Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

3η Εργασία
Ονοματεπώνυμο: Αγησίλαος Κολλιόπουλος
Αριθμός Μητρώου: 1072803
Τμήμα: ΗΜΤΥ

Ερωτήσεις κατανόησης και Εργασία για το μάθημα:
Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

1) Επίδειξη μηχανισμού 3-WAY HANDSHAKE με χρήση tcpdump
Θα χρησιμοποιήσουμε το tcpdump για την καταγραφή του μηχανισμού σύνδεσης του TCP πρωτοκόλλου (3-WAY HANDSHAKE). Στο τερματικό του υπολογιστή συνδεόμαστε στο VM:

ssh debian@192.168.1.XX

Σε άλλο τερματικό εκτελούμε την εντολή:

```
agiskallas@debian-agis:~$ sudo tcpdump -vvv -nn -i enp0s3 -s 1500 -S -X -c 5 'src 192.168.1.10' or '
dst 192.168.1.3' and 'port 22'
```

Εδώ βλέπουμε τα πακέτα που κατέγραψε το tcpdump με flags SYN & PSH:

```
00:27:53.940068 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.13.22 > 192.168.1.3.56607: Flags [S.], cksum 0x8387 (incorrect -> 0xf8fc), seq 3350059233, ack 1763250388, win 64240, options [mss 1460,nop,no
p,sackOK,nop,wscale 7], length 0
        0x0000:  4500 0034 0000 4000 4006 b763 c0a8 010d  E..4..@.@..c....
        0x0010:  c0a8 0103 0016 dd1f c7ad d8e1 6919 10d4  ............i...
        0x0020:  8012 faf0 8387 0000 0204 05b4 0101 0402  ................
        0x0030:  0103 0307                                ....
00:27:53.948252 IP (tos 0x0, ttl 64, id 527, offset 0, flags [DF], proto TCP (6), length 80)
    192.168.1.13.22 > 192.168.1.3.56607: Flags [P.], cksum 0x83a3 (incorrect -> 0xcdca), seq 3350059234:3350059274, ack 1763250388, win 502, length 40: SSH:
 SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u1
        0x0000:  4500 0050 020f 4000 4006 b538 c0a8 010d  E..P..@.@..8....
        0x0010:  c0a8 0103 0016 dd1f c7ad d8e2 6919 10d4  ............i...
        0x0020:  5018 01f6 83a3 0000 5353 482d 322e 302d  P.......SSH-2.0-
        0x0030:  4f70 656e 5353 485f 392e 3270 3120 4465  OpenSSH_9.2p1.De
        0x0040:  6269 616e 2d32 2b64 6562 3132 7531 0d0a  bian-2+deb12u1..
00:27:53.953414 IP (tos 0x0, ttl 64, id 528, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.1.13.22 > 192.168.1.3.56607: Flags [.], cksum 0x837b (incorrect -> 0x3281), seq 3350059274, ack 1763250421, win 502, length 0
        0x0000:  4500 0028 0210 4000 4006 b55f c0a8 010d  E..(..@.@.._....
        0x0010:  c0a8 0103 0016 dd1f c7ad d90a 6919 10f5  ............i...
        0x0020:  5010 01f6 837b 0000                      P....{..
00:27:53.954581 IP (tos 0x0, ttl 64, id 529, offset 0, flags [DF], proto TCP (6), length 1120)
    192.168.1.13.22 > 192.168.1.3.56607: Flags [P.], cksum 0x87b3 (incorrect -> 0x391f), seq 3350059274:3350060354, ack 1763250421, win 502, length 1080
        0x0000:  4500 0460 0211 4000 4006 b126 c0a8 010d  E..`..@.@..&....
        0x0010:  c0a8 0103 0016 dd1f c7ad d90a 6919 10f5  ............i...
        0x0020:  5018 01f6 87b3 0000 0000 0434 0714 121c  P.........4....
        0x0030:  8955 de8d faec 3e6b 3f7b a2c3 462c 0000  .U....>k?{..F,..
        0x0040:  0109 736e 7472 7570 3736 3178 3235 3531  ..sntrup761x2551
        0x0050:  392d 7368 6135 3132 406f 7065 6e73 7368  9-sha512@openssh
        0x0060:  2e63 6f6d 2c63 7572 7665 3235 3531 392d  .com,curve25519-
        0x0070:  7368 6132 3536 2c63 7572 7665 3235 3531  sha256,curve2551
        0x0080:  392d 7368 6132 3536 406c 6962 7373 682e  9-sha256@libssh.
        0x0090:  6f72 672c 6563 6468 2d73 6861 322d 6e69  org,ecdh-sha2-ni
        0x00a0:  7374 7032 3536 2c65 6364 682d 7368 6132  stp256,ecdh-sha2
        0x00b0:  2d6e 6973 7470 3338 342c 6563 6468 2d73  -nistp384,ecdh-s
        0x00c0:  6861 322d 6e69 7374 7035 3231 2c64 6966  ha2-nistp521,dif
        0x00d0:  6669 652d 6865 6c6c 6d61 6e2d 6772 6f75  fie-hellman-grou
        0x00e0:  702d 6578 6368 616e 6765 2d73 6861 3235  p-exchange-sha25
        0x00f0:  362c 6469 6666 6965 2d68 656c 6c6d 616e  6,diffie-hellman
        0x0100:  2d67 726f 7570 3136 2d73 6861 3531 322c  -group16-sha512,
```

Figure 1:Tcpdump

---

2) Πειραματιστείτε και εκτελέστε τις παρακάτω εντολές. Εξηγείστε την έξοδο που δίνουν.
Ο παρακάτω πίνακας επεξηγεί τη σημασία των παραμέτρων στην εντολή tcpdump:

Παράμετρος	**Επεξήγηση**
-v	Verbose mode
-vvv	Even more verbose output. For example, telnet SB.. options are printed in full.
-n	Do not resolve hostnames and port numbers in the readable forms.
-nn	Do not resolve hostnames and port numbers in the readable forms. Display numerical values IP address and port numbers

-i eth0	Sets the network interface to ethernet
-i wlan0	Sets the network interface to wireless network interface.
-s 1514	Defines the snaplen (snapshot length) for the packet capture
host <IPADDRESS>	Capture packets either coming in or out of this IP
-S	Print Absolute rather than relative, TCP sequence numbers
-X	Outputs the data of each packet in both hex and ASCII format
-c 5	Limits the number of packets to capture to 5
'src 192.168.1.102' or	Capture packets coming from 192.168.1.102 or
'dst 192.168.1.102' and 'port 22'	or capture packets coming to 192.168.1.102 and port 22

- tcpdump -v -n host 192.168.1.105
  Καταγράφει πακέτα που έρχονται ή φεύγουν από την IP που καθορίζει το host. Οι παράμετροι προσδιορίζουν την απεικόνιση της εξόδου της εντολής.

- tcpdump -vvv -nn -i eth0 -s 1514 host 192.168.1.105 -S -X -c 5
  Καταγράφει 5 πακέτα, μεγέθους 1514 μέσω ethernet που έρχονται ή φεύγουν από την IP που καθορίζει το host. Οι παράμετροι προσδιορίζουν την απεικόνιση της εξόδου της εντολής.

- tcpdump -vvv -nn -i wlan0 -s 1514 host 192.168.1.105 -S -X -c 5
  Καταγράφει 5 πακέτα, μεγέθους 1514 μέσω wlan που έρχονται ή φεύγουν από την IP που καθορίζει το host. Οι παράμετροι προσδιορίζουν την απεικόνιση της εξόδου της εντολής.

- tcpdump -nnvvvXSs 1514 host 192.168.1.105 and dst port 22
  Καταγράφει πακέτα, μεγέθους 1514 που έρχονται ή φεύγουν από την IP που καθορίζει το host, με προορισμό τη θύρα 22. Οι παράμετροι προσδιορίζουν την απεικόνιση της εξόδου της εντολής.

- tcpdump -vvv -nn -i eth0 -s 1514 -S -X -c 5 'src 192.168.1.102' or 'dst 192.168.1.102 and port 22'
  Καταγράφει 5 πακέτα, μεγέθους 1514 μέσω ethernet με πηγή ή προορισμό τις IP και port. Οι παράμετροι προσδιορίζουν την απεικόνιση της εξόδου της εντολής.

- tcpdump -vvv -nn -i eth0 -s 1514 -S -X -c 5 src or dst 71.98.70.149
  Καταγράφει 5 πακέτα, μεγέθους 1514 μέσω ethernet με πηγή ή προορισμό την IP. Οι παράμετροι προσδιορίζουν την απεικόνιση της εξόδου της εντολής.

- 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'
  Καταγράφει 5 πακέτα, μεγέθους 1514 μέσω wlan με πηγή ή προορισμό τις IP και port. Οι παράμετροι προσδιορίζουν την απεικόνιση της εξόδου της εντολής.

- tcpdump udp -i wlan0
  Καταγράφει udp πακέτα μέσω wlan

- tcpdump udp -i any -c 10
  Καταγράφει udp πακέτα από όλα τα δίκτυα, σταματώντας στα 10.

---

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

1. Εκτελούμε το port_scan.py από τον υπολογιστή για να ανιχνεύσουμε ποιες θύρες είναι ανοικτές στην εικονική μηχανή debian. Ανοιχτή είναι η πόρτα 22.

```
agiskallas@debian-agis:~/Lab3$ python3 port_scan.py 192.168.1.10 22 443
22.....................................................................
.....................................................................
.....................................................................
.....................................................................

The open ports:


22:  ssh 22/tcp # SSH Remote Login Protocol
```

Figure 2:Result from port_scan

2. Εκτελούμε το *DoS5.py* εκκινώντας μια DoS επίθεση στο VM με την εντολή, στην θύρα 22 με αριθμό πακέτων μεγαλύτερο από τον αριθμό των προσπαθειών που έχουμε ορίσει στο fail2ban πακέτο. Δώστε την έξοδο σε όλες τις προσπάθειες.

Επιτιθέμενος

```
        0x0020:  5002 2000 f6b7 0000                      P.......
18:08:39.645886 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.10 tell 192.168.1.13,
 length 28
        0x0000:  0001 0800 0604 0001 0800 279c 7c17 c0a8  ..........'.|...
        0x0010:  010d 0000 0000 0000 c0a8 010a            ............
18:08:39.742137 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.49737 > 192.168.1.10.22: Flags [S], cksum 0x2cf2 (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a c249 0016 0000 0000 0000 0000  .....I..........
        0x0020:  5002 2000 2cf2 0000                      P...,...
18:08:39.801656 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.45892 > 192.168.1.10.22: Flags [S], cksum 0x3bf7 (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a b344 0016 0000 0000 0000 0000  .....D..........
        0x0020:  5002 2000 3bf7 0000                      P...;...
18:08:39.834041 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.39397 > 192.168.1.10.22: Flags [S], cksum 0x5556 (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a 99e5 0016 0000 0000 0000 0000  ................
        0x0020:  5002 2000 5556 0000                      P...UV..
18:08:39.870116 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.18768 > 192.168.1.10.22: Flags [S], cksum 0xa5eb (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a 4950 0016 0000 0000 0000 0000  ....IP..........
        0x0020:  5002 2000 a5eb 0000                      P.......
18:08:39.901751 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.39661 > 192.168.1.10.22: Flags [S], cksum 0x544e (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a 9aed 0016 0000 0000 0000 0000  ................
        0x0020:  5002 2000 544e 0000                      P...TN..
```

Figure 3: Tcpdump(attacker)

Θύμα

```
agiskallas@debian-agis:~$ sudo tcpdump -vvv -nn -i enp0s3 -s 1500 -S -X 'src 111.111.111.111'
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 1500 bytes
18:08:38.934024 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.49737 > 192.168.1.10.22: Flags [S], cksum 0x2cf2 (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a c249 0016 0000 0000 0000 0000  .....I..........
        0x0020:  5002 2000 2cf2 0000 0000 0000 0000       P...,..........
18:08:38.993375 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.45892 > 192.168.1.10.22: Flags [S], cksum 0x3bf7 (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a b344 0016 0000 0000 0000 0000  .....D..........
        0x0020:  5002 2000 3bf7 0000 0000 0000 0000       P...;..........
18:08:39.026066 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.39397 > 192.168.1.10.22: Flags [S], cksum 0x5556 (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a 99e5 0016 0000 0000 0000 0000  ................
        0x0020:  5002 2000 5556 0000 0000 0000 0000       P...UV........
18:08:39.061802 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.18768 > 192.168.1.10.22: Flags [S], cksum 0xa5eb (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a 4950 0016 0000 0000 0000 0000  ....IP..........
        0x0020:  5002 2000 a5eb 0000 0000 0000 0000       P.............
18:08:39.093399 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    111.111.111.111.39661 > 192.168.1.10.22: Flags [S], cksum 0x544e (correct), seq 0, win 8192, len
gth 0
        0x0000:  4500 0028 0001 0000 4006 da3e 6f6f 6f6f  E..(....@..>oooo
        0x0010:  c0a8 010a 9aed 0016 0000 0000 0000 0000  ................
        0x0020:  5002 2000 544e 0000 0000 0000 0000       P...TN........
```

Figure 4: Tcpdump(victim)

3. Για άλλη απόδειξη ότι έχουμε ξεκινήσει με επιτυχία μια DoS επίθεση από SYN flooding, μπορούμε να τρέξουμε την εντολή (σε άλλο παράθυρο στη μηχανή του θύματος):
   netstat -n | grep tcp

```
agiskallas@debian-agis:~$ netstat -n | grep tcp
tcp        0      0 192.168.1.10:22         111.111.111.111:57375   SYN_RECV
tcp        0      0 192.168.1.10:22         111.111.111.111:57796   SYN_RECV
tcp        0      0 192.168.1.10:22         111.111.111.111:45378   SYN_RECV
tcp        0      0 192.168.1.10:22         111.111.111.111:51572   SYN_RECV
tcp        0      0 192.168.1.10:22         111.111.111.111:63571   SYN_RECV
tcp6       0      0 2a02:586:c824:778:39380 2a04:4e42:8d::644:80    TIME_WAIT
```

Figure 5:Netstat filtering only tcp

Το VM έχει λάβει το πακέτο SYN για να ξεκινήσει το 3-way handshake, αλλά δεν λαμβάνει το ACK για να το ολοκληρώσει. Το SYN έχει χρονισμό περί τα 75''. Αν δεν λάβει απάντηση σε αυτό το διάστημα τερματίζει την προσπάθεια σύνδεσης.

---

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

- **netstat-a**
  Εμφανίζει όλες τις διαθέσιμες πληροφορίες
- **netstat -at**
  Εμφανίζει όλες τις tcp συνδέσεις

- **netstat -au**
  Εμφανίζει όλες τις udp συνδέσεις

- **netstat -l**
  Εμφανίζει όλες τα listening sockets

- **netstat -lt**
  Εμφανίζει όλες τα listening tcp sockets

- **netstat -lu**
  Εμφανίζει όλες τα listening udp pockets

- **netstat -s**
  Εμφανίζει στατιστικά στοιχεία για όλα τα πρωτόκολλα

- **netstat -st**
  Εμφανίζει στατιστικά στοιχεία για το tcp

- **netstat -su**
  Εμφανίζει στατιστικά στοιχεία για το udp

- **netstat -tp**
  Εμφανίζει τις tcp συνδέσεις μαζί με το πρόγραμμα στο οποίο ανήκουν

- **netstat -ac 5 | grep tcp**
  Καταγράφει όλα τα πακέτα ανά 5” και η έξοδος του περνάει στο grep το οποίο εμφανίζει μόνο τις γραμμές που περιέχουν τον όρο tcp.

- **netstat -r**
  Εμφανίζει όλα τα routing tables

- **netstat -c**
  Καταγράφει συνέχεια πακέτα και εμφανίζει στατιστικά δικτύου

- **netstat -ap | grep http**
  Καταγράφει όλα τα πακέτα μαζί με το πρόγραμμα στο οποίο ανήκουν και η έξοδος του περνάει στο grep το οποίο εμφανίζει μόνο τις γραμμές που περιέχουν τον όρο http.

- Με την εντολή **netstat -t | grep -E ‘ssh | https’** μπορούμε να δούμε τα στατιστικά χρήσης των υπηρεσιών ssh και https.

- Εκτελούμε τις εντολές: **netstat -tap | grep LISTEN** και **netstat -tap | grep ESTABLISHED**

Figure 6:Results from the above commands

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

- Με την χρήση της εντολής netcat κάνουμε port scanning στο VM:

nc -z -v domain.com 20-25

Εντοπίζουμε ανοιχτή την πόρτα 22.

- Στέλνουμε ένα αρχείο από τον host υπολογιστή στο VM εκτελώντας αντίστοιχα τις παρακάτω εντολές:

nc 192.168.1.XX 4444 < file_name (host)
nc -lnvp 4444 > file_name (VM)

- Δημιουργούμε μια backdoor πόρτα στο VM και εκτελούμε εντολές απομακρυσμένα από τον host υπολογιστή ως εξής:

nc -lnvp 4444 -e "/bin/bash" (VM)
nc 192.168.1.XX 4444 (host)

Μπορούμε να αναγνωρίσουμε ότι είναι ανοιχτή η πόρτα με την εντολή:

sudo tcpdump -i enp0s3 -n 'src 192.168.1.XX' and not arp