Types of scans defended against

- TCP Half Open Scan
- TCP Null Scan
- UDP Scan

https://nmap.org/book/man-port-scanning-techniques.html

Kernel module makes use of netfilter framework and intercepts all the incoming packets using hooks. We, looking into the packet can decide whether to send it through (using NF_ACCEPT) or drop the packet (using NF_DROP).

https://www.geeksforgeeks.org/services-and-segment-structure-in-tcp/

It identifies the packet targeted by looking into the packet header which contains various types of information such as sender address, receiver address/port, protocol used etc. Finally, after performing various computations, it drops the suspected packets via NF_DROP.

Compiling and Loading:

1. In the file packet_filter.c at line 48 change the ip to the ip of VM1. This is done to simplify the code or else we would have to maintain a separate data for all the connecting ips.
2. Type “make” to compile the script.
3. Type “make load” to load the script in the kernel.
4. Perform the test commands (Given below).
5. Type “make unload”. After this command all the data collected so far will be logged. The module is constantly collecting and blocking the packets, calling unload is a signal to log the insights on data collected so far.
6. Type “dmesg” to check the logs.

Testing:

TCP Half Open Scans: nmap by default does tcp half open scans.

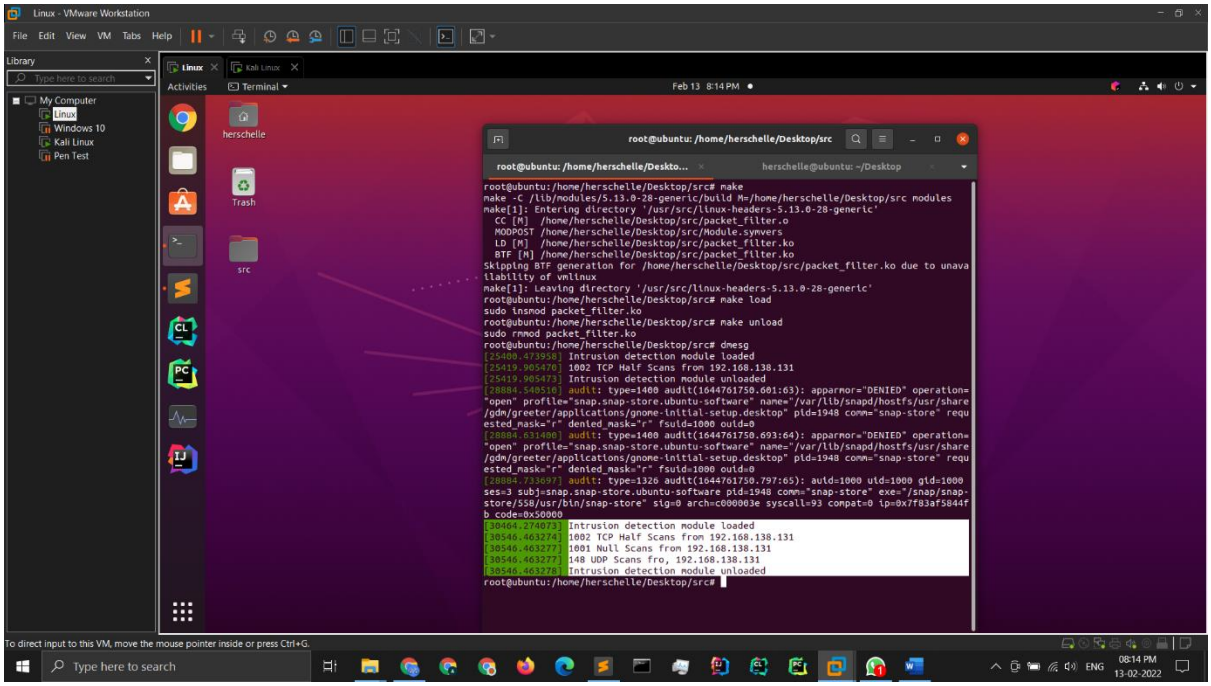
Command: nmap 192.168.138.130

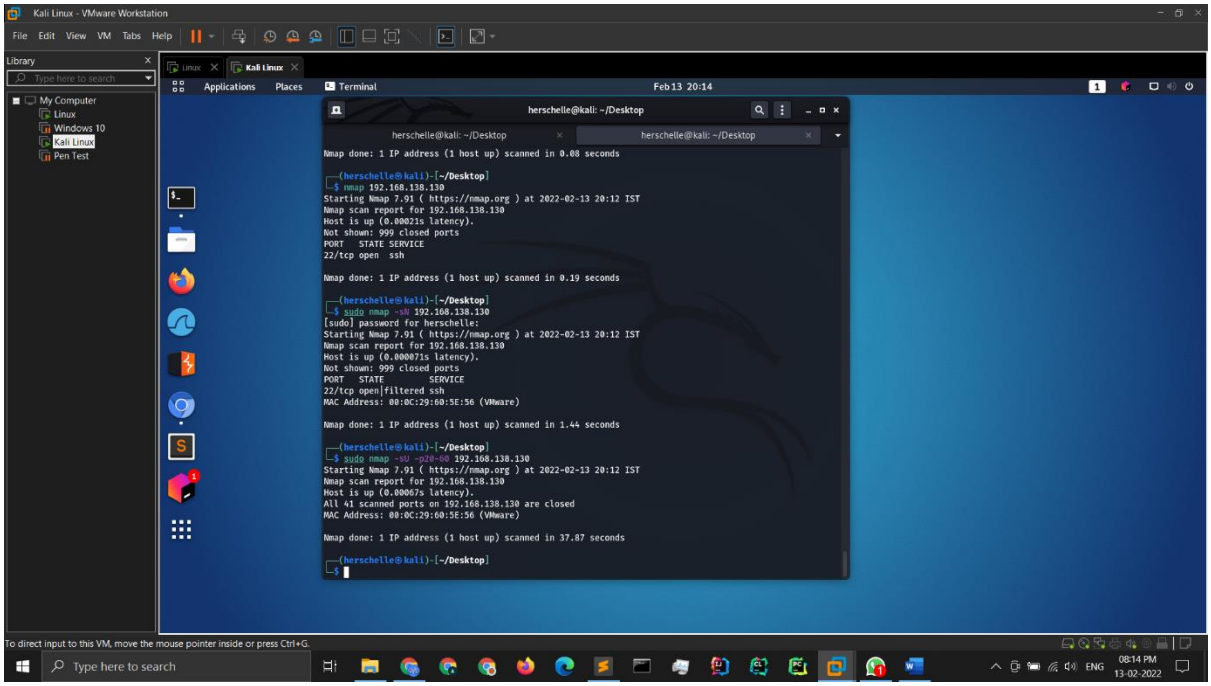
UDP Scans: -sU for udp and -p20-60 for scanning ports 20-60. UDP scans are very slow and could take 18 hours to scan all 65536 ports. Scanning 40 ports takes around 40 seconds.

Command: nmap -sU -p20-60 192.168.138.130

TCP Null Scans:

Command: nmap -sN 192.168.138.130


Linux - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Linux
Windows 10
Kali Linux
Pen Test
Activities
Terminal
Feb 13 8:14 PM
herschelle
Trash
src
root@ubuntu: /home/herschelle/Desktop/src
root@ubuntu: /home/herschelle/Deskto...
herschelle@ubuntu: ~/Desktop
root@ubuntu:/home/herschelle/Desktop/src# make
make -C /lib/modules/5.13.0-28-generic/build M=/home/herschelle/Desktop/src modules
make[1]: Entering directory '/usr/src/linux-headers-5.13.0-28-generic'
CC [M] /home/herschelle/Desktop/src/packet_filter.o
MODPOST /home/herschelle/Desktop/src/Module.symvers
LD [M] /home/herschelle/Desktop/src/packet_filter.ko
BTF [M] /home/herschelle/Desktop/src/packet_filter.ko
Skipping BTF generation for /home/herschelle/Desktop/src/packet_filter.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.13.0-28-generic'
root@ubuntu:/home/herschelle/Desktop/src# make load
sudo insmod packet_filter.ko
root@ubuntu:/home/herschelle/Desktop/src# make unload
sudo rmmod packet_filter.ko
root@ubuntu:/home/herschelle/Desktop/src# dmesg
[25403.473958] Intrusion detection module loaded
[25419.905470] 1002 TCP Half Scans from 192.168.138.131
[25419.905473] Intrusion detection module unloaded
[28884.540516] audit: type=1400 audit(1644761750.601:63): apparmor="DENIED" operation="open" profile="snap.snap-store.ubuntu-software" name="/var/lib/snapd/hostfs/usr/share/gdm/greeter/applications/gnome-initial-setup.desktop" pid=1948 comm="snap-store" requested_mask="r" denied_mask="r" fsuid=1000 ouid=0
[28884.631490] audit: type=1400 audit(1644761750.693:64): apparmor="DENIED" operation="open" profile="snap.snap-store.ubuntu-software" name="/var/lib/snapd/hostfs/usr/share/gdm/greeter/applications/gnome-initial-setup.desktop" pid=1948 comm="snap-store" requested_mask="r" denied_mask="r" fsuid=1000 ouid=0
[28884.733697] audit: type=1326 audit(1644761750.797:65): auid=1000 uid=1000 gid=1000 ses=3 subj=snap.snap-store.ubuntu-software pid=1948 comm="snap-store" exe="/snap/snap-store/558/usr/bin/snap-store" sig=0 arch=c000003e syscall=93 compat=0 ip=0x7f83af5844fb code=0x50000
[30404.274073] Intrusion detection module loaded
[30546.463274] 1002 TCP Half Scans from 192.168.138.131
[30546.463277] 1001 Null Scans from 192.168.138.131
[30546.463277] 148 UDP Scans fro, 192.168.138.131
[30546.463278] Intrusion detection module unloaded
root@ubuntu:/home/herschelle/Desktop/src#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
08:14 PM
13-02-2022


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Linux
Windows 10
Kali Linux
Pen Test
Applications
Places
Terminal
Feb 13 20:14
herschelle@kali: ~/Desktop
herschelle@kali: ~/Desktop
herschelle@kali: ~/Desktop
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
┌──(herschelle㉿kali)-[~/Desktop]
└─$ nmap 192.168.138.130
Starting Nmap 7.91 (https://nmap.org) at 2022-02-13 20:12 IST
Nmap scan report for 192.168.138.130
Host is up (0.00021s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp open ssh
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
┌──(herschelle㉿kali)-[~/Desktop]
└─$ sudo nmap -sN 192.168.138.130
[sudo] password for herschelle:
Starting Nmap 7.91 (https://nmap.org) at 2022-02-13 20:12 IST
Nmap scan report for 192.168.138.130
Host is up (0.00071s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp open|filtered ssh
MAC Address: 00:0C:29:60:5E:56 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
┌──(herschelle㉿kali)-[~/Desktop]
└─$ sudo nmap -sU -p20-60 192.168.138.130
Starting Nmap 7.91 (https://nmap.org) at 2022-02-13 20:12 IST
Nmap scan report for 192.168.138.130
Host is up (0.00067s latency).
All 41 scanned ports on 192.168.138.130 are closed
MAC Address: 00:0C:29:60:5E:56 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 37.87 seconds
┌──(herschelle㉿kali)-[~/Desktop]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
08:14 PM
13-02-2022