί την απάντηση της υπηρεσίας σε συγκεκριμένες αιτήσεις και αποκαλύπτει το είδος και την έκδοση της υπηρεσίας. Μέσω telnet μπορούμε να ανακαλύψουμε τις παραπάνω πληροφορίες από τις υπηρεσίες που τρέχουν στο server dtps.unipi. Έτσι έχουμε:

- **Port 21 / ftp → Banner: Pure-FTPd [privsep] [TLS]**
- **Port 25 / smtp → Banner: Not available**
- **Port 80 / http → Banner: ApachePowered–By: PHP/5.3.3**
- **Port 110 / pop3 → Banner: Not available**
- **Port 143 / imap → Banner: Courier-Imap**
- **Port 443 / https → Banner: ?xml version=1.0 encoding=ISO-8859-1**

Κάνοντας το ίδιο για το server unipi εξάγουμε τη παρακάτω πληροφορία:

- **Port 25 / smtp → Banner: ***********
- **Port 80 / http → Banner: Apache/2.0.54(Unix) DAV/2**
- **Port 143 / imap → Banner: Courier-Imap**
- **Port 8080 / http-proxy → Banner: squid/3.0 STABLE9 Version: 1.0**

2.3 Εύρεση άλλων πόρων

Στο σημείο αυτό πρέπει να αναφερθεί ότι δε κατέστη δυνατή η εύρεση άλλων πόρων όπως λογαριασμούς χρηστών ή διαμοιραζόμενων δικτυακών πόρων. Τα εργαλεία που χρησιμοποιήθηκαν δεν επέστρεψαν κανένα δεδομένο. Πιθανοί λόγοι για αυτό είναι είτε διότι τέτοιοι πόροι δεν υπάρχουν είτε δεν είναι προσβάσιμοι από το διαδίκτυο. Τέλος, ένας πιθανός λόγος μπορεί να είναι το γεγονός ότι οι ρυθμίσεις ασφαλείας δεν επιτρέπουν την αποκάλυψη αυτών των πόρων με τις γνωστές και περισσότερο χρησιμοποιούμενες μεθόδους.

3. ΑΝΑΛΥΣΗ ΑΔΥΝΑΜΙΩΝ ΣΥΣΤΗΜΑΤΩΝ

3.1 Ανάλυση αδυναμιών του λογισμικού των servers.

Με βάση την έξοδο του λογισμικού nmap γνωρίζουμε ότι με μεγάλη πιθανότητα το λειτουργικό σύστημα που τρέχει στο server unipi είναι το OpenBSD 4.0. Ακολουθούν με μικρότερη πιθανότητα και άλλα λειτουργικά ίδιου τύπου δηλαδή τύπου UNIX με μικρότερη πιθανότητα αλλά όχι με διαφορά από το πρώτο. Ετσι ένας επιτιθέμενος έχει ένα μικρό έυρος λειτουργικών συστημάτων ίδιου τύπου με βάση τα οποία μπορεί να ξεκινήσει την έρευνα του για αδυναμίες. Αυτό που έχει σημασία είναι το γεγονός ότι οποιοδήποτε από τα λειτουργικά που αναφέρεται στην έξοδο του nmap βρίσκεται σε έκδοση ξεπερασμένη. Αυτό σημαίνει πως για έναν επιτιθέμενο είναι πολύ εύκολο να βρει ένα σύνολο αδυναμιών οι οποίες θα έχουν διορθωθεί σε επόμενες εκδόσεις του ίδιου λειτουργικού.

Μέσω διαφόρων μεθόδων είναι δυνατό να γίνει χρήση αυτών των αδυναμιών (exploitation). Αυτό μπορεί να έχει σαν αποτέλεσμα ανεπανόρθωτες ζημιές και στο πληροφοριακό σύστημα αλλά και στο ίδιο το πανεπιστήμιο.

Η πιο κοινή και δημοφιλής μέθοδος είναι με την χρήση exploits, τα οποία ουσιαστικά είναι ένα μικρό τμήμα κώδικα ή εντολών τα οποία εκμεταλεύονται μια αδυναμία, ένα προγραμματιστικό κενό, μια δυσλειτουργία ή κάτι που δεν εχει ληφθεί υπόψη στο λειτουργικό σύστημα,το λογισμικό ή και το υλικό (hardware) για το οποίο είναι φτιαγμένα να επιτεθούν. Κύριος σκοπός των exploits είναι η απόκτηση του απόλυτου ελέγχου του επιτιθέμενου στο σύστημα (η αύξηση των δικαιωμάτων που έχει ως χρήστης (privilege escalation) και η άρνηση παροχής υπηρεσιών (DDOS - Denial of Service Attack).

Με μία σύντομη αναζήτηση στο διαδίκτυο είναι δυνατό να βρεθούν μεγάλες βιβλιοθήκες με exploits, οι οποίες ενημερώνονται καθημερινά με καινούργια exploits που εκμεταλευονται προσφάτως ανακαλυφθήσες αδυναμίες και είναι δωρεάν το να τα κατεβάσει κανείς. Ενώ οι πλατφόρμες με τις οποίες μπορεί να εκτελεστεί ένα exploit και να επιτεθεί μέσω του διαδικτύου ή και τοπικού δικτύου είναι open source με τεράστια υποστηρικτική κοινότητα και ανοιχτό εκπαιδευτικό υλικό για τη χρήση τους. Αντιλαμβανόμαστε έτσι ότι οποιοδήποτε out-of-date σύστημα από το θέμα της ασφάλειας είναι εύκολος στόχος για κάποιον κακόβουλο ο οποίος γνωρίζει να χρησιμοποιεί exploits.

Τα ίδια ισχύουν και για το server dtps.unipi όπου έχουμε αποκάλυψη hardware που χρησιμοποιείται με το λογισμικό που αυτό τρέχει. Με μια απλή αναζήτηση ένας επιτιθέμενος μπορεί εύκολα να αποκτήσει πρόσβαση σε βάσεις δεδομένων οι οποίες περιέχουν exploits για αυτό το λογισμικό. Χρησιμοποιώντας αυτά τα exploits ο επιτιθέμενος μπορεί να εκμεταλλευτεί τυχόν αδυναμίες του λογισμικού οι οποίες δεν έχουν διορθωθεί.

3.2 Ανάλυση αδυναμιών με το λογισμικό OpenVAS

Στη συνέχεια κάνοντας χρήση του εξειδικευμένου λογισμικού OpenVas ελέγξαμε τους προς μελέτη servers για τυχόν αδυναμίες, τις σημαντικότερες εκ των οποίων θα παρουσιάσουμε στη πορεία. Τρέχουμε το συγκεκριμένο λογισμικό για το server dtps.unipi του οποίου η έξοδος παρουσιάζεται παρακάτω:

Summary

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan started at: Sun Jan 16 12:56:09 2011
Scan finished at: Sun Jan 16 13:21:28 2011

Host	Possible Issues	Holes	Warnings	Notes	False Positives
dtps.unipi.gr	Security hole(s) found	3	4	12	0
Total: 1		3	4	12	0

Reports per Host

dtps.unipi.gr

Scan of this host started at: Sun Jan 16 12:56:09 2011
Scan of this host finished at: Sun Jan 16 13:21:28 2011

Service (Port)	Issue regarding port
ssh (22/tcp)	Security note(s) found
http (80/tcp)	Security hole(s) found
general/SMBClient	No Information
smtp (25/tcp)	Security hole(s) found
ftp (21/tcp)	Security note(s) found
general/tcp	Security note(s) found
ldap (389/tcp)	No Information

[return to summary]

Security Issues and Fixes - Host dtps.unipi.gr

dtps.unipi.gr - ssh (22/tcp)

Informational
no key given for SLAD checks. SLAD checks will be disabled. OID : 1.3.6.1.4.1.25623.1.0.90002
Informational
no key given for SLAD checks. SLAD checks will be disabled. OID : 1.3.6.1.4.1.25623.1.0.90003

[return to dtps.unipi.gr]

dtps.unipi.gr - http (80/tcp)

Vulnerability
The remote host is running Invision Power Board - a CGI suite designed to set up a bulletin board system on the remote web server. A vulnerability has been discovered in the sources/calendar.php file that allows unauthorized users to inject SQL commands. An attacker may use this flaw to gain the control of the remote database Solution : Upgrade to the latest version of this software. See also : http://www.invisionboard.com/download/index.php?act=dl&s=1&id=12&p=1 Risk factor : High BID : 9232 OID : 1.3.6.1.4.1.25623.1.0.11977
Vulnerability
The remote host is running a version of Kayako eSupport which is vulnerable to a SQL injection vulnerability as well as a cross site scripting. Solution : Upgrade to the newest version of this software Risk factor : High CVE : CAN-2004-1412, CAN-2004-1413 BID : 12037 OID : 1.3.6.1.4.1.25623.1.0.16022
Warning

Overview:

Turnkey eBook Store is prone to a cross-site scripting vulnerability.

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site and to steal cookie-based authentication credentials.

Turnkey eBook Store 1.1 is vulnerable; other versions may also be affected.

Risk factor : Medium
BID : 34324
OID : 1.3.6.1.4.1.25623.1.0.100098

Warning

The remote server is running a version of PsNews (a content management system) which is older than 1.2.

This version is affected by multiple cross-site scripting flaws. An attacker may exploit these to steal the cookies from legitimate users of this website.

Solution : Upgrade to a newer version.
Risk factor : Medium

CVE : CVE-2004-1665
BID : 11124
OID : 1.3.6.1.4.1.25623.1.0.14685

Warning

The remote host is running PHProxy, a web HTTP proxy written in PHP.

There is a bug in the remote version software which makes it vulnerable to HTML and JavaScript injection.

An attacker may use this bug to preform web cache poisoning, xss attack, etc.

Solution : Upgrade to the newest version of this software
Risk factor : Medium
BID : 12115
OID : 1.3.6.1.4.1.25623.1.0.16069

Warning

The remote web server seems to be vulnerable to a format string attack on HTTP 1.0 header value.
An attacker might use this flaw to make it crash or even execute arbitrary code on this host.

Solution : upgrade your software or contact your vendor and inform him of this vulnerability

Risk factor : High
OID : 1.3.6.1.4.1.25623.1.0.15642

Informational

The remote web server type is :

Apache

and the 'ServerTokens' directive is ProductOnly
Apache does not permit to hide the server type.

OID : 1.3.6.1.4.1.25623.1.0.10107

Informational

An information leak occurs on Apache based web servers
whenever the UserDir module is enabled. The vulnerability allows an external
attacker to enumerate existing accounts by requesting access to their home
directory and monitoring the response.

Solution:
1) Disable this feature by changing 'UserDir public_html' (or whatever) to
'UserDir disabled'.

Or

2) Use a RedirectMatch rewrite rule under Apache -- this works even if there
is no such entry in the password file, e.g.:

RedirectMatch ^/~(.*)$ http://my-target-webserver.somewhere.org/$1

Or

3) Add into httpd.conf:
ErrorDocument 404 http://localhost/sample.html
ErrorDocument 403 http://localhost/sample.html
(NOTE: You need to use a FQDN inside the URL for it to work properly).

Additional Information:
http://www.securiteam.com/unixfocus/5WP0C1F5FI.html

Risk factor : Low
CVE : CAN-2001-1013
BID : 3335
OID : 1.3.6.1.4.1.25623.1.0.10766

Informational

Overview:
This host is running IP.Board, an outstanding bulletin board system.

See also:
http://www.invisionpower.com/community/board/

Risk factor : None

IP.Board Version '1.3 Final' was detected on the remote host in the following directory(s):

/forum

OID : 1.3.6.1.4.1.25623.1.0.100107

Informational

The following directories were discovered:
/bak, /includes, /wwwstat, /wwwstats, /~admin, /~stats, /~webstats, /1, /10, /2, /3, /4, /5, /6, /7, /8, /9, /Agent, /Agents, /Album, /CS, /CVS, /DMR, /DocuColor, /GXApp, /HB, /HBTemplates, /IBMWebAS, /JBookIt, /Log, /Msword, /NSearch, /NetDynamic, /NetDynamics, /ROADS, /SilverStream, /Templates, /WebBank, /WebDB, /WebShop, /Web_store, /XSL, /_ScriptLibrary, /_derived, /_fpclass, /_mem_bin, /_notes, /_objects, /card, /cart, /cash, /caspsamp, /catalog, /cd, /cdrom, /ce_html, /cert, /certificado, /cfappman, /cfdocs, /cliente, /clientes, /cm, /cmsample, /cobalt-images, /code, /comments, /communicator, /compra, /compras, /compressed, /conecta, /conf, /connect, /console, /controlpanel, /corp, /correo, /counter, /cron, /crons, /crypto, /csr, /css, /cuenta, /currency, /cvsweb, /cybercash, /d, /darkportal, /dat, /error, /fcgi-bin, /filemanager, /files, /foldoc, /form, /form-totaller, /formsmgr, /forum, /forums, /fotos, /fpadmin, /fpdb, /fpsample, /framesets, /ftproot, /g, /gfx, /grocery, /guest, /guestbook, /guests, /help, /hide, /hit_tracker, /hitmatic, /hostingcontroller, /ht, /html, /hyperstat, /ibank, /icons, /idea, /ideas, /imagenes, /imagery, /images, /img, /imp, /impreso, /inc, /shell-cgi, /shipping, /shop, /site, /siteminder, /siteminderagent, /siteserver, /sitestats, /siteupdate, /smreportsviewer, /soapdocs, /software, /solaris, /source, /sql, /src, /staff, /stats-bin-p, /status, /storage, /store, /stronghold-status, /style, /styles, /stylesheet, /subir, /sun, /support, /supporter, /system, /tar, /tech, /technote

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

Other references : OWASP:OWASP-CM-006

OID : 1.3.6.1.4.1.25623.1.0.11032

Informational

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

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. See also :

http://www.kb.cert.org/vuls/id/867593

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Plugin output :

Solution :

Add the following lines for each virtual host in your configuration file :

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

CVE : CVE-2004-2320
BID : 9506, 9561, 11604
OID : 1.3.6.1.4.1.25623.1.0.11213

[return to dtps.unipi.gr]

dtps.unipi.gr - smtp (25/tcp)

Vulnerability

The remote SMTP server crashes when it is send a command

with a too long argument.

A cracker might use this flaw to kill this service or worse,
execute arbitrary code on your server.

Solution : upgrade your MTA or change it.

Risk factor : High
OID : 1.3.6.1.4.1.25623.1.0.11772

Informational

Remote SMTP server banner :
220 **********

OID : 1.3.6.1.4.1.25623.1.0.10263

[return to dtps.unipi.gr]

dtps.unipi.gr - ftp (21/tcp)

Informational

Remote FTP server banner :
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 14:01. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 15 minutes of inactivity.

OID : 1.3.6.1.4.1.25623.1.0.10092

[return to dtps.unipi.gr]

dtps.unipi.gr - general/tcp

Informational

ICMP based OS fingerprint results:

Linux Kernel 2.6.11 (accuracy 91%) Linux Kernel 2.6.10 (accuracy 91%) Linux Kernel 2.6.9 (accuracy 91%) Linux Kernel 2.6.8 (accuracy 91%) Linux
Kernel 2.6.7 (accuracy 91%) Linux
Kernel 2.6.6 (accuracy 91%) Linux
Kernel 2.6.5 (accuracy 91%) Linux
Kernel 2.6.4 (accuracy 91%) Linux
Kernel 2.6.3 (accuracy 91%) Linux
Kernel 2.6.2 (accuracy 91%) Linux
Kernel 2.6.1 (accuracy 91%) Linux
Kernel 2.6.0 (accuracy 91%) Linux
Kernel 2.4.30 (accuracy 91%) Linux
Kernel 2.4.29 (accuracy 91%) Linux
Kernel 2.4.28 (accuracy 91%) Linux
Kernel 2.4.27 (accuracy 91%) Linux
Kernel 2.4.26 (accuracy 91%)
Linux Kernel 2.4.25 (accuracy 91%)
Linux Kernel 2.4.24 (accuracy 91%)
Linux Kernel 2.4.23 (accuracy 91%)
Linux Kernel 2.4.22 (accuracy 91%)
Linux Kernel 2.4.21 (accuracy 91%)
Linux Kernel 2.4.20 (accuracy 91%)
Linux Kernel 2.4.19 (accuracy 91%)
Linux Kernel 2.0.36 (accuracy 91%)
Linux Kernel 2.0.34 (accuracy 91%)
Linux Kernel 2.0.30 (accuracy 91%)

OID : 1.3.6.1.4.1.25623.1.0.102002

Informational

Nikto could not be found in your system path.
OpenVAS was unable to execute Nikto and to perform the scan you requested.
Please make sure that Nikto is installed and that nikto.pl or nikto is available in the PATH variable defined for your environment.
OID : 1.3.6.1.4.1.25623.1.0.14260

Informational

Information about this scan :

OpenVAS version : 2.0.2
Scanner IP : 192.168.0.8
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : no
Max hosts : 20
Max checks : 4
Scan duration : unknown (ping_host.nasl not launched?)

OID : 1.3.6.1.4.1.25623.1.0.19506

[return to dtps.unipi.gr]

Appendix: NVT Information

NVT 1.3.6.1.4.1.25623.1.0.11772: Generic SMTP overflows

Summary Tries overflows on SMTP commands arguments
Category destructive_attack
Family SMTP problems
Version $Revision: 3477 $
Signed by not signed

Description

The remote SMTP server crashes when it is send a command
with a too long argument.

A cracker might use this flaw to kill this service or worse,
execute arbitrary code on your server.

Solution : upgrade your MTA or change it.

Risk factor : High

NVT 1.3.6.1.4.1.25623.1.0.14260: Nikto (NASL wrapper)

Summary Assess web server security with Nikto
Category infos
Family CGI abuses
Version 1.6
Signed by not signed

Description

This plugin uses nikto(1) to find weak CGI scripts
and other known issues regarding web server security.
See the preferences section for configuration options.

Risk factor : None

Parameters

Force scan even without 404s no

NVT 1.3.6.1.4.1.25623.1.0.90002: SLAD Run

Summary Connects to SLAD to tun programs remotely
Category infos
Family SLAD
Version 1.0
Signed by not signed

Description

This script connects to SLAD on a remote host to run
remote scanners.
To work properly, this script requires to be provided
with a valid SSH login by means of an SSH key with pass-
phrase if the SSH public key is passphrase-protected, or
a password to log in.

NVT 1.3.6.1.4.1.25623.1.0.19506: Information about the scan

Summary Displays information about the scan
Category end
Family General
Version $Revision: 3059 $
Signed by not signed

Description

This script displays, for each tested host, information about the scan itself:

- The version of the plugin set
- The type of plugin feed (Direct, Registered or GPL)
- The version of the OpenVAS Engine
- The port scanner(s) used
- The port range scanned
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.90003: SLAD Fetch Results

Summary Connects to SLAD to fetch installed plugins
Category infos **Family** SLAD **Version** 1.0
Signed by not signed

Description

This script connects to SLAD on a remote host to fetch the result from scripts started earlier.
To work properly, this script requires to be provided
with a valid SSH login by means of an SSH key with pass- phrase if the SSH public key is
passphrase-protected, or
a password to log in.

NVT 1.3.6.1.4.1.25623.1.0.11977: Invision Power Board Calendar SQL Injection Vulnerability

Summary Detect Invision Power Board Calender SQL Injection

Category infos **Family** CGI abuses **Version** $Revision: 38 $

BID 9232

Signed by not signed

Description

The remote host is running Invision Power Board - a CGI suite designed to set up a bulletin board system on the remote web server.

A vulnerability has been discovered in the sources/calendar.php file that allows unauthorized users to inject SQL commands.

An attacker may use this flaw to gain the control of the remote database

Solution : Upgrade to the latest version of this software.

See also : http://www.invisionboard.com/download/index.php?act=dl&s=1&id=12&p=1

Risk factor : High

NVT 1.3.6.1.4.1.25623.1.0.11032: Directory Scanner

Summary Directory Scanner

Category infos

Family Misc.

Version $Revision: 38 $

XRefs OWASP:OWASP-CM-006

Signed by not signed

Description

This plugin attempts to determine the presence of various common dirs on the remote web server

NVT 1.3.6.1.4.1.25623.1.0.10263: SMTP Server type and version

Summary SMTP Server type and version

Category infos

Family General

Version $Revision: 118 $

Signed by not signed

Description

This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.
Solution: Change the login banner to something generic.

Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.15642: Format string on HTTP header value

Summary Sends an HTTP request with %s inside a HTTP header
Category destructive_attack
Family Gain root remotely
Version $Revision: 3475 $
Signed by not signed

Description

The remote web server seems to be vulnerable to a format string attack on HTTP 1.0 header value.
An attacker might use this flaw to make it crash or even execute arbitrary code on this host.

Solution : upgrade your software or contact your vendor and inform him of this vulnerability

Risk factor : High

NVT 1.3.6.1.4.1.25623.1.0.10107: HTTP Server type and version

Summary HTTP Server type and version
Category infos
Family General
Version $Revision: 38 $
Signed by not signed

Description

This detects the HTTP Server's type and version.

Solution: Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display'
Be sure to remove common logos like apache_pb.gif.
With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.10766: Apache UserDir Sensitive Information Disclosure

Summary Apache UserDir Sensitive Information Disclosure
Category infos
Family Misc.

Version $Revision: 3429 $
CVE CAN-2001-1013
BID 3335
Signed by not signed

Description

An information leak occurs on Apache based web servers
whenever the UserDir module is enabled. The vulnerability allows an external
attacker to enumerate existing accounts by requesting access to their home
directory and monitoring the response.

Solution:
1) Disable this feature by changing 'UserDir public_html' (or whatever) to
'UserDir disabled'.

Or

2) Use a RedirectMatch rewrite rule under Apache -- this works even if there
is no such entry in the password file, e.g.:
RedirectMatch ^/~(.*)$ http://my-target-webserver.somewhere.org/$1

Or

3) Add into httpd.conf:
ErrorDocument 404 http://localhost/sample.html
ErrorDocument 403 http://localhost/sample.html
(NOTE: You need to use a FQDN inside the URL for it to work properly).

Additional Information:
http://www.securiteam.com/unixfocus/5WP0C1F5FI.html

Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.11213: http TRACE XSS attack

Summary http TRACE XSS attack
Category infos
Family CGI abuses : XSS
Version $Revision: 38 $
CVE CVE-2004-2320
BID 9506, 9561, 11604
Signed by not signed

Description

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

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. See also :

http://www.kb.cert.org/vuls/id/867593

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

NVT 1.3.6.1.4.1.25623.1.0.102002: OS fingerprinting

Summary Detects remote operating system version
Category infos
Family Service detection
Version 1.0.0
Signed by not signed

Description

This script performs ICMP based OS fingerprinting (as described by Ofir Arkin and Fyodor Yarochkin in Phrack #57). It can be used to determine remote operating system version.

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

Risk factor: None

NVT 1.3.6.1.4.1.25623.1.0.14685: PsNews XSS

Summary check PsNews XSS flaws
Category infos

Family CGI abuses : XSS **Version** $Revision: 3476 $ **CVE** CVE-2004-1665
BID 11124

Signed by not signed

Description

The remote server is running a version of PsNews (a content management system) which is older than 1.2.

This version is affected by multiple cross-site scripting flaws. An attacker may exploit these to steal the cookies from legitimate users of this website.

Solution : Upgrade to a newer version.
Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.16069: PHProxy XSS

Summary Checks for the presence of a PHProxy XSS
Category attack
Family CGI abuses : XSS
Version $Revision: 3476 $
BID 12115
Signed by not signed

Description

The remote host is running PHProxy, a web HTTP proxy written in PHP.

There is a bug in the remote version software which makes it vulnerable to HTML and JavaScript injection.

An attacker may use this bug to preform web cache poisoning, xss attack, etc.

Solution : Upgrade to the newest version of this software
Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.16022: Kayako eSupport SQL Injection and Cross-Site-Scripting

Summary Checks for the presence of an SQL and XSS in Kayako
Category attack
Family CGI abuses : XSS
Version $Revision: 3475 $
CVE CAN-2004-1412, CAN-2004-1413
BID 12037
Signed by not signed

Description

The remote host is running a version of Kayako eSupport which is vulnerable

to a SQL injection vulnerability as well as a cross site scripting.

Solution : Upgrade to the newest version of this software
Risk factor : High

NVT 1.3.6.1.4.1.25623.1.0.100107: IP.Board Detection

Summary Checks for the presence of IP.Board
Category infos
Family Service detection
Version 1.1
Signed by not signed

Description

Overview:
This host is running IP.Board, an outstanding bulletin board system.

See also:
http://www.invisionpower.com/community/board/

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.100098: Turnkey eBook Store 'keywords' Parameter Cross Site Scripting Vulnerability

Summary Determine if Turnkey eBook Store is prone to Cross Site Scripting vulnerabilitie
Category infos
Family Web application abuses
Version 1.0
BID 34324
Signed by not signed

Description

Overview:

Turnkey eBook Store is prone to a cross-site scripting vulnerability.

An attacker may leverage this issue to execute arbitrary script code
in the browser of an unsuspecting user in the context of the affected
site and to steal cookie-based authentication credentials.

Turnkey eBook Store 1.1 is vulnerable
other versions may also be
affected.

Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.10092: FTP Server type and version

Summary FTP Server type and version
Category infos
Family General
Version $Revision: 38 $
Signed by not signed

Description

This detects the FTP Server type and version by connecting to the server and processing the buffer received.
The login banner gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Solution: Change the login banner to something generic.

Risk factor : Low

Κάνοντας το ίδιο και για το server unipi.grλαμβάνουμε τη παρακάτω έξοδο:

Summary

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan started at: Sun Jan 16 12:30:15 2011
Scan finished at: Sun Jan 16 12:51:03 2011

Host	Possible Issues	Holes	Warnings	Notes	False Positives
www.unipi.gr	Security warning(s) found	0	3	11	0
Total: 1		0	3	11	0

Reports per Host

www.unipi.gr

Scan of this host started at: Sun Jan 16 12:30:15 2011
Scan of this host finished at: Sun Jan 16 12:51:03 2011

Service (Port)	Issue regarding port
ssh (22/tcp)	Security note(s) found
http (80/tcp)	Security warning(s) found
general/SMBClient	No Information
smtp (25/tcp)	Security note(s) found
general/tcp	Security note(s) found
ldap (389/tcp)	No Information

[return to summary]

Security Issues and Fixes - Host www.unipi.gr

www.unipi.gr - ssh (22/tcp)

Informational
no key given for SLAD checks. SLAD checks will be disabled. OID : 1.3.6.1.4.1.25623.1.0.90002
Informational
no key given for SLAD checks. SLAD checks will be disabled. OID : 1.3.6.1.4.1.25623.1.0.90003

[return to www.unipi.gr]

www.unipi.gr - http (80/tcp)

Warning
The following files are calling the function phpinfo() which

disclose potentially sensitive information to the remote attacker :
/phpinfo.php

Solution : Delete them or restrict access to them
Risk factor : Low
OID : 1.3.6.1.4.1.25623.1.0.11229

Warning

Overview : The host is running Apache, which is prone to cross-site scripting vulnerability.

Vulnerability Insight :

Input passed to the module mod_proxy_ftp with wildcard character is not properly sanitized before returning to the user.

Impact : Remote attackers can execute arbitrary script code.

Impact Level : Application

Affected Software/OS :
Apache 2.0.0 to 2.0.63 and Apache 2.2.0 to 2.2.9 on All Platform

***
Note: The script might report a False Positive as it is only checking for the vulnerable version of Apache. Vulnerability is only when mod_proxy and mod_proxy_ftp is configured with the installed Apache version.
***

Fix : Fixed is available in the SVN repository,
http://svn.apache.org/viewvc?view=rev&revision=682871
http://svn.apache.org/viewvc?view=rev&revision=682868

References : http://httpd.apache.org/
http://www.securityfocus.com/archive/1/495180
http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

CVSS Score :
CVSS Base Score : 5.8 (AV:N/AC:M/Au:NR/C:P/I:P/A:N)
CVSS Temporal Score : 4.5
Risk factor : Medium
CVE : CVE-2008-2939
BID : 30560
OID : 1.3.6.1.4.1.25623.1.0.900107

Warning

Overview: This host is running Apache Web Server and is prone to Information Disclosure Vulnerability.

Vulnerability Insight:
This flaw is caused due to an error in 'mod_proxy_ajp' when handling

improperly malformed POST requests.

Impact:
Successful exploitation will let the attacker craft a special HTTP POST request and gain sensitive information about the web server.

Impact level: Application

Affected Software/OS:
Apache HTTP Version 2.2.11

Workaround:
Update mod_proxy_ajp.c through SVN Repository (Revision 767089)
http://www.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff

Fix: No solution or patch is available as on 29th April, 2009. Information regarding this issue will be updated once the solution details are available.
For further updates refer, http://httpd.apache.org/download.cgi

References:
http://secunia.com/advisories/34827
http://xforce.iss.net/xforce/xfdb/50059
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=766938&r2=767089

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:P/I:N/A:N)
CVSS Temporal Score : 4.0
Risk factor: Medium
CVE : CVE-2009-1191
BID : 34663
OID : 1.3.6.1.4.1.25623.1.0.900499

Informational

The remote web server type is :

Apache/2.0.54 (Unix) DAV/2

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
OID : 1.3.6.1.4.1.25623.1.0.10107

Informational

The following directories were discovered:
/cgi-bin, /testing, /Templates, /helpdesk, /icons, /images, /search

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

Other references : OWASP:OWASP-CM-006
OID : 1.3.6.1.4.1.25623.1.0.11032

Informational

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

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. See also :

http://www.kb.cert.org/vuls/id/867593

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Plugin output :

Solution :
Add the following lines for each virtual host in your configuration file :

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

CVE : CVE-2004-2320
BID : 9506, 9561, 11604
OID : 1.3.6.1.4.1.25623.1.0.11213

[return to www.unipi.gr]

www.unipi.gr - smtp (25/tcp)

Informational
Remote SMTP server banner : 220 **********
OID : 1.3.6.1.4.1.25623.1.0.10263
Informational

Some antivirus scanners dies when they process an email with a
too long string without line breaks.
Such a message was sent. If there is an antivirus on your MTA,
it might have crashed. Please check its status right now, as
it is not possible to do it remotely

OID : 1.3.6.1.4.1.25623.1.0.11270

Informational

The file 42.zip was sent 2 times. If there is an antivirus in your MTA, it might
have crashed. Please check its status right now, as it is
not possible to do so remotely

BID : 3027
OID : 1.3.6.1.4.1.25623.1.0.11036

[return to www.unipi.gr]

www.unipi.gr - general/tcp

Informational

ICMP based OS fingerprint results:

HP UX 11.0 (accuracy 91%)
Sun Solaris 10 (SunOS 5.10) (accuracy 91%)

OID : 1.3.6.1.4.1.25623.1.0.102002

Informational

Nikto could not be found in your system path.
OpenVAS was unable to execute Nikto and to perform the scan you
requested.
Please make sure that Nikto is installed and that nikto.pl or nikto is
available in the PATH variable defined for your environment.
OID : 1.3.6.1.4.1.25623.1.0.14260

Informational

Information about this scan :

OpenVAS version : 2.0.2
Scanner IP : 192.168.0.8
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : no
Max hosts : 20
Max checks : 4
Scan duration : unknown (ping_host.nasl not launched?)

OID : 1.3.6.1.4.1.25623.1.0.19506

Appendix: NVT Information

NVT 1.3.6.1.4.1.25623.1.0.11270: SMTP too long line

Summary Sends a too long single line to the MTA

Category denial

Family SMTP problems

Version $Revision: 3477 $

Signed by not signed

Description

Some antivirus scanners dies when they process an email with a
too long string without line breaks.
Such a message was sent. If there is an antivirus on your MTA,
it might have crashed. Please check its status right now, as
it is not possible to do it remotely

NVT 1.3.6.1.4.1.25623.1.0.14260: Nikto (NASL wrapper)

Summary Assess web server security with Nikto

Category infos

Family CGI abuses

Version 1.6

Signed by not signed

Description

This plugin uses nikto(1) to find weak CGI scripts
and other known issues regarding web server security.
See the preferences section for configuration options.

Risk factor : None

Parameters

Force scan even without 404s no

NVT 1.3.6.1.4.1.25623.1.0.90002: SLAD Run

Summary Connects to SLAD to tun programs remotely

Category infos

Family SLAD

Version 1.0

Signed by not signed

Description

This script connects to SLAD on a remote host to run
remote scanners.
To work properly, this script requires to be provided
with a valid SSH login by means of an SSH key with pass-
phrase if the SSH public key is passphrase-protected, or
a password to log in.

NVT 1.3.6.1.4.1.25623.1.0.900499: Apache mod_proxy_ajp Information Disclosure Vulnerability

Summary Check for Apache Web Server version
Category infos
Family Web application abuses
Version $Revision: 1.0 $
CVE CVE-2009-1191
BID 34663
Signed by not signed

Description

Overview: This host is running Apache Web Server and is prone to
Information Disclosure Vulnerability.

Vulnerability Insight:
This flaw is caused due to an error in 'mod_proxy_ajp' when handling
improperly malformed POST requests.

Impact:
Successful exploitation will let the attacker craft a special HTTP POST
request and gain sensitive information about the web server.

Impact level: Application

Affected Software/OS:
Apache HTTP Version 2.2.11

Workaround:
Update mod_proxy_ajp.c through SVN Repository (Revision 767089)
http://www.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff

Fix: No solution or patch is available as on 29th April, 2009. Information
regarding this issue will be updated once the solution details are available.
For further updates refer, http://httpd.apache.org/download.cgi

References:
http://secunia.com/advisories/34827
http://xforce.iss.net/xforce/xfdb/50059

http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=766938&r2=767089

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:P/I:N/A:N)
CVSS Temporal Score : 4.0
Risk factor: Medium

NVT 1.3.6.1.4.1.25623.1.0.19506: Information about the scan

Summary Displays information about the scan
Category end
Family General
Version $Revision: 3059 $
Signed by not signed

Description

This script displays, for each tested host, information about the scan itself:

- The version of the plugin set
- The type of plugin feed (Direct, Registered or GPL)
- The version of the OpenVAS Engine
- The port scanner(s) used
- The port range scanned
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.90003: SLAD Fetch Results

Summary Connects to SLAD to fetch installed plugins
Category infos
Family SLAD
Version 1.0
Signed by not signed

Description

This script connects to SLAD on a remote host to fetch
the result from scripts started earlier.
To work properly, this script requires to be provided
with a valid SSH login by means of an SSH key with pass-
phrase if the SSH public key is passphrase-protected, or
a password to log in.

NVT 1.3.6.1.4.1.25623.1.0.11032: Directory Scanner

Summary Directory Scanner
Category infos
Family Misc.
Version $Revision: 38 $
XRefs OWASP:OWASP-CM-006
Signed by not signed

Description

This plugin attempts to determine the presence of various
common dirs on the remote web server

NVT 1.3.6.1.4.1.25623.1.0.10263: SMTP Server type and version

Summary SMTP Server type and version
Category infos
Family General
Version $Revision: 118 $
Signed by not signed

Description

This detects the SMTP Server's type and version by connecting to the server
and processing the buffer received.
This information gives potential attackers additional information about the
system they are attacking. Versions and Types should be omitted
where possible.

Solution: Change the login banner to something generic.

Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.10107: HTTP Server type and version

Summary HTTP Server type and version
Category infos
Family General
Version $Revision: 38 $
Signed by not signed

Description

This detects the HTTP Server's type and version.

Solution: Configure your server to use an alternate name like
'Wintendo httpD w/Dotmatrix display'
Be sure to remove common logos like apache_pb.gif.

With Apache, you can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.11213: http TRACE XSS attack

Summary http TRACE XSS attack
Category infos
Family CGI abuses : XSS
Version $Revision: 38 $
CVE CVE-2004-2320
BID 9506, 9561, 11604
Signed by not signed

Description

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

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. See also :

http://www.kb.cert.org/vuls/id/867593

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

NVT 1.3.6.1.4.1.25623.1.0.900107: Apache mod_proxy_ftp Wildcard Characters XSS Vulnerability

Summary Check for vulnerable version of Apache
Category infos
Family CGI abuses : XSS

Version $Revision: 1.1 $
CVE CVE-2008-2939
BID 30560
Signed by not signed

Description

Overview : The host is running Apache, which is prone to cross-site scripting vulnerability.

Vulnerability Insight :

Input passed to the module mod_proxy_ftp with wildcard character is not properly sanitized before returning to the user.

Impact : Remote attackers can execute arbitrary script code.

Impact Level : Application

Affected Software/OS :
Apache 2.0.0 to 2.0.63 and Apache 2.2.0 to 2.2.9 on All Platform

***
Note: The script might report a False Positive as it is only checking for the vulnerable version of Apache. Vulnerability is only when mod_proxy and mod_proxy_ftp is configured with the installed Apache version.
***

Fix : Fixed is available in the SVN repository,
http://svn.apache.org/viewvc?view=rev&revision=682871
http://svn.apache.org/viewvc?view=rev&revision=682868

References : http://httpd.apache.org/
http://www.securityfocus.com/archive/1/495180
http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

CVSS Score :
CVSS Base Score : 5.8 (AV:N/AC:M/Au:NR/C:P/I:P/A:N)
CVSS Temporal Score : 4.5
Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.102002: OS fingerprinting

Summary Detects remote operating system version
Category infos
Family Service detection
Version 1.0.0
Signed by not signed

Description

This script performs ICMP based OS fingerprinting (as described by Ofir Arkin and Fyodor Yarochkin in Phrack #57). It can be used to determine remote operating system version.

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

Risk factor: None

NVT 1.3.6.1.4.1.25623.1.0.11036: SMTP antivirus scanner DoS

Summary 42.zip antivirus MTA DoS
Category denial
Family Denial of Service
Version $Revision: 3477 $
BID 3027
Signed by not signed

Description

This script sends the 42.zip recursive archive to the mail server. If there is an antivirus filter, it may start eating huge amounts of CPU or memory.

Solution: Reconfigure your antivirus / upgrade it

Risk factor : High

NVT 1.3.6.1.4.1.25623.1.0.11229: phpinfo.php

Summary Checks for the presence of phpinfo.php
Category infos **Family** CGI abuses **Version** $Revision: 3476 $
Signed by not signed

Description

Many PHP installation tutorials instruct the user to create a file called phpinfo.php. This file is often times left in the root directory after completion.
Some of the information that can be garnered from this file includes: The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, The system version(unix / linux), and the root directory of the web server.

Solution : remove it

Risk factor : Low

This file was generated by OpenVAS, the free security scanner.

Εχουμε συνοπτικά για το server unipi τις παρακάτω αδυναμίες:

- **Αρχεία κάλούν τη συνάρτηση phpinfo() η οποία μπορεί να αποκαλύψει δυνητικά ευαίσθητη πληροφορία σε έναν επιτιθέμενο.**
- **Ο web server Apache είναι ευάλωτος σε επίθεση τύπου XSS (cross-site scripting).**
- **Ο web server Apache διαθέτει μια αδυναμία κατά την οποία μπορεί να αποκαλύψει ευαίσθητη πληροφορία κατά το χειρισμό αλλοιωμένων POST αιτήσεων.**

Για το server dtps.unipi ανακαλύφθησαν οι παρακάτω αδυναμίες:

- **Αδυναμία στη σουίτα invision power board η οποία μπορεί να οδηγήσει σε επίθεση τύπου sql injection.**
- **Αδυναμία στο λογισμικό Kayako eSupport μπορεί να οδηγήσει σε επίθεσεις του τύπου sql injection και XSS.**
- **Αδυναμία στο script turnkey ebook store μπορεί να οδηγήσει σε επίθεση του τύπου XSS.**
- **Το σύστημα διαχείρισης PsNews διαθέτει αδυναμίες οι οποίες μπορούν να οδηγήσουν σε επίθεση του τύπου XSS.**
- **Bug στο λογισμικό PHProxy το κάνει ευάλωτο σε επιθέσεις τύπου HTML injection, Javascript injection, XSS, web cache poisoning.**
- **Ο web server είναι ευάλωτος σε επίθεση κατά την οποία ένας επιτιθέμενος μπορεί να αλλοιώσει τη συμβολοσειρά στη επικεφαλίδα του προτύπου HTTP 1.0.**
- **Η υπηρεσία SMTP μπορεί να σταματήσει να λειτουργεί εάν ένας επιτιθέμενος στείλει μια εντολή με πολύ μεγάλο όρισμα.**

3.3 Ανάλυση αδυναμιών με το λογισμικό Acunetix Web Vulnerability Scanner

Το συγκεκριμένο λογισμικό αναλαμβάνει μέσω ενός συνόλου δοκιμών που διαθέτει στη βάση δεδομένων του να εξετάσει έναν οποιονδήποτε web server για τυχόν αδυναμίες που παρουσιάζει. Παρακάτω παραουσιάζουμε τις σημαντικότερες εξ' αυτών που αφορούν το server dtps.unipi.

- **Το script Sql_injection.script είναι ευάλωτο σε πειθέσεις του τύπου sql injection.**

- **Η κρυπτογράφηση της κίνησης πραγματοποιείται μέσω του πρωτοκόλλου SSL 2.0 του οποίοιυ η έκδοση είναι ξεπερασμένη και με γνωστές αδυναμίες. Πιθανή εκμετάλλευση της αδυναμίας αυτής μπορεί να οδηγήσει σε επίθεση του τύπου man-in-the-middle.**

- **Το ssl πιστοποιητικό που χρησιμοποιείται φαίνεται να είναι λήξει ή να μην έχει γίνει έγκυρο. Ωστόσω ο server θα συνεχίσει να επεξεργάζεται κίνηση χωρίς να επηρεάζεται από το γεγονός αυτό ή η σύνδεση θα διακόπεται απότομα.**

- **Ο server χρησιμοποιεί ssl αλγόριθμους οι οποίοι είτε προσφέρουν αδύναμη κρυπτογράφηση είτε μηδαμινή.**

- **Δε παρέχεται μηχανισμός κλειδώματος λογαριασμού σε περίπτωση επαναλαμβανόμενης εισαγωγής λαναθασμένων διαπιστευτηρίων.**

- **Ο server διαθέτει καταλόγους οι οποίοι ενδέχεται να αποκαλύπτουν ευαίσθητη πληροφορία.**

- **Η μέθοδος HTTP TRACE είναι ενεργοποιημένη στο server κάτι που σε συνδυασμό με αδυναμίες στο browser μπορεί να οδηγήσει στην διαρροή ευαίσθητης πληροφορίας, ακόμα και δεδομένων αυθεντικοποίησης.**

Για το server unipi το λογισμικό ανακάλυψε τις παρακάτω σημαντικές αδυναμίες.

- **Ο server διαθέτει script ευάλωτο σε επιθέσεις του τύπου sql injection.**

- **Ο server διαθέτει script ευάλωτο σε επιθέσεις του τύπου XSS (cross-site scripting).**

- **Στο server χρησιμοποιείται έκδοση του Apache server η οποία είναι ξεπερασμένη και διαθέτει αδυναμίες τις οποίες μπορεί να εκμεταλλευθεί ένα επιτιθέμενος.**

- **Υπάρχουν περιπτώσεις που η ιστοσελίδα του server εμφανίζει μηνυμα σφάλματος ή προειδοποίησης το οποίο μπορεί να οδηγήσει σε διαρροή πληροφορίας. Επιπλέον, το μήνυμα αυτό μπορεί να φανερώνει τη τοποθεσία του αρχείου που παρήγαγε το μήνυμα.**

- **Ανακαλύφθηκε backup αρχείο το οποίο μπορεί να αποκαλύπτει πληροφορίες όπως scripts, ρυθμίσεις του server καθώς και άλλη ευαίσθητη πληροφορία.**

- **Στο server ανακαλύφθηκε η σελίδα phpinfo η οποία ανακαλύπτει πολλές πληροφορίες γαι τη τωρινή κατάσταση της php που χρησιμοποιείται από το server (έκδοση της php, πληροφορία για το server καθώςκαι του περιβάλλοντος λειτουργίας της php, έκδοση λειτουργικού συστήματος, διαδρομές, κύριες και τοπικές τιμές ρυθμίσεων, HTTP επικεφαλίδες καθώς και την άδεια της PHP.**

- **Πηγαίος κώδικας κάποιου script μπορεί να αποκαλύψει ευαίσθητη πληροφορία όπως συμβολοσειρές σύνδεσης της βάσης δεδομένων, λογική της εφαρμογής αναλύοντάς τον.**

- **Στο server τρέχει η εφαρμογή WS_FTP η οποία δημιουργεί ένα log file το οποίο περιέχει ευαίσθητη πληροφορία την οποία μπορεί να εκμεταλλευθεί ένας επιτιθέμενος.**

- **Η μέθοδος HTTP TRACE είναι ενεργοποιημένη στο server κάτι που σε συνδυασμό με αδυναμίες στο browser μπορεί να οδηγήσει στην διαρροή ευαίσθητης πληροφορίας, ακόμα και δεδομένων αυθεντικοποίησης.**

- **Μία ή περισσότερες e-mail διευθύνσεις βρέθηκαν στο server. Αυτές οι διευθύνσεις είναι πολύ εύκολο να βρεθούν από προγράμματα τα οποία αναζητούν e-mails από το διαδίκτυο. Το αποτέλεσμα είναι ένας επιτιθέμενος να πραγματοποιήσει μαζική αποστολή spam mails σε αυτές τις διευθύνσεις.**

- **Οποιαδήποτε αίτηση σε ιστοσελίδα η οποία δεν υφίσταται στο server επιστρέφει μια σελίδα λάθους η οποία αποκαλύπτει έκδοση του web server καθώς και μια λίστα όλων των modules που τρέχουν σε αυτόν. Με αυτή τη πληροφορία ένας επιτιθέμενος μπορεί να πραγματοποιήσει περαιτέρω επιθέσεις.**

- **Ο javascript κώδικας που τρέχει στο server χρησιμοποιεί τη συνάρτηση eval(). Η συνάρτηση αυτή αξιολογεί οποιαδήποτε συμβολοσειρά δίνεται ως είσοδος και μετά την εκτελεί. Εάν η είσοδος δίνεται από ένα κακόβουλο τότε αυτός μπορεί να εκτελέσει επιθέση του τύπου XSS.**

Μία ή περισσότερες έγκυρες διαδρομές ανακαλύφθησαν στο server. Η πληροφορία αυτή μπορεί να δώσει σε έναν επιτιθέμενο γνώση σχετικά με δομή του συστήματος αρχείων στο server κάτι που θα μπορούσε να χρησιμοποιήσει για την εκτέλεση επιθέσεων.

3.4 Ανάλυση αδυναμιών με το λογισμικό Nikto

Στο βήμα αυτό θα κάνουμε μια ανάλυση των αδυναμιών οι οποίες ανακαλύφθησαν στους υπό μελέτη servers. Συνοψίζοντας από τα προηγούμενα βήματα έχουμε ανακαλύψει τις παρακάτω πληροφορίες:

- **Domain names και IP διευθύνσεις**
- **Πληροφοριακή υποδομή**
- **Υπηρεσίες και ports στις οποίες αυτές τρέχουν**
- **Λειτουργικά συστήματα των προς μελέτη servers**

Συνεχίζοντας, κάνουμε χρήση του εργαλείου Nikto το οποίο αποτελεί ένα web server scanner ώστε να ανακαλύψουμε αδυναμίες που τυχόν υπάρχουν στο λογισμικό του web server αλλά και λανθασμένες ρυθμίσεις. Εκτελώντας το λογισμικό Nikto για το server unipi λαμβάνουμε τη παρακάτω έξοδο:

- Nikto v2.1.3

+ Target IP: 195.251.229.6

+ Target Hostname: www.unipi.gr

+ Target Port: 80

+ Start Time: 2011-01-14 12:06:46

+ Server: Apache/2.0.54 (Unix) DAV/2

+ Apache/2.0.54 appears to be outdated (current is at least Apache/2.2.16). Apache 1.3.42 and 2.0.63 are also current.

+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE

+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ OSVDB-32774: /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Contains PHP configuration information and is vulnerable to Cross Site Scripting (XSS).

+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-20406: /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: PHP contains a flaw that allows a remote cross site scripting attack.

+OSVDB-
24484:/phpinfo.php?cx[]=pDCWNTXTjmzcZzgGptO4ev4DXomlLfuSatl1C8NKgg62yGPAb9T
1VhrPF7va0swjqLNpn1Sc30ERUpNePearxpXmmjGyl7HLGZFdUxK35oZnliQ97ndpMlXf64kj
8vai0v9Sk5cN0TmuyUPZPUu6VhJQXRJtRrKyt0q9bB3aUwAF6nidPphzvEdPmOX2ikrRTGin
N6Scd4KTXRY8ATd7JdFWob85QBXIoewzMXSqiDrjnqsBQkCGUb1a6S0joMVlcosICuCCHy
yByR6VRRqJzU8MBe1UsAhAswlRlm4zbMRJXU5xEg38GDCxfCsXKSmR5BSuuikCjmUFZq
ylS8LEvLIWFzj1kL2wLcoE1wL0QHMuUZYcKpVmDaJASA6l6fEaT3uktDO5LJhn0oEVsrOCx
7rA2skg2d1pFu5F89dp3NOXZzrpOrn6oa49Ala9FX5EloXmzoOt0GMzIsuuiJtfolj3PdvFjZNfe
dPUUeUzwaG00miBgY4QgrTuVjjtzvEFbrN1H6ablMEYZ2PrEsS2sv8BtKsfBTh6MUoXvHUrD
5N6muS7Sn4rkA1Ae7KbyaR2STTYUdghd9VOfptJ7XkG5DtnFqmRRiwhXVqFr8qtnA5xYdyz
QQY4MBUQyUFvKuATKc9rMvQurKsPpYlpM7wF1l1Jp9mxvnNHM0kX0VEbxr9XhMelZHgtE
N3WX9WPX6kE9AtC4NTknSdi2X3Sykc4df3HsGvSMsUE70k1cwXZ8cD9COgjeV3kwTJZ2z0
SYJBo5vZvlPUExZDwRbgBNCLBLwhOVgILcJKDjQOCG24i7FM8NCCtj0RXOqOTFl4YguDm
0bsOXwkdNFtuudBT6aoUbuN3cm3mo98yaOQM74OLnwkiV5eZKVOe1mZ1ZyxFPsjKNy1h
MpiLxSLIkEi3xRhbR5r71Rpi3yPaYZ5zKJTXOcC4ytBf8v2PoX75JUDyommK6k79DjA8RyYrR
OlHNk8USIkZUj6ai8TG63Qjc2Y9T4WCUOH3yXhBLXWfCKnnPKPQSlHUifRLgmD12utq14ZX
T0wENz8d55eKxcmUum4miNbTCe5XjDQfKTXyd8JpHaGo6flh8J7mmDWz07rBtQ9TtQd5UA
jm7roCPqrvnn6lUZDWoMhFWbDkZNAxWq1WgJQmXgNvr4pS2KNV85qvJrxxByVCRwThM
mGuh1ehU2K0V98melpSqKGoUXy7gUEeBXhoYp9NdbPFly5G8mXF1w9Kiv2j63n2orphkhn
FeVyyoJq8HV28DyGoscBKdPYyZHy8FMS51tlYZf4IzilvQQQxJNAPuZvHQpvsevfCCOhdSA
MFz2m97JUqkalMeusvyyrlgbl5a38DmhcLBNW8MGnkqfiof5Cjf4jjZgEmPvsLmDN2Avwg2m
oEeYr84QaDahQBO3UrdaA0nH4nRzRxCsDwLKU4Z5a82nEeuPv9ARjrwHBvBog9oJfpD429
65oiDF3AptTjySYaVFCZJQrQGKajFCBieav7dX6wVZ2staLN6G9mTfMPwXqMtqnMRGAG3z
99LDK2p3QoNcIqO7q0wpXLHxTzVnYBTFFbtY3hTCOJFZPQLyUSQKrarQGTHxwgu7GX0oy
f0uPQxdMwyixCEYr8enzAoBaf2ArcdIzRsgaTv7mynuoVKqHgcEqYVvKfOkDCF9EZYppuvM
QYk411HpKmUA4mrysjw8OVflzswV29QzSSPREnXhld7uC0Y0eyYTzQ2VJg29Nl9EJxzqmFL
0gVuBWQL8S6ptGFaW9yVDgvi3kOvnxoT8S85AxAU5gMf97BIPRQY4hSH1DsgCjK3vkVLH
CEx45Fqd3IHtN99aD8AM0XE2t9r5iGBYAmhyIE2pDMhz5bLLANNzJ3C881FClnQUy4mEHL
NiRvE7ZsyOwGpcuRdYVgWzW3dfuzZtmwEwaTtl4E3wDTMJeG5b5UJDWHBjmkkRR6d83V
ZE3HXuEUlPJsVjVzqH1a6mH2HSAkuBAcqZ29LZwiQbEQw9cUJlAEtxq5tKWMb3P7lgcjp5ir
8toVGsY41MF6VP0gcFmwu66Wai0l87LVHDeDJAg7cjhhnyJhlVL0sXikDySflVwVDwrH2zce
MaMJX1wMgUkyl5TSuFgDNnGcjRFn2b4ar8Di3AMZVuG5Sdb40HkDJITfwH7G9gHnBedIuS
KQEeiohN39UYYBfbcW6YbtnbVili4DttWQM2lCoQ0AYZrELwbfzQTRLycsrJ7HpJ3jjxSnwm
Oh2DggzBNB8UFEsZpGzYobC6Zso0lYhUjtOzQAC6BnzcX3FbS3QjDD1tkLUZpkkWWq20jYi
fHLLedkd0m6shwYubSdPkhZLbhDjrakuw2WVFJT7ZwBBolDjTOSEb8QTTs0tZTKCxnJr7Pe
xH9JyCwlkfKgDaaXG3vrzDGSVTHjBwPcREVOP5nK9mn5bDEYwryqkV1zP6gzMGskeZ7jUt
TE5XeNV4OOBl46hNahnxZwrk3o5luv4EWf1DPuYuxVNlObjGTNYuHiRr9ZdOpsJb2WcvZBP
eNE1wTr1PRH0bwas2RoNK6wTUQ1Q4BXGsgj3YA6mYb2P3bgQ9DoZ0Xg5h45Cttl3amoYld
H4ZTSHFwlDqTxqTeWv7oh6XGv21tnVEKUu5o10fPYLKY9mpEdCON7XLYxPuOKGhvMa0Q
CrEq6OEUWEunDQ2Xrc9JXNVhCj6B1LCBVtY5UBEBfo9XeP20G4UU4ZY0uK9sDMEyPPlH
XWjPYt8DVJcnn6YxR0QZFvh4BCIsOblINBkx9DlA3dm0YKxjpqWcQgzkWtteuTHVlsp64zSA
ClqBPciDzvo2jAp8OriitZzY3QZRewQxP5xlGK8GwCP3hrNw0BLJ68fbA3RpJRFscYHx4oYc
Elf8T3hxqhOEjSb8v7Fstbnj0f2PoZ4YeDZXom2kYcNckRDCsA9mQo8pl2dfRwrgwAIKTPJlx
W1XEmtcgRs2hlVsqdLR65PSxbNyeYu6ebkRMHQhwg7ManuhCdziDUD4mVmGHdvXIh6ve
8aO0E3kGwihDu1Q14wl52ZzDnUs0Hk5frQg25eV5xPntZuqUi2LeRZ2QvfR9H4CW5oxpFvyL
xWSydA4FqFqUCfP3oaVpRZMZ5dZtAUaLGwDwnuq0V9hqCPsatM4nYl7PpRlNuecfd6lj1cD
8e9ewX0zrhbHwDWSo9UQOL8SgC0YVSXhWU5vby3rxlF8RhD4l4ie9ikZshalk5hJFMug6Lz0
wL6KPZKgQalZ3dtrb8JWcHvyFRqFxkr4FXZKgw3EOraki247sHdNlxLfwenV1Qq4flG6SkELN
DKwbH6HoonBbgt4rLn1pxkV96mayLsrdjy0j7EJq0STP0lnVFpjElOwtO1qd9yxfTGJ7Hez3vm
BgWMKA39L5mQgSfhUDa7PaXsniaeGl6vobySMtf4ekuCfY1kPBZhDhxRK5tOOVqvCPXSLI
3B9MClsynyHaUwlcH73h6dtSbq2wl3OCO0uD1lJERgUjw1PX0gocemfUT2Y2J9Y8w4Wz37B
A9dDwwvwctN5otMyyXAoaPkWzzyrUjAWWDd8U27Gpfnfhv54KVRrPdswUAy1uOpxckrCat
FibPDaq3AJa7pMDH7Hg2tL14vlCuZi851UjWR0VXpo8kWs1MSHUM3kZawUGqW59SShi4Y9
nBTYl1RAyscvloVslFFbleMs2nySnEi3QgthXx5tZ3McBve1tClG5yoWTAgu4KEHwYJmBlRH
DAp4zTMa4gd2IlfSsWozjwenph5EPHVweebnLAgTg34MZEjGjrfOVeMjzrvln4MjblwQWF4JG
96E4i0pFBNvTXzywzVNS36cqweY391YJk50CN2U0RV3QKGy7fHasinUzjwQoBOSMpKUTZd

5fABdnK7cE3NVJtKHDT3YBKnuEYeddW4ZQBFyvw5tltWIFCTvakVzmLUnYMMgTBxRkqsI 6pIvaWs1SifeQ0KLYKS1QghJxJvZOO1LnbwlY2flLjjasuwnBJwchRf6FziGYbknlDx5WXlY7s aDzvKxmTCR5qA3QKYRYiPelt4Fs4AiyN5JlzhV5ov8xoPH4VQSPOe1ub259LQVmNug1tnRZ fpKg85JONxUN<script>alert(foo)</script>: PHP 5.1.2 and 4.4.2 phpinfo() Function Long Array XSS

+ OSVDB-3233: /icons/README: Apache default file found.
+ 6417 items checked: 2 error(s) and 10 item(s) reported on remote host
+ End Time: 2011-01-14 12:11:48 (302 seconds)

+ 1 host(s) tested

Συνοψίζοντας από τη παραπάνω αναφορά του προγράμματος Nikto προκύπτουν οι εξής σημαντικές αδυναμίες:

- **Ο web server που χρησιμοποιείται δεν είναι ενημερωμένος με αποτέλεσμα να μην υπάρχει προστασία σε ανακαλυφθέντα κενά ασφαλείας.**

- **Η μέθοδος TRACE είναι ενεργή με αποτέλεσμα ο web server να είναι ευάλωτος σε επιθέσεις του τύπου XST (cross-site tracing).**

- **Υπάρχει πληροφορία για ρύθμιση της PHP η οποία είναι ευάλωτη σε επιθέσεις του τύπου XSS (cross-site scripting).**

- **Επιπλέον αδυναμία στη PHP επιτρέπει την απομακρυσμένη εκτέλεση επιθέσεων του τύπου XSS (cross-site scripting).**

Στη συνέχεια παραθέτουμε την έξοδο του προγράμματος για το server dtps.unipi.

- Nikto v2.1.3

+ Target IP: 195.251.226.211
+ Target Hostname: dtps.unipi.gr
+ Target Port: 80
+ Start Time: 2011-01-14 12:18:32

+ Server: Apache
+ Retrieved x-powered-by header: PHP/5.3.3
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-637: Enumeration of users is possible by requesting ~username (responds with 'Forbidden' for users, 'not found' for non-existent users).

+DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+/index.php?option=search&searchword=<script>alert(document.cookie);</script>: Mambo Site Server 4.0 build 10 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /index.php?dir=<script>alert('Vulnerable')</script>: Auto Directory Index 1.2.3 and prior are vulnerable to XSS attacks.

+/index.php/content/search/?SectionID=3&SearchText=<script>alert(document.cookie)</script>: eZ publish v3 and prior allow Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+/index.php/content/advancedsearch/?SearchText=<script>alert(document.cookie)</script>&PhraseSearchText=<script>alert(document.cookie)</script>&SearchContentClassID=-1&SearchSectionID=-1&SearchDate=-1&SearchButton=Search: eZ publish v3 and prior allow Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+/?mod=<script>alert(document.cookie)</script>&op=browse: Sage 1.0b3 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+OSVDB-25497: /index.php?rep=<script>alert(document.cookie)</script>: GPhotos index.php rep Variable XSS.

+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests which contain specific QUERY strings.

+ OSVDB-2790: /index.php?vo=\"><script>alert(document.cookie);</script>: Ralusp Sympoll 1.5 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-3092: /forum/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6417 items checked: 28 error(s) and 15 item(s) reported on remote host
+ End Time: 2011-01-14 12:28:45 (613 seconds)

+ 1 host(s) tested

Συνοψίζοντας, οι σημαντικότερες αδυναμίες που ανακαλύφθησαν είναι οι εξής:

- **Η μέθοδος TRACE είναι ενεργή με αποτέλεσμα ο web server να είναι ευάλωτος σε επιθέσεις του τύπου XST (cross-site tracing).**
- **Το σύστημα διαχείρισης Mambo site server 4.0 που χρησιμοποείται από το server είναι ευάλωτο σε επιθέσεις του τύπου XSS (cross-site scripting).**
- **Το σύστημα Auto Directory Index 1.2.3 το οποίο δημιουργεί μια λίστα όλων των αρχείων σε ένα κατάλογο είναι ευάλωτο σε επιθέσεις του τύπου XSS (cross-site scripting).**
- **Το σύστημα διαχείρισης eZ publish v3 που χρησιμοποείται από το server είναι ευάλωτο σε επιθέσεις του τύπου XSS (cross-site scripting).**

- **Το λογισμικό Sage 1.0b3 που τρέχει στο server είναι ευάλωτο σε επιθέσεις του τύπου XSS (cross-site scripting).**

- **Η PHP μπορεί να αποκαλύψει ευαίσθητη πληροφορία ως απάντηση σε συγκεκριμένα HTTP αιτήματα τα οποία περιέχουν συγκεκριμένες σειρές συμβολοσειρών.**

- **Το σύστημα διαχείρισης Ralusp Sympoll 1.5 που χρησιμοποείται από το server είναι ευάλωτο σε επιθέσεις του τύπου XSS (cross-site scripting).**

4.ΣΕΝΑΡΙΑ ΑΠΩΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΘΕΣΕΩΝ

ΣΕΝΑΡΙΟ 1: ΑΠΩΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΣ ΑΠΟ ΚΑΤΑΚΛΥΣΜΟ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ΜΕ ΑΧΡΗΣΤΑ ΜΗΝΥΜΑΤΑ

Το επόμενο σενάριο που θα περιγράψουμε αφορά επίθεση η οποία έχει σαν στόχο τους διακομιστές οι οποίοι είναι υπεύθυνοι για το ηλεκτρονικό ταχυδρομείο. Πιο συγκεκριμένα, ένας επιτιθέμενος έχει τη δυνατότητα πολύ έυκολα να ανακαλύψει λογαριασμούς ηλεκτρονικού ταχυδρομείου που ανήκουν στο πανεπιστήμιο και να πραγματοποιήσει μια μαζική αποστολή άχρηστων μηνυμάτων σε αυτούς τους λογαριασμούς γεμίζοντας σε πολύ μικρό χρονικό διάστημα τον διαθέσιμο αποθηκευτικό χόρο του διακομιστή. Το αποτέλεσμα είναι χρήσιμα e-mail τα οποία θα φθάνουν στο server να απορρίπτονται διότι δε θα υπάρχει διαθέσιμος χώρος για την αποθήκευση τους και άρα παρακώλυση επικοινωνιών. Καθίσταται σαφές ότι ο server θα πρέπει να είναι ρυθμισμένος να απορρίπτει e-mail από αποστολείς οι οποίες προσπαθούν να τον κατακλύσουν. Δηλαδή σε περίπτωση που παρατηρείται αποστολή μεγάλου αριθμού e-mails από μία συγκεκριμένη διεύθυνση ηλεκτρονικού ταχυδρομείου τότε ο server θα πρέπει να απορρίπτει όλα τα e-mails τα οποία περιέχουν αυτή τη διεύθυνση αποστολής.

ΣΕΝΑΡΙΟ 2: ΠΡΑΓΜΑΤΟΠΟΙΗΣΗ ΕΠΙΘΕΣΗΣ ΑΡΝΗΣΗΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ (DENIAL OF SERVICE ATTACK)

Το σενάριο που παρουσιάζουμε στη συνέχεια παρουσιάζει αρκετές ομοιότητες με το προηγούμενο και αφορά τον ίδιο τον web server. Σε μία παρόμοια περίπτωση όπως και η προηγούμενη ένας επιτιθέμενος έχει τη δυνατότητα να πραγματοποιήσει μαζική αποστολή αιτήσεων στο server ο οποίος αδυνατώντας να απαντήσει σε όλες αυτές τις αιτήσεις, τις τοποθετεί σε μια ουρά αναμονής για να απαντηθούν όταν έρθει η σειρά τους. Ωστόσο ο επιτιθέμενος συνεχίζει να αποστέλλει αιτήσεις με αποτέλεσμα να γεμίσει η ουρά αναμονής και ο server πλέον να απορρίπτει αιτήσεις ακόμα και από κανονικούς χρήστες. Η συγκεκριμένη επίθεση ονομάζεται επίθεση άρνησης παροχής υπηρεσιών (**Denial of Service Attack**) και καθιστά αδύνατη τη προσπέλαση της ιστοσελίδας.

ΣΕΝΑΡΙΟ 3: ΠΛΑΣΤΟΓΡΑΦΗΜΕΝΑ E-MAILS

Σε αυτό το σενάριο ο επιτιθέμενος έχει τη δυνατότητα να στείλει e-mails σε λογαριασμούς ηλεκτρονικού ταχυδρομείου που ανήκουν στο πανεπιστήμιο προσποιούμενος κάποιον χρήστη που διαθέτει λογαριασμό ηλεκτρονικού ταχυδρομείου μέσα σε αυτό. Η μέθοδος αυτή πραγματοποιείται πλαστογραφώντας τη διεύθυνση αποστολής με μία έγκυρη διεύθυνση που ανήκει στο πανεπιστήμιο και αποστολή του ηλεκτρονικού μηνύματος στο υποψήφιο θύμα. Δεδομένου ότι το e-mail φαίνεται ως απόλυτα έγκυρο καθώς για ένα μέσο χρήστη χωρίς ιδιαίτερες γνώσεις δεν είναι εύκολο να διαπιστώσει τη πλαστογραφία, ο επιτιθέμενος μπορεί να προσποιηθεί οποιονδήποτε εργαζόμενο του πανεπιστημίου είτε επιστημονικό είτε διοικητικό προσωπικό με αποτέλεσμα να υπάρχει κίνδυνος διαρροής πληροφορίας.

4.1 Μελέτη Αξιολόγησης Που Δεν Εχει Πραγματοποιηθεί

Οπως αναφέρθηκε στην αρχή της παρούσας αναφοράς, η ανάλυση ασφαλείας της πληροφοριακής υποδομής πραγματοποιήθηκε μην έχοντας προηγούμενη γνώση για την εσωτερική πληροφοριακή δομή καθώς και μην έχοντας άνθρωπο εκ των έσω ο οποίος θα μπορούσε να δίνει πολύτιμες πληροφορίες. Μια ανάλυση ασφαλείας δε περιορίζεται μόνο στο σενάριο κατά το οποίο ο μελετητής πραγματοποιεί τη διαδικασία ανάλυσης όντας εξωτερικά του δικτύου χωρίς προηγούμενη γνώση για την εσωτερική λειτουργία του πανεπιστημίου. Γι’ αυτό στη παρούσα ενότητα θα κάνουμε λόγο για μελέτη που πραγματοποιείται εσωτερικά του πανεπιστημίου ώστε να ανακαλυφθούν τυχόν αδυναμίες που μπορούν να θέσουν σε κίνδυνο τη πληροφοριακή υποδομή του.

Πρώτα από όλα, δεδομένου ότι οι εργαζόμενοι οι οποίοι χειρίζονται ηλεκτρονικό υπολογιστή χρειάζεται να χρησιμοποιούν υπηρεσίες της πληροφοριακής υποδομής με διαπιστευτήρια (όνομα χρήστη και κωδικό πρόσβασης) τα οποία ανήκουν αποκλειστικά σε αυτούς, είναι σημαντικό να αποφευχθεί ένα λάθος το οποίο συμβαίνει συχνά. Παρατηρείται το φαινόμενο στο οποίο οι εργαζόμενοι καταγράφουν το όνομα χρήστη και κωδικό πρόσβασης που τους ανήκει σε ένα χαρτί και το τοποθετούνε πάνω στην οθόνη του συστήματος που χρησιμοποιούνε ώστε να μη χρειάζεται να απομνημονεύσουν τα στοιχεία αυτά. Οποιεσδήποτε έχει φυσική πρόσβαση στο χώρο εργασίας είναι πολύ εύκολο να καταγράψει αυτά τα στοιχεία και να τα χρησιμοποιήσει για προσωπικούς σκοπούς.

Ενα επιπλέον σύνηθες λάθος που γίνεται από τους εργαζόμενους είναι η χρήση των ίδιων διαπιστευτηρίων για πρόσβαση σε περισσότερες του ενός υπηρεσίες. Αποτελεί συνήθεις πρακτική για έναν επιτιθέμενο όταν καταφέρνει να αποκτά το ζεύγος όνομα χρήστη-κωδικός πρόσβασης να επιχειρεί να συνδεθεί σε όλες τις υπηρεσίες που

χρησιμοποιούνται από τους χρήστες μιας εταιρείας χρησιμοποιώντας αυτό το ζεύγος μόνο. Για κάθε διαφορετική υπηρεσία είναι επιτακτικό να χρησιμοποιείται διαφορετικό ζεύγος το οποίο να είναι γνωστό μόνο στο χρήστη και να φυλάσσεται σε ασφαλές μέρος. Πρέπει να τονίσουμε ότι για να είναι ασφαλής ένας κωδικός πρόσβασης πρέπει να αποτελεί ένα συνδυασμό από γράμματα, αριθμούς και ειδικούς χαρακτήρες ώστε να είναι ανθεκτικός σε επιθέσεις εξαντλητικής αναζήτησης. Τέλος, ο κωδικός πρόσβασης πρέπει να ανανεώνεται περιοδικά όπως ορίζεται στη πολιτική ασφάλειας που εφαρμόζεται στο πανεπιστήμιο.

Μία ακόμα παράμετρος στην οποία πρέπει να δοθεί έμφαση αποτελεί η ασφάλεια κάθε είδους συσκευών οι οποίες χρησιμοποιούν κάποιο ζεύγος όνομα χρήστη-κωδικό πρόσβασης το οποίο απαιτείται για τη σύνδεση κάποιου διαχειριστή στη συσκευή. Το λάθος που γίνεται είναι ότι πολλοί διαχειριστές αφήνουν το προκαθορισμένο από το εργοστάσιο ζεύγος διαπιστευτηρίων και το οποίο είναι πολύ εύκολο για τον οποιοδήποτε αν γνωρίζει το μοντέλο να μάθει το ζεύγος αυτό με μια απλή αναζήτηση στο διαδίκτυο. Οπότε το προκαθορισμένο ζεύγος πρέπει να αλλάζει σύμφωνα με τους κανόνες που αναφέρθηκαν παραπάνω.

Συνεχίζοντας, πρέπει να δοθεί ιδιαίτερη προσοχή και να ενημερωθούν οι χρήστες των συστημάτων εντός του πανεπιστημίου να μην χρησιμοποιούν usb stiks τα οποία χρησιμοποιούν στη καθημερινότητα τους καθώς σε περίπτωσης μόλυνσης του usb stik και χρήσης του σε σύστημα εντός του πανεπιστημίου ο κίνδυνος εξάπλωσης του κακόβουλου προγράμματος σε όλο το δίκτυο είναι πολύ μεγάλος. Προτείνεται ο διαμοιρασμός και χρήση usb stiks τα οποία θα χρησιμοποιούνται εντός του πανεπιστημίου μόνο και εφαρμογή αντίστοιχης πολιτικής η οποία θα ορίζει ρητά τη χρήση τους για μεταφορά αρχείων εντός του πανεπιστημίου.

Συνεχίζοντας με τη μελέτη ασφάλειας η οποία δεν πραγματοποίηθηκε, αναφέρουμε την μελέτη των συστημάτων που χρησιμοποιούνται στο εσωτερικό του πανεπιστημίου στο κατά πόσο χρησιμοποιούνε μηχανισμούς ασφαλείας σε περίπτωση που οι εξωτερικοί μηχανισμοί αποδειχτούν ανεπαρκείς σε ενδεχόμενη επίθεση. Πιο συγκεκριμένα, δεν ελέγχθηκε εάν όλα τα συστήματα χρησιμοποιούν προγράμματα καταπολέμησης κακόβουλου λογισμικού (antivirus) και εάν κάτι τέτοιο υφίσταται κατά πόσο είναι ενημερώμενα με τις τελευταίες αναβαθμίσεις. Σε περίπτωση που οι εξωτερικοί μηχανισμοί ασφάλειας δεν καταφέρουν να ανακόψουν μία ενδεχόμενη επίθεση τότε οι εσωτερικοί μηχανισμοί αποτελούν το τελευταίο επίπεδο ασφάλειας.

Ενα επιπλέον χαρακτηριστικό που δεν ελέγχθηκε αφορά τη κουλτούρα ασφάλειας την οποία διαθέτουν οι χρήστες των συστημάτων μέσα στο πανεπιστήμιο. Με τον όρο κουλτούρα ασφάλειας εννοούμε το κατά πόσο ενήμεροι είναι οι χρήστες των συστημάτων για τους κινδύνους που διέπουν το διαδίκτυο καθώς και το κατά πόσο μπορούν να αντιληφθούν εάν οι ενέργειες τους θέτουν σε κίνδυνο την πληροφοριακή υποδομή. Δεν είναι λίγα τα περιστατικά στα οποία εργαζόμενοι τρέχουν εφαρμογές στο διαδίκτυο οι οποίες είναι μολυσμένες με κακόβουλα προγράμματα. Οι συνέπειες

μπορεί να ποικίλλουν από υποκλοπή δεδομένων και κωδικών πρόσβασης μέχρι διαγραφή χρήσιμων δεδομένων.

Συνοψίζοντας, παρουσιάζουμε παρακάτω τη μελέτη ασφάλειας που δεν έχει πραγματοποιηθεί:

- **Φύλαξη διαπιστευτήριων (όνομα χρήστη-κωδικός πρόσβασης) σε ασφαλές μέρος για πρόσβαση σε υπηρεσίες.**
- **Χρήση διαφορετικού ζεύγους όνομα χρήστη-κωδικός πρόσβασης για κάθε υπηρεσία που απαιτεί τέτοιο ζεύγος.**
- **Εφαρμογή κανόνων για τη δημιουργία δύσκολων κωδικών πρόσβασης και ανανέωσης τους περιοδικά.**
- **Αλλαγή προκαθορισμένου από το εργοστάσιο ζεύγους όνομα χρήστη-κωδικός πρόσβασης για συσκευες που χρησιμοποιούνται.**
- **Χρήση αφαιρούμενων μέσων αποθήκευσης τα οποία ανήκουν αποκλειστικά στο πανεπιστήμιο και δεν χρησιμοποιούνται εκτός αυτού.**
- **Χρήση antivirus και firewalls στα συστήματα που χρησιμοποιούνται στο εσωτερικό του πανεπιστημίου.**

Επίπεδο κουλτούρας ασφαλείας εργαζομένων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ

- HACKING EXPOSED 6 NETWORK SECURITY SECRETS & SOLUTIONS 2009, Stuart McClure , Joel Scambray , George Kurtz

- PENETRATION TESTER'S OPEN SOURCE TOOLKIT VOLUME 2 2007, Aaron W. Bayles, Keith Butler, Adair John Collins, Haroon Meer, Eoin Miller, Gareth Murray Phillips, Michael J. Schearer, Jesse Varsalone, Thomas Wilhelm, Mark Wolfgang

- PROFESSIONAL PENETRATION TESTING CREATING AND OPERATING A FORMAL HACKING LAB 2010, Thomas Wilhelm

ΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ

- www.vulnerabilityassessment.co.uk

- http://nmap.org

- http://cirt.net/nikto2

- http://www.openvas.org/

- http://packetstormsecurity.org/

- http://www.securityfocus.com/