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).

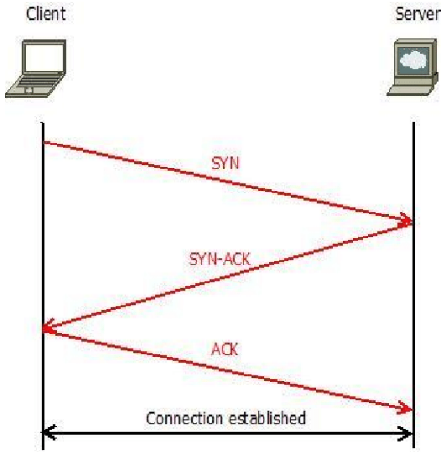
Am creat o mașină virtuală de bază (base), pe care am clonat-o pentru a crea cele 3 mașini virtuale. Una dintre ele este victima (C1), una este atacatorul (C2) și cealaltă este observatorul (Router):

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

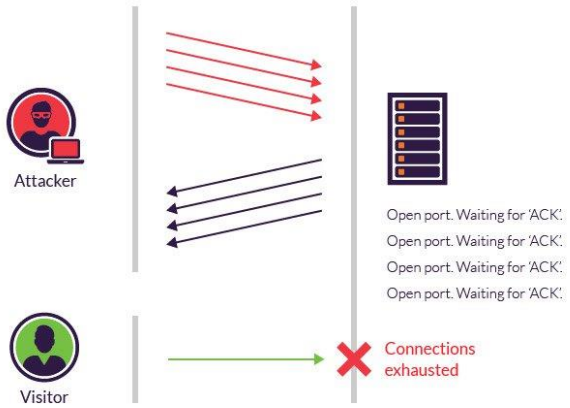
Exercițiul 2 – Atac SYN Flooding

Un atac cibernetic de tip DoS (Denial of Service) este o încercare frauduloasă de a indisponibiliza sau bloca resursele unui calculator. Un atac asupra conectivităţii 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

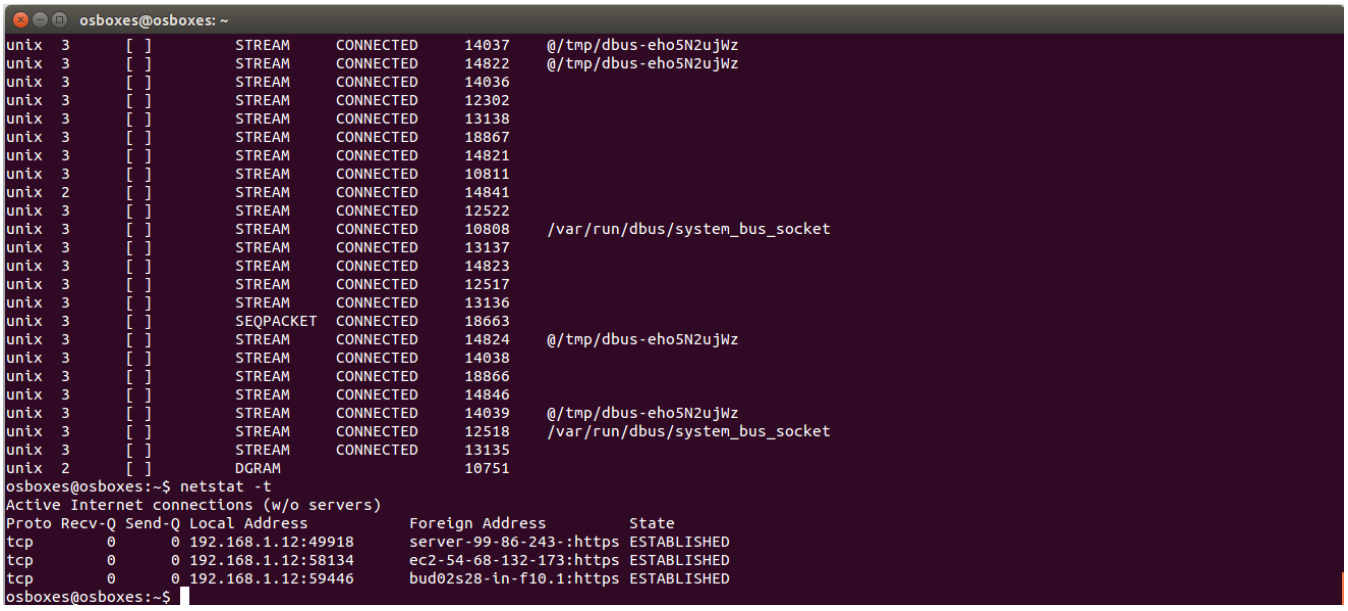
Aplicații folosite:

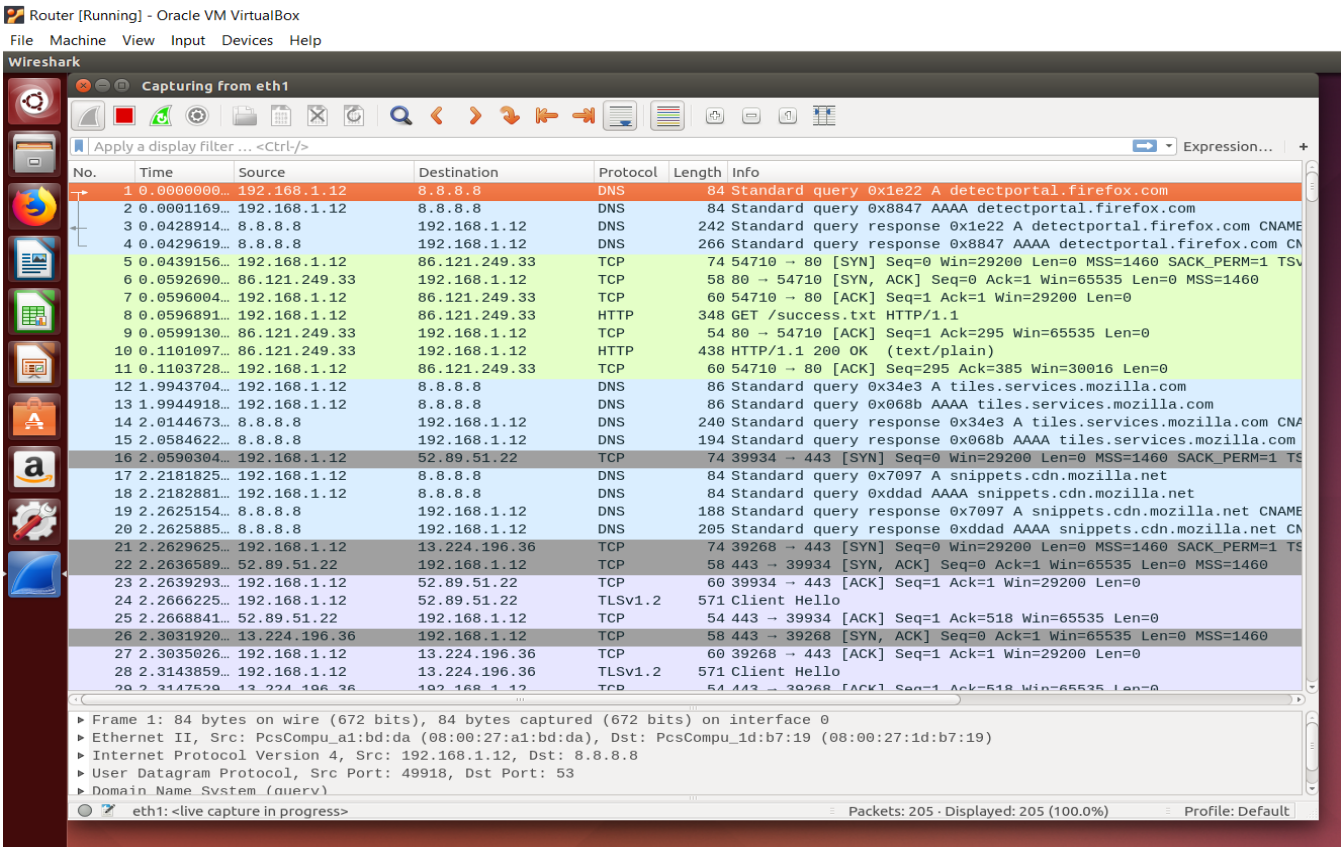
Wireshark – pentru a monitoriza traficul de date din rețeaua locală
Netwox – pentru implementarea atacurilor

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 ESTABILISHED.





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

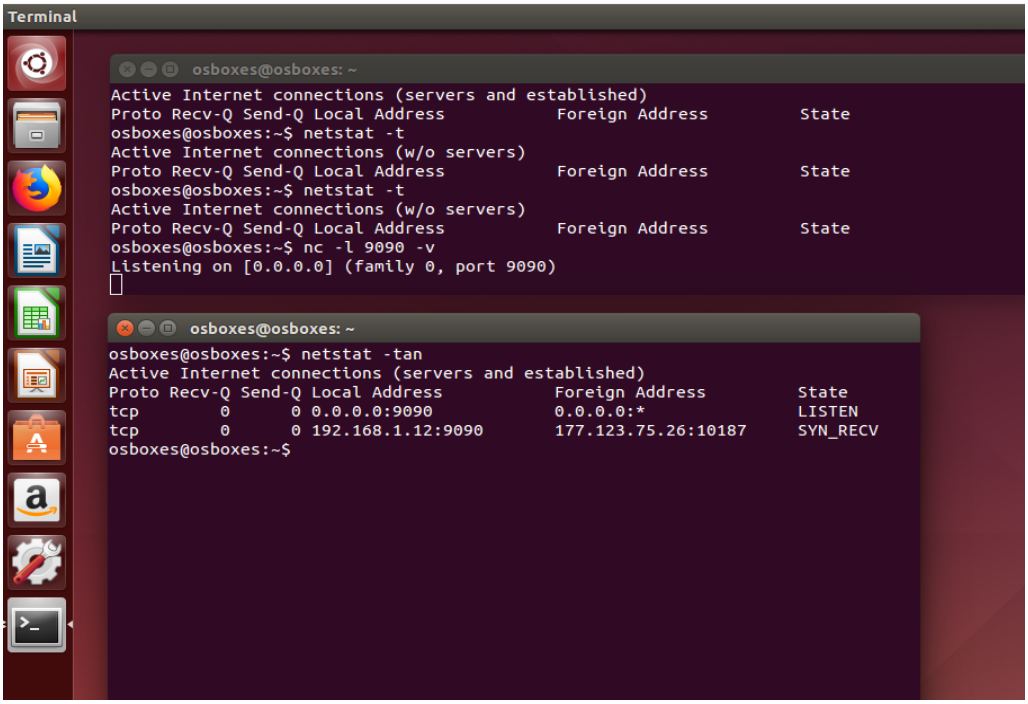
Mașina atacator rulează comanda `sudo netwox 76 -i 192.168.1.12 -p 9090`, care (prin tool-ul 76 Synflood al comenzii `netwox`) trimite multe pachete TCP SYN.

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:

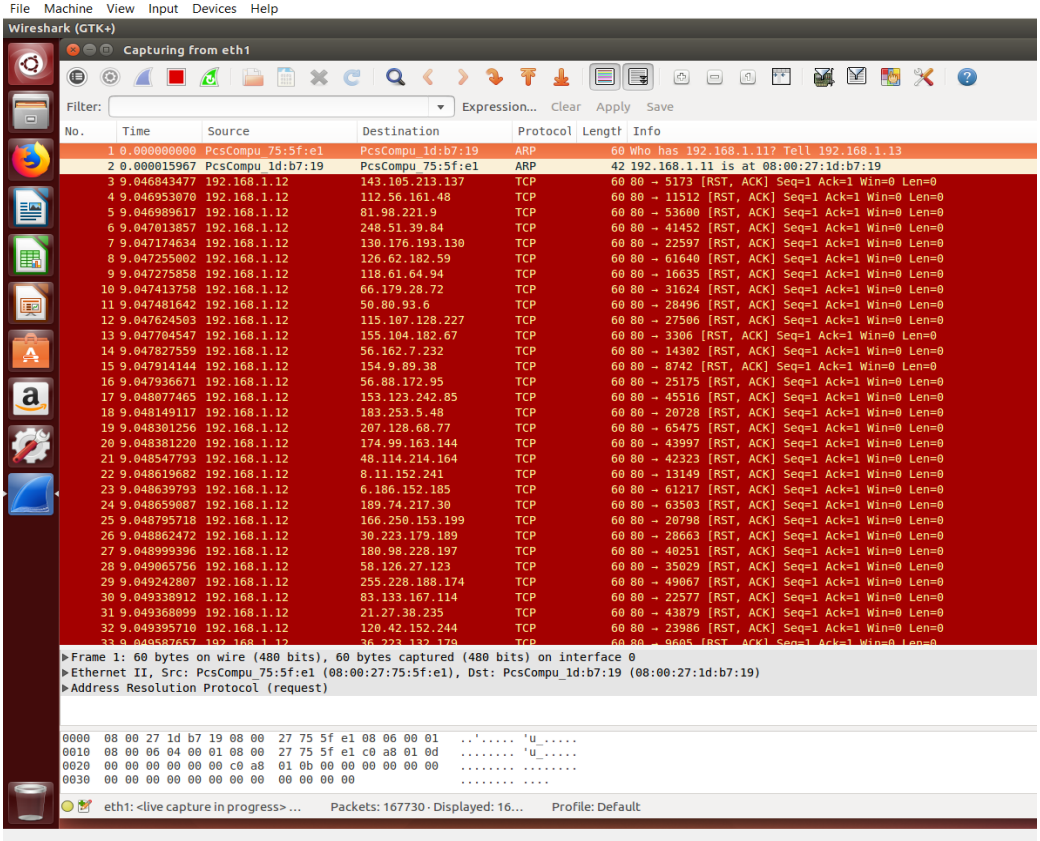
C1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



Router [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



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