

Attactive Directory

Introduction: Attacktive Directory is a simulated environment designed to replicate a corporate Active Directory infrastructure for educational and testing purposes. This environment presents various vulnerabilities and misconfigurations commonly found in real-world Active Directory deployments. This report aims to provide a comprehensive overview of the Attacktive Directory environment, focusing on enumeration, exploitation, and privilege escalation techniques.

Task 1: Deploy The Machine The initial task involves deploying the Attacktive Directory environment, which provides a controlled setting for conducting security assessments and learning about Active Directory vulnerabilities.

Task 2: Setup This task involves setting up the environment for exploration and exploitation. It may include configuring network settings, establishing connections, and preparing tools for enumeration and exploitation.

Task 3: Enumeration Welcome to Attacktive Directory Enumeration is a crucial phase in any security assessment. In this task, the focus is on gathering information about the Active Directory environment, including domain structure, domain controllers, user accounts, group memberships, and other relevant entities.

Task 4: Enumeration Enumerating Users via Kerberos Kerberos is the primary authentication protocol used in Active Directory environments. By enumerating users via Kerberos, attackers can identify valid user accounts and potentially exploit weak credentials or misconfigurations.

Task 5: Exploitation Abusing Kerberos Building upon the information gathered during enumeration, attackers can exploit vulnerabilities in the Kerberos authentication system to gain unauthorized access to resources within the Active Directory environment. Common exploitation techniques include Kerberoasting, Pass-the-Ticket attacks, and Golden Ticket attacks.

Task 6: Enumeration Back to the Basics In this task, the focus returns to enumeration, emphasizing the importance of thorough reconnaissance in identifying potential attack vectors and weaknesses within the Active Directory infrastructure.

Task 7: Domain Privilege Escalation Elevating Privileges within the Domain Privilege escalation is the process of obtaining higher levels of access within the Active Directory domain than initially granted. Attackers leverage misconfigurations, vulnerabilities, and weaknesses to escalate privileges and gain control over critical systems and data.

Task 8: Flag Submission Panel The final task involves submitting flags, which typically represent achievements or milestones reached during the assessment. Flags may include sensitive information extracted from compromised systems or evidence of successful exploitation.

cs-sa07-24019
John_Mbithi_Mutave

The screenshot displays the TryHackMe web application interface. At the top, a navigation bar includes the TryHackMe logo, links to Dashboard, Learn, Compete, and Other, and a user profile section with 'Access Machines', a search icon, a notification bell, a 'Go Premium' button, and a user avatar.

The main content area features a 'Target Machine Information' table:

Title	Target IP Address	Expires	
AttacktiveDirect	10.10.73.148	25min 54s	? Add 1 hour Terminate

Below the table is a list of tasks:

- Task 1: Deploy The Machine (Intro)
- Task 2: Setup (Intro)
- Task 3: Welcome to Attacktive Directory (Enumeration)
- Task 4: Enumerating Users via Kerberos (Enumeration)
- Task 5: Abusing Kerberos (Exploitation)
- Task 6: Back to the Basics (Enumeration)
- Task 7: Elevating Privileges within the Domain (Domain Privilege Escalation)
- Task 8: Flag Submission Panel (Flag Submission Panel)

A Windows taskbar is visible at the bottom, showing the Start button, a search bar, and various application icons. A notification from Microsoft 365 and Office is present in the bottom right corner of the taskbar.

TryHackMe

Mu

ChatGPT

Spotify

Latest

(61) W

CSA2-2

Hack T

tryhackme.com/r/room/attacktivedirectory

Title	Target IP Address	Expires
AttacktiveDirect	10.10.73.148	24min 32s

Task 1

Intro

Deploy The Machine

Accessing Attacktive

To access the Virtual Machine, you will need to first connect to our network using OpenVPN

(Please note the browser-based machine will be able to access this machine, you will not need to do anything else)

Answer the questions below

Go to your [access](#) page. Select your VPN

OpenVPN Access Details

VPN Server Name	EU-Regular-1
Server Status	✓
Connected	✓
Internal Virtual IP Address	10.8.166.178

No answer needed

Return to your access page. You can verify you are connected by looking on w

S&P 500
-0.39%

Search

cs-sa07-24019

John_Mbithi_Mutave

TryHackMe

Mu

ChatGPT

Spotify

Latest

(61) WhatsApp

CSA2-2

HackT

tryhackme.com/r/room/attacktivedirectory

Title	Target IP Address	Expires
AttacktiveDirect	10.10.73.148	23min 59s

Installing Bloodhound and Neo4j

Bloodhound is another tool that we'll be utilizing while attacking Attacktive Directo being bloodhound and neo4j. You can install it with the following command:

```
apt install bloodhound neo4j
```

Now that it's done, you're ready to go!

Troubleshooting

If you are having issues installing Bloodhound and Neo4j, try issuing the following c

```
apt update && apt upgrade
```

If you are having issues with Impacket, reach out to the [TryHackMe Discord](#) for help

Answer the questions below

Install Impacket, Bloodhound and Neo4j

No answer needed

Task 3

Enumeration

Welcome to Attacktive Directory

S&P 500
-0.39%

Search

cs-sa07-24019
John_Mbithi_Mutave

TryHa:Mu:ChatG:Spoti:Latest(61) W:CSA2:Hack:TrjXln(27) FeX.com:TryHa:Attack:TryHa:MSN:TryHa:

tryhackme.com/r/room/attacktivedirectory

?

Add 1 hour

Terminate

Title	Target IP Address	Expires
AttacktiveDirect	10.10.73.148	23min 15s

being an overly complex utility, it cannot enumerate everything. Therefore after an initial nmap scan we'll be using other utilities to help us enumerate the services running on the device.

For more information on nmap, check out the [nmap room](#).

Notes: Flags for each user account are available for submission. You can retrieve the flags for user accounts via RDP (Note: the login format is spookysc.local\User at the Window's login prompt) and Administrator via Evil-WinRM.

Answer the questions below

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

✓ Correct Answer

What is the NetBIOS-Domain Name of the machine?

✓ Correct Answer

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

✓ Correct Answer

Hint

Task 4 ✓ Enumeration Enumerating Users via Kerberos

Activate Windows
Go to Settings to activate Windows.

68°F
Partly cloudy

Search

ENG
UK

9:20 AM
6/14/2024

TryHackMeSolChatGPTSpotifyLatest(61) WCSA2HackTj(27) Fx.comTryHackAttackTryHackMSNTryHack

tryhackme.com/r/room/attacktivedirectory

?

Add 1 hour

Terminate

Title	Target IP Address	Expires
AttacktiveDirect	10.10.73.148	22min 33s

Note: Several users have informed me that the latest version of Kerbrute does not contain the UserEnum flag in Kerbrute, if that is the case with the version you have selected, try a older version!

Enumeration:

For this box, a modified [User List](#) and [Password List](#) will be used to cut down on time of enumeration of users and password hash cracking. It is **NOT** recommended to brute force credentials due to account lockout policies that we cannot enumerate on the domain controller.

Answer the questions below

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

✓ Correct Answer

Hint

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

✓ Correct Answer

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

✓ Correct Answer

Task 5

Exploitation

Abusing Kerberos

Activate Windows
Go to Settings to activate Windows.

68°F
Partly cloudy

Search

ENG
UK

9:21 AM
6/14/2024

cs-sa07-24019
John_Mbithi_Mutave

TryHackMe | Sol | ChatGPT | Spotify | Latest | (61) W | CSA2 | Hack | TryHackMe | (27) Fe | x.com | TryHackMe | Attack | TryHackMe | MSN | TryHackMe

tryhackme.com/room/attacktivedirectory

Title

AttacktiveDirect

Target IP Address

10.10.73.148

Expires

21min 42s

?

Add 1 hour

Terminate

Remember: Impacket may also need you to use a python version ≥ 3.7 . In the AttackBox you can do this by running your command with `python3.9 /opt/impacket/examples/GetNPUsers.py`.

Answer the questions below

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?

svc-admin

✓ Correct Answer

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

Kerberos 5 AS-REP etype 23

✓ Correct Answer

Hint

What mode is the hash?

18200

✓ Correct Answer

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

management2005

✓ Correct Answer

Task 6

Enumeration

Back to the Basics

Activate Windows

Go to Settings to activate Windows.

Nairobi express... Construction

Search

ENG UK

9:21 AM 6/14/2024

cs-sa07-24019
John_Mbithi_Mutave

TryHackMeSolChatGPTSpotifyLatest(61) WCSA2HackTTrj(27) Fx.comTryHackAttackTryHackMSNTryHack

tryhackme.com/room/attacktivedirectory

Title

AttacktiveDirect

Target IP Address

10.10.73.148

Expires

20min 54s

?

Add 1 hour

Terminate

smbclient

✓ Correct Answer

Hint

Which option will list shares?

-L

✓ Correct Answer

Hint

How many remote shares is the server listing?

6

✓ Correct Answer

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

backup

✓ Correct Answer

What is the content of the file?

YmFja3VwQHhNwb29reXNlYy5sb2NhbmDpiYWNRdXAyNTE3ODYw

✓ Correct Answer

Hint

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

backup@spookysec.local:backup2517860

✓ Correct Answer

Task 7

Domain Privilege Escalation

Elevating Privileges within the Domain

Activate Windows
Go to Settings to activate Windows.

68°F
Partly cloudy

Search

ENG
UK

9:22 AM
6/14/2024

cs-sa07-24019
John_Mbithi_Mutave

TryHackMeSolChatGPTSpotifyLatest(61) WiCSA2HackTn(27) FeX.comTryHackAttackTryHackMSNTryHack

tryhackme.com/r/room/attacktivedirectory

?

Add 1 hour

Terminate

Title	Target IP Address	Expires
AttacktiveDirect	10.10.73.148	20min 20s

domain controller) has to offer. Exploiting this, we will effectively have full control over the AD Domain.

Answer the questions below

What method allowed us to dump NTDS.DIT?

DRSUAPI

✓ Correct Answer

Hint

What is the Administrators NTLM hash?

0e0363213e37b94221497260b0bc4fc

✓ Correct Answer

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

Pass The Hash

✓ Correct Answer

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

-H

✓ Correct Answer

Hint

Task 8

Flag Submission

Flag Submission Panel

Activate Windows
Go to Settings to activate Windows.

68°F
Partly cloudy

Search

ENG
UK

9:23 AM
6/14/2024

cs-sa07-24019
John_Mbithi_Mutave

The screenshot shows a web browser window with the URL `tryhackme.com/r/room/attacktivedirectory`. The browser's address bar and tabs are visible at the top. The main content area displays the 'Flag Submission Panel' for 'Task 8'. The panel includes instructions: 'Submit the flags for each user account. They can be located on each user's desktop. If you enjoyed this box, you may also enjoy my [blog post!](#)'. Below the instructions, there are three rows of input fields for flags, each with a 'Correct Answer' button to its right. The flags are: `TryHackMe{K3rb3r0s_Pr3_4uth}` for 'svc-admin', `TryHackMe{B4ckM3UpSc0tty!}` for 'backup', and `TryHackMe{4ctiveD1rectoryM4st3r}` for 'Administrator'. The 'Expires' column shows '19min 43s'. At the bottom of the browser window, the Windows taskbar is visible, showing the system clock as 9:23 AM on 6/14/2024.

Title	Target IP Address	Expires
AttacktiveDirect	10.10.73.148	19min 43s

Flag Submission Panel

Submit the flags for each user account. They can be located on each user's desktop.

If you enjoyed this box, you may also enjoy my [blog post!](#)

Answer the questions below

svc-admin

✓ Correct Answer

backup

✓ Correct Answer

Administrator

✓ Correct Answer

The screenshot shows the same web browser window, but now displaying the 'AttacktiveDirectory' room's completion screen. A large white modal window with the title 'Congratulations!' is centered on the screen. The modal text says: 'You've completed the room! Share this with your friends:'. Below this text are three social media sharing buttons: 'Twitter', 'Facebook', and 'LinkedIn'. At the bottom of the modal is a 'Leave feedback' link. The background of the room is visible behind the modal, showing a 'Cyber Defense > Threat Emulation > Attacktive Directory' breadcrumb, a 'Start AttackBox' button, and a 'Scoreboard' chart. The Windows taskbar at the bottom shows the system clock as 9:15 AM on 6/14/2024.

Congratulations!

You've completed the room! Share this with your friends:

[Twitter](#) [Facebook](#) [LinkedIn](#)

[Leave feedback](#)

Shareable link - <https://tryhackme.com/r/room/attacktivedirectory>

Conclusion: Attacktive Directory provides a valuable learning platform for understanding the complexities of Active Directory security and practicing techniques for identifying and mitigating common vulnerabilities. By following the tasks outlined in this report, security professionals can gain practical experience in reconnaissance, exploitation, and privilege escalation within Active Directory environments, ultimately enhancing their skills in defending against real-world threats.