Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

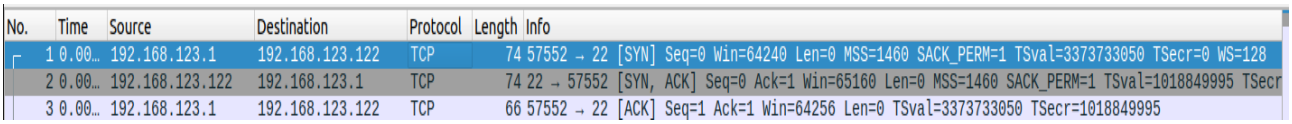
Άσκηση 4
DoS,DDoS,tcpdump
netcat,netstat

Αναγνωστόπουλος Άγγελος Νικόλαος
5ο Έτος ΗΜΤΥ
up1066593

1) Three-way-handshake με tcpdump:

Για να είναι πιο ευανάγνωστα τα αποτελέσματα θα κάνουμε το βήμα αυτό με χρήση wireshark (το οποίο είναι μία γραφική διεπαφή για το tcpdump). Τα υπόλοιπα ερωτήματα της άσκησης γίνονται κανονικά από το terminal, όμως το wireshark μας επιτρέπει να δούμε πολύ καλύτερα την χειραψία του TCP και να εξετάσουμε τα πακέτα που αυτή περιλαμβάνει.

Σκανάρουμε το εικονικό δίκτυο που έχουμε δημιουργήσει για τα VM μας, με IPv4 range 192.168.123.XYZ. Τα πακέτα που μας ενδιαφέρουν είναι τα 3 πρώτα. Παρατηρούμε ότι το πρώτο πακέτο έχει αναμένο το SYN bit, το δέυτερο τα SYN και ACK και το τρίτο μόνο το ACK, όπως και θα περιμέναμε. Επίσης ο σχετικός αριθμός ακολουθίας (Seq) αυξάνεται κάθε φορά κατά 1, υποδηλώνοντας ότι πρόκειται για το επόμενο TCP πακέτο. Μετά από την εγκατάσταση της χειραψίας μπορεί να ξεκινήσει να δουλεύει το SSH.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00…	192.168.123.1	192.168.123.122	TCP	74	57552 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3373733050 TSecr=0 WS=128
2	0.00…	192.168.123.122	192.168.123.1	TCP	74	22 → 57552 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1018849995 TSecr
3	0.00…	192.168.123.1	192.168.123.122	TCP	66	57552 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3373733050 TSecr=1018849995

Figure 1: Wireshark capture of TCP handshake

2) Εκτέλεση εντολών:

tcpdump -v -n host 192.168.1.105
Επέστρεψε μου με κάποιες λεπτομέριες όλα τα πακέτα χωρίς να χρησιμοποιήσεις dns (Δλδ. μην μεταφράσεις τα ονόματα σε διευθύνσεις IP και αντίστροφα)

tcpdump -vvv -nn -i eth0 -s 1514 host 192.168.1.105 -S -X -c 5
Με πολλές λεπτομέριες, για το interface eth0 και για μέγεθος πακέτου 1514 bytes, χωρίς να κάνεις μετάφραση ονομάτων ή lookups, επέστρεψέ μου για τα 5 πρώτα πακέτα, ολόκληρα τα πακέτα που κατέγραψες.

tcpdump -vvv -nn -i wlan0 -s 1514 host 192.168.1.105 -S -X -c 5
Το ίδιο για το wireless interface

tcpdump -nnvvvXSs 1514 host 192.168.1.105 and dst port 22
Τα nnvvvXSs τα είδαμε ήδη, εδώ όμως επιστρέφει μόνο τα πακέτα πυο προορίζονται για την θύρα 22 (by default ssh)

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'
Για το iface eth0 και τα 5 πρώτα πακέτα, επέστρεψε μου ολόκληρα τα πακέτα που ξεκινάνε από το src και πάνε στην port 22 του dst

tcpdump -vvv -nn -i eth0 -s 1514 -S -X -c 5 src or dst 71.98.70.149
Όλα τα πακέτα που αφορούν την ip src/dst (Πιάνει και input και output)

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'
Έιτε την κίνηση από το iface wlan0 του src, είτε τα πακέτα που φτάνουν στην θύρα 22 του dst

tcpdump udp -i wlan0
Πιάσε μόνο τα udp πακέτα του ασύρματου iface

tcpdump udp -i any -c 10
Πιάσε μόνο τα 10 πρώτα udp πακέτα σε όλα τα ifaces

Ενδεικτικά, μία σύνδεση στο github όσο κάνουμε καταγραφή με το tcpdump, μας επιστρέφει το εξής αποτέλεσμα:

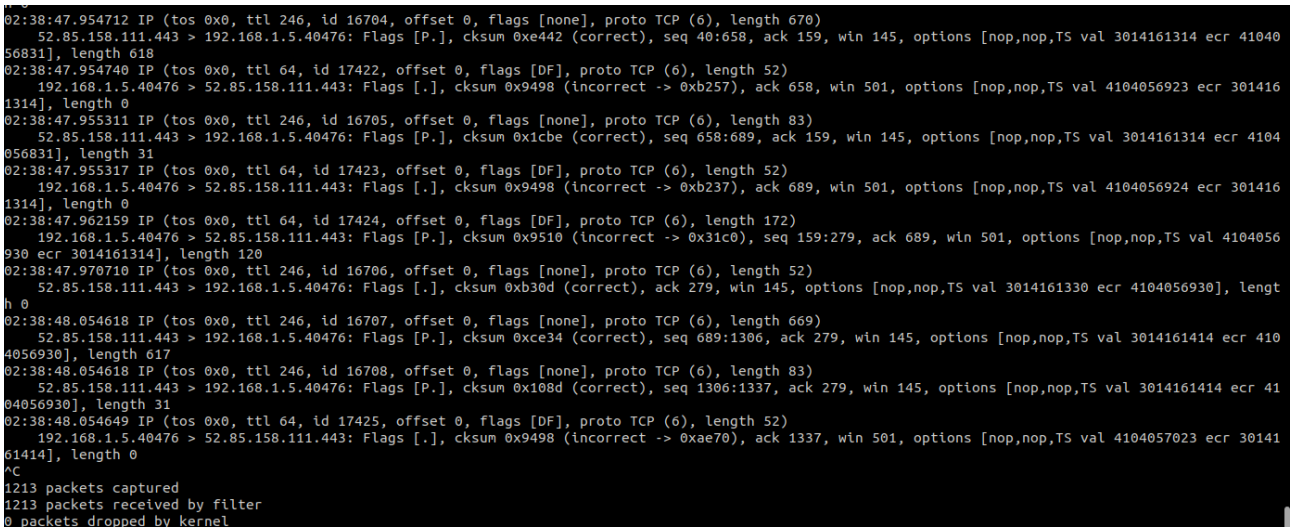


Figure 2: Github connection output on tcpdump

3) Το ερώτημα αυτό το έκανα με το δικό μου script που μου ζητήσατε να υλοποιήσω για την βαθμολόγιση των ασκήσεων στους DNS κατά την φάση του testing. Σας επισυνάπτω εδώ το output. Τον κώδικα μπορούμε να τον συζητήσουμε και παρέα αλλά είναι ένα απλό python script και υπάρχει όλο στο link: https://github.com/AngelosAnagnostopoulos/networks_security_scripts

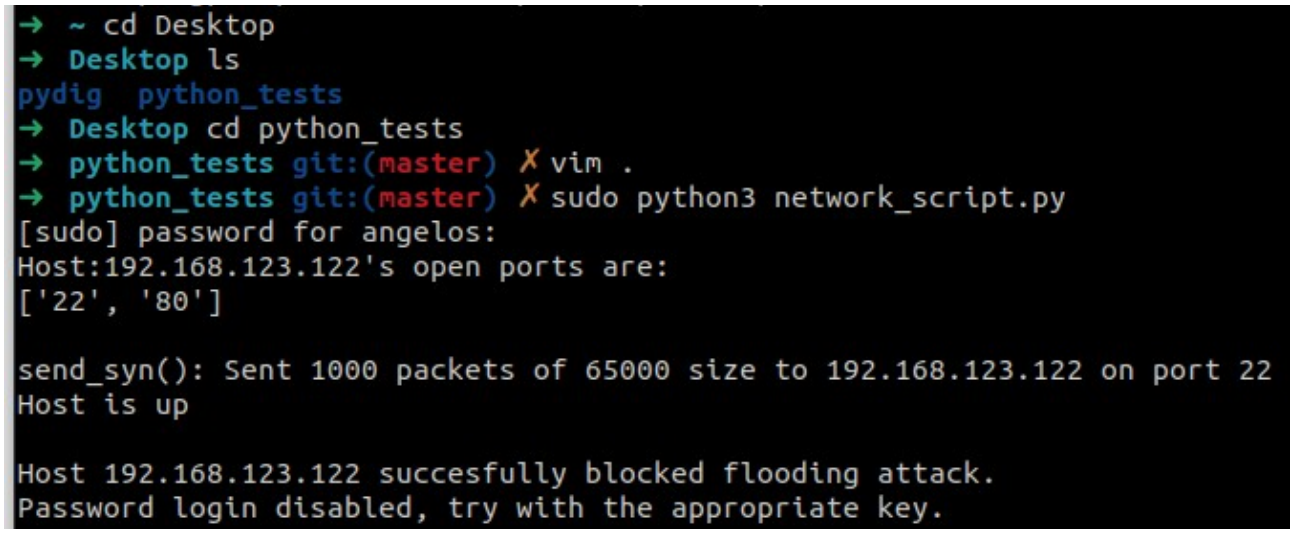


Figure 3: Custom network script output for VM

Εάν καταφέρναμε να “κρεμάσουμε” τον server, δεν θα είχαμε καθόλου response. Μιας και έχουμε όμως αρκετούς πόρους για να αντέξουμε την επίθεση, το αποτέλεσμα του netcat είναι το εξής ενδιαφέρον. Βλέπουμε πολλές συνδέσεις σε διάφορες πόρτες να περιμένουν στο SYN_RECV και στο TIME_WAIT. Αυτό συμβαίνει γιατί το tcp περιμένει το επόμενο πακέτο για την εγκατάσταση του 3-way-handshake που όμως δεν έρχεται ποτέ. Μετά από λίγη ώρα το TTL των πακέτων έχει ξεπεραστεί και γίνονται drop. Αν όμως η επίθεση συνέχιζε για ώρα τότε ο server μας ενδεχομένως να είχε πρόβλημα.

```
tcp        0      0 debian:ssh              RevivedPP:63917         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:42462         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:50976         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:57105         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:19189         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:19280         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:15872         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:37308         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:62186         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:21829         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:59636         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:22308         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:37758         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:13343         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:23784         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:22185         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:15040         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:42289         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:20116         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:11213         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:37497         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:46490         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:13388         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:58881         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:60075         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:29881         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:2220          SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:4089          SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:17912         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:27171         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:32589         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:8971          SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:35043         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:55784         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:45545         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:4052          SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:28071         SYN_RECV
tcp        0      0 debian:ssh              RevivedPP:26100         SYN_RECV
tcp6       0      0 debian:http             RevivedPP:48362         TIME_WAIT
tcp6       0      0 debian:http             RevivedPP:33860         TIME_WAIT
tcp6       0      0 debian:http             RevivedPP:48378         TIME_WAIT
tcp6       0      0 debian:http             RevivedPP:48388         TIME_WAIT
tcp6       0      0 debian:http             RevivedPP:48400         TIME_WAIT
tcp6       0      0 debian:http             RevivedPP:48416         TIME_WAIT
tcp6       0      0 debian:http             RevivedPP:48356         TIME_WAIT
angelos@debian ~ % sudo fail2ban-client set sshd unbanip 192.168.122.1
```

Figure 4: Netstat output during flood attack

```
0
angelos@debian ~ % netstat | grep tcp
tcp        0      0 debian:ssh              RevivedPP:54684         ESTABLISHED
angelos@debian ~ %
```

Figure 5: Netstat output after flood attack

4) Από τα man pages του netstat:

netstat [**−AaLlnW**] [**−f** *address_family* | **−p** *protocol*] [**−M** *core*] [**−N** *system*]
netstat [**−gilns**] [**−f** *address_family*] [**−M** *core*] [**−N** *system*]
netstat −i | **−I** *interface* [**−w** *wait*] [**−abdgt**] [**−M** *core*] [**−N** *system*]
netstat −s [**−s**] [**−f** *address_family* | **−p** *protocol*] [**−M** *core*] [**−N** *system*]
netstat −i | **−I** *interface* **−s** [**−f** *address_family* | **−p** *protocol*] [**−M** *core*] [**−N** *system*]
netstat −m [**−M** *core*] [**−N** *system*]
netstat −r [**−Aaln**] [**−f** *address_family*] [**−M** *core*] [**−N** *system*]
netstat −rs [**−s**] [**−M** *core*] [**−N** *system*]

Και η έξοδος του netstat -tap για τα tcp πακέτα LISTEN και ESTABLISHED:

```
→ python_tests git:(master) ✗ sudo netstat -tap | grep LISTEN
tcp        0      0 0.0.0.0:50511           0.0.0.0:*               LISTEN      2745/rpc.mountd
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      923/systemd-resolve
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      1378/sshd: /usr/sbi
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN      1/init
tcp        0      0 localhost:6463          0.0.0.0:*               LISTEN      10543/Discord --typ
tcp        0      0 localhost:postgresql    0.0.0.0:*               LISTEN      1423/postgres
tcp        0      0 0.0.0.0:nfs             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:51959           0.0.0.0:*               LISTEN      2745/rpc.mountd
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      91235/qemu-system-x
tcp        0      0 0.0.0.0:54955           0.0.0.0:*               LISTEN      2745/rpc.mountd
tcp        0      0 RevivedPP:domain        0.0.0.0:*               LISTEN      1494/dnsmasq
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      26574/cupsd
tcp        0      0 0.0.0.0:42053           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:47081           0.0.0.0:*               LISTEN      2741/rpc.statd
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN      1/init
tcp6       0      0 [::]:52677              [::]:*                  LISTEN      2745/rpc.mountd
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      26574/cupsd
tcp6       0      0 [::]:nfs                [::]:*                  LISTEN      -
tcp6       0      0 [::]:56937              [::]:*                  LISTEN      2745/rpc.mountd
tcp6       0      0 [::]:40535              [::]:*                  LISTEN      2745/rpc.mountd
tcp6       0      0 [::]:42043              [::]:*                  LISTEN      2741/rpc.statd
tcp6       0      0 [::]:43813              [::]:*                  LISTEN      -
```

```
→ python_tests git:(master) ✗ sudo netstat -tap | grep ESTABLISHED
tcp        0      0 RevivedPP:39410         okeanos:ssh             ESTABLISHED 93037/ssh
tcp        0      0 RevivedPP:59418         123.208.120.34.bc:https ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:60032         151.101.192.134:https   ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:46958         ec2-44-239-182-10:https ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:43164         stackoverflow.com:https ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:34966         146.75.118.137:https    ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:46464         ec2-35-174-127-31:https ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:60004         151.101.192.134:https   ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:35066         93.184.220.29:http      ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:60012         151.101.192.134:https   ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:53718         stackoverflow.com:https ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:33080         146.75.118.49:https     ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:49588         server-52-85-158-:https ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:54684         192.168.123.122:ssh     ESTABLISHED 91388/ssh
tcp        0      0 RevivedPP:53330         lb-140-82-114-25-:https ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:55520         162.159.134.234:https   ESTABLISHED 10497/Discord --typ
tcp        0      0 RevivedPP:33538         ec2-52-89-114-252:https ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:60026         151.101.192.134:https   ESTABLISHED 4647/firefox
tcp        0      0 RevivedPP:42450         140.227.186.35.bc:https ESTABLISHED 4647/firefox
tcp6       0      0 RevivedPP:36714         2606:4700::6812:1:https ESTABLISHED 4647/firefox
tcp6       0      0 RevivedPP:47250         2606:4700::6810:9:https ESTABLISHED 4647/firefox
tcp6       0      0 RevivedPP:53754         2a02:582:a00::d4cd:http ESTABLISHED 4647/firefox
```

Τα στατιστικά της κίνησής μας μπορούμε να τα δούμε με την εντολή netstat -s και την εντολή ss -s:

```
→ python_tests git:(master) ✗ ss -s
Total: 1260
TCP:   33 (estab 8, closed 0, orphaned 3, timewait 0)

Transport Total     IP        IPv6
RAW       1         0         1
UDP       69        38        31
TCP       33        24        9
INET      103       62        41
FRAG      0         0         0
```

```
→ python_tests git:(master) ✗ netstat -s
Ip:
    Forwarding: 1
    665200 total packets received
    1 with invalid headers
    1013 forwarded
    0 incoming packets discarded
    655054 incoming packets delivered
    519380 requests sent out
    20 outgoing packets dropped
Icmp:
    440 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 417
        echo requests: 5
        echo replies: 16
        timestamp reply: 2
    429 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 392
        echo requests: 30
        echo replies: 5
        timestamp requests: 2
```

5) Για το netcat στο VM μας έχουμε:

```
→ python_tests git:(master) ✗ netcat -z -v 192.168.123.122 20-25
netcat: connect to 192.168.123.122 port 20 (tcp) failed: Connection refused
netcat: connect to 192.168.123.122 port 21 (tcp) failed: Connection refused
Connection to 192.168.123.122 22 port [tcp/ssh] succeeded!
netcat: connect to 192.168.123.122 port 23 (tcp) failed: Connection refused
netcat: connect to 192.168.123.122 port 24 (tcp) failed: Connection refused
netcat: connect to 192.168.123.122 port 25 (tcp) failed: Connection refused
→ python_tests git:(master) ✗
```

Μπορούμε να στείλουμε τα περιεχόμενα ενός αρχείου κάνοντας τα pipe από το cat. Στην εικόνα φαίνεται ο netcat server που στήθηκε στο VM, καθώς και αυτό που του στείλαμε με το host machine μας μέσω της τελευταίας εντολής:

```
angelos@debian ~ % netcat -l 4444
192.168.123.122,up1066593
_
```

```
netcat: port number invalid: test
→ python_tests git:(master) ✗ cat servers.txt |  netcat 192.168.123.122 4444
```

Figure 6: Two terminals shown in the same picture. The VM has a running server and receives the text's contents through the host machine on port 4444.

Με αυτό τον τρόπο μπορούμε να εκτελέσουμε όποια εντολή θέλουμε από το host machine και μέσω του piping και του netcat, στην θύρα 4444 του VM θα λάβουμε το αντίστοιχο output. Αυτό θα μπορούσε να το ανιχνεύσει ένα απλό port scanning του VM μας, που θα μας ενημέρωνε για την ύπαρξη ανοιχτής θύρας στην 4444, πχ. με την ακριβώς παραπάνω εντολή, αλλάζοντας το port range. Για του λόγου το αληθές:

```
→ python_tests git:(master) ✗ netcat -z -v 192.168.123.122 4444
Connection to 192.168.123.122 4444 port [tcp/*] succeeded!
```

Figure 7: Scanning the open port 4444 while server is running

Fin