Attacktive Directory: TryHackMe Writeup

Attacktive Directory

99% of corporate networks run off of AD. But can you exploit a vulnerable Domain Controller?

In this room, we are going to learn how to exploit a vulnerable Domain Controller and get full control over it.

Specifically, we will learn how to:
1. Enumerate a domain's users using Kerbrute
2. Exploit Kerberos misconfigurations using Impacket
3. Crack hashes using hashcat
4. Perform further enumeration after gaining initial access to the target system using smbclient
5. Elevate our privileges within the Domain

[Task 1] Deploy the machine

Deploy your attacker machine as well as the Attacktive Directory machine.

[Task 2] Setup

Impacket is a collection of Python classes for working with network protocols. It is widely used in the field of cybersecurity for various purposes, including network analysis, penetration testing, and security assessments.

BloodHound is a single-page Javascript web application that uses graph theory to reveal hidden relationships within an Active Directory or Azure environment. Attackers can use BloodHound to identify attack paths, and defenders can use it to eliminate them.

[Task 3] Enumeration — Welcome to Attacktive Directory

Let's get started with a simple Nmap host discovery and service scanning.

Port 139 and 445: SMB ports used for file sharing and communication between computers.

Answer:
1. Tool for enumerating port 139/445: enum4linux

2. NetBIOS-Domain Name: THM-AD

3. Common TLD for AD domains: .local

[Task 4] Enumeration — Enumerating Users via Kerberos

Knowing that port 88 is open, we can use Kerbrute to brute-force and enumerate valid Active Directory users.

Answer:
1. Kerbrute command: userenum

2. Notable accounts discovered: svc-admin

3. Another notable account: backup

[Task 5] Exploitation — Abusing Kerberos

We can abuse ASREPRoasting, which exploits accounts that don't require pre-authentication.

Answer:
1. ASREPRoastable account: svc-admin

2. Hash type: Kerberos 5, etype 23, AS-REP

3. Hash mode: 18200

4. Password: management2005

[Task 6] Enumeration — Back to Basics

Using smbclient, we enumerate SMB shares on the domain controller.

Answer:
1. Utility for SMB shares: smbclient

2. Option to list shares: -L

3. Accessible share with a text file: backup

4. Content of the file: YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODY

5. Decoded content: backup@spookysec.local:backup2517860

[Task 7] Domain Privilege Escalation — Elevating Privileges within the Domain

We use the backup account to dump the NTDS.DIT file, gaining full control over the domain.

Answer:
1. Method to dump NTDS.DIT: DRSUAPI

2. Administrator NTLM hash: 0e0363213e37b94221497260b0bcb4fc

3. Attack method: pass the hash

4. Evil-WinRM option to use hash: -H

[Task 8] — Flag Submission Panel

1. Administrator: TryHackMe{4ctiveD1rectoryM4st3r}

2. svc-admin: TryHackMe{K3rb3r0s_Pr3_4uth}

3. backup: TryHackMe{B4ckM3UpSc0tty!}