Active Directory Penetration Testing Report

Done by Lia Potikyan

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

Executive Summary

This penetration test aimed to assess the security posture of an Active Directory (AD) environment provided by TryHackMe. The assessment involved several phases, including reconnaissance, enumeration, exploitation, and privilege escalation. By leveraging tools like Impacket, BloodHound, Kerbrute, and Evil-WinRM, various vulnerabilities and misconfigurations were identified and exploited.

Scope

The scope of this penetration test focused on the Attacktive Directory room provided by TryHackMe. It included the enumeration of users and services, exploitation of vulnerabilities within the AD environment, and privilege escalation to gain administrative access.

Start Date	End Date
April 2, 2024	April 4, 2024

The penetration testing followed a systematic approach

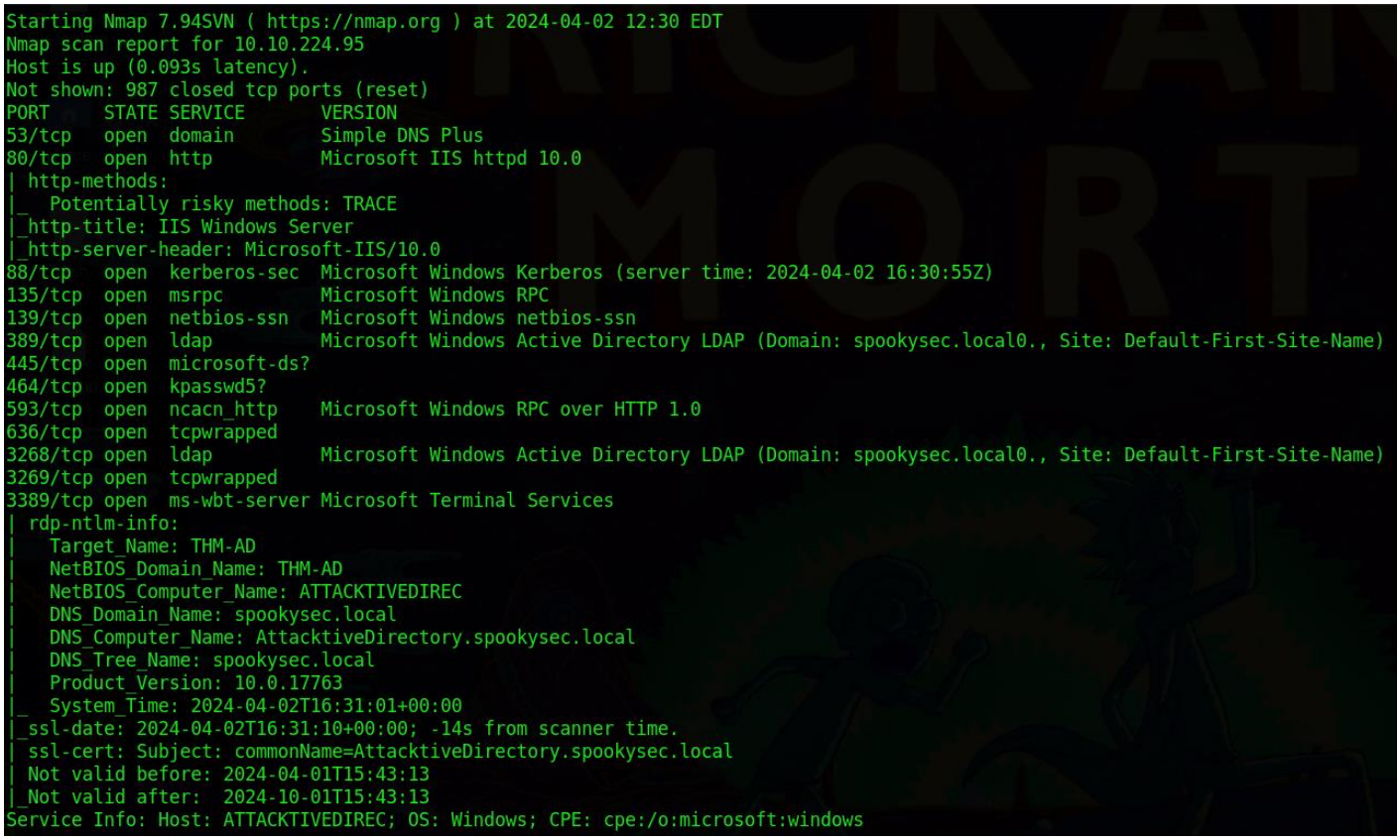
Enumeration: Utilized tools like Nmap for network scanning and Enum4linux for enumerating users and shares.
Exploitation: Leveraged Kerbrute for user enumeration and ASREPRoasting. Utilized Impacket tools for exploiting weaknesses in Kerberos and dumping password hashes.
Privilege Escalation: Used Pass the Hash technique and Evil-WinRM for privilege escalation and obtaining administrator access.
Flag Retrieval: Retrieved flags from compromised accounts using Evil-WinRM.

Findings

Identified vulnerabilities in the Active Directory environment.
Successfully enumerated users and extracted password hashes.
Exploited ASREPRoasting vulnerability to retrieve password hashes without authentication.
Dumped NTDS.DIT using Impacket tools, gaining access to sensitive information.
Utilized Pass the Hash technique for authentication without plaintext passwords.
Leveraged Evil-WinRM for privilege escalation and flag retrieval.

Enumeration and Weakness Discovery

Thorough enumeration and scanning revealed misconfigurations, outdated software, and exploitable vulnerabilities.



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 12:30 EDT
Nmap scan report for 10.10.224.95
Host is up (0.093s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-04-02 16:30:55Z)
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?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   DNS_Tree_Name: spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2024-04-02T16:31:01+00:00
|_ssl-date: 2024-04-02T16:31:10+00:00; -14s from scanner time.
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2024-04-01T15:43:13
|_Not valid after:  2024-10-01T15:43:13
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

User Enumeration and Password Extraction

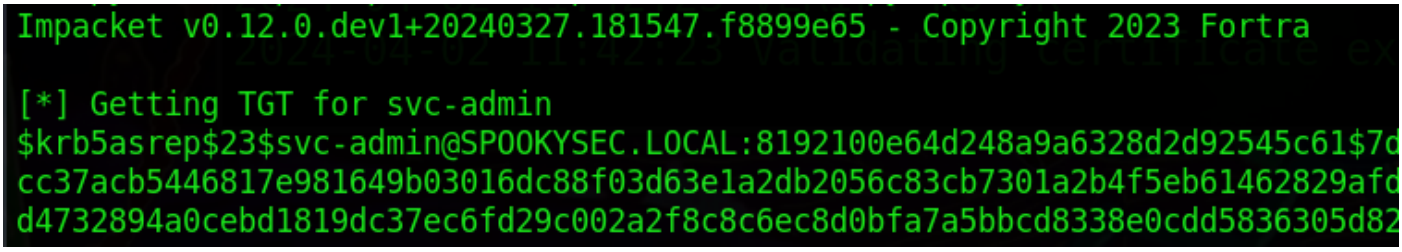
Tools like Enum4linux aided in user enumeration, while Kerbrute and Impacket were used to extract password hashes from the domain controller.

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

Version: v1.0.3 (9dad6e1) - 04/02/24 - Ronnie Flathers @ropnop

2024/04/02 13:18:09 >  Using KDC(s):
2024/04/02 13:18:09 >   10.10.224.95:88

2024/04/02 13:18:09 >  [+] VALID USERNAME:       james@spookysec.local
2024/04/02 13:18:11 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2024/04/02 13:18:13 >  [+] VALID USERNAME:       James@spookysec.local
2024/04/02 13:18:14 >  [+] VALID USERNAME:       robin@spookysec.local
2024/04/02 13:18:22 >  [+] VALID USERNAME:       darkstar@spookysec.local
2024/04/02 13:18:27 >  [+] VALID USERNAME:       administrator@spookysec.local
2024/04/02 13:18:37 >  [+] VALID USERNAME:       backup@spookysec.local
2024/04/02 13:18:42 >  [+] VALID USERNAME:       paradox@spookysec.local
2024/04/02 13:19:10 >  [+] VALID USERNAME:       JAMES@spookysec.local
2024/04/02 13:19:20 >  [+] VALID USERNAME:       Robin@spookysec.local
```

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Apr  2 13:06:28 2024

 =========================================( Target Information )=========================================

Target ........... 10.10.224.95
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 ============================( Enumerating Workgroup/Domain on 10.10.224.95 )============================


[E] Can't find workgroup/domain


 ================================( Nbtstat Information for 10.10.224.95 )================================

Looking up status of 10.10.224.95
No reply from 10.10.224.95

 ===================================( Session Check on 10.10.224.95 )===================================


[+] Server 10.10.224.95 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.10.224.95 )================================

Domain Name: THM-AD
Domain Sid: S-1-5-21-3591857110-2884097990-301047963

[+] Host is part of a domain (not a workgroup)
```

ASREPRoasting Exploitation

Exploited the ASREPRoasting vulnerability to retrieve password hashes without authentication by targeting accounts with "Does not require Pre-Authentication" set.



NTDS.DIT Dumping

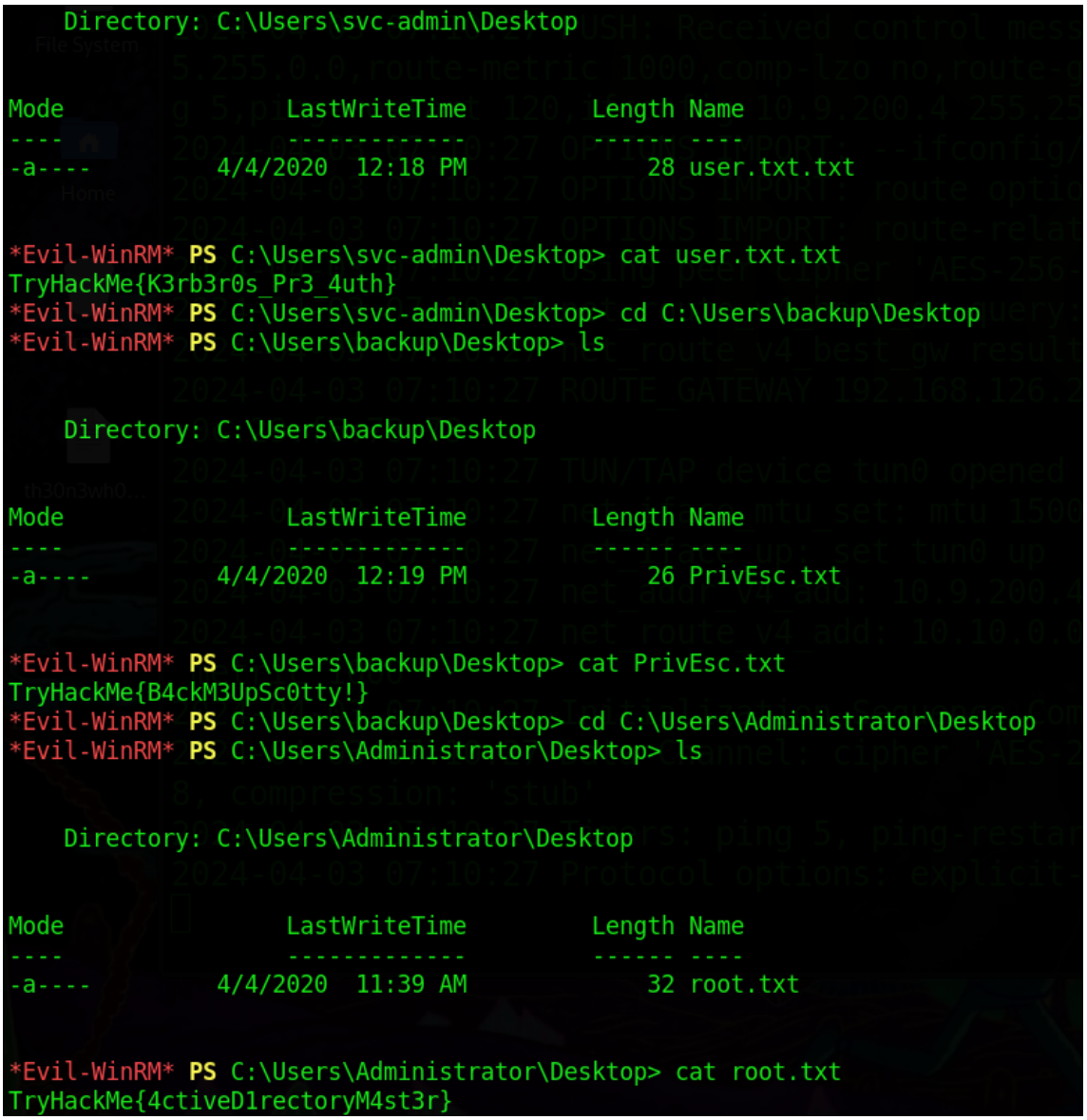
Used Impacket's secretsdump.py to dump the NTDS.DIT file, gaining access to sensitive information including password hashes and user accounts.

Pass the Hash Authentication

Leveraged Pass the Hash technique to authenticate to remote services without plaintext passwords, bypassing traditional authentication mechanisms.

Evil-WinRM Privilege Escalation

Utilized Evil-WinRM for remote command execution and privilege escalation, gaining elevated access to the system and retrieving flags from compromised accounts.



Solution

Patch and Update:
Address identified vulnerabilities by applying patches and updates to misconfigured systems and outdated software versions. Regularly monitor for new security advisories and apply patches promptly.
Enhanced Authentication Mechanisms:
Implement stronger authentication mechanisms to mitigate vulnerabilities such as ASREPRoasting. Enforce stricter password policies, enable multi-factor authentication, and limit privileges for accounts vulnerable to such attacks.
Access Control and Monitoring:
Implement access controls to restrict unauthorized access to sensitive resources. Utilize monitoring tools to detect and respond to suspicious activities, including unauthorized access attempts and unusual user behavior.
Regular Security Assessments:
Conduct regular security assessments, including penetration testing and vulnerability scanning, to proactively identify and remediate security weaknesses within the Active Directory environment.

Conclusion

The penetration testing exercise on the Active Directory environment revealed critical vulnerabilities and weaknesses that could potentially compromise the security of the organization. Through thorough enumeration, exploitation of vulnerabilities, and privilege escalation techniques, the assessment highlighted the importance of robust security

measures to protect against unauthorized access and data breaches.

By implementing the recommended solutions, including patching vulnerabilities, enhancing authentication mechanisms, enforcing access controls, and conducting regular security assessments, organizations can strengthen the security posture of their Active Directory environment and mitigate the risks associated with potential cyber threats.

Overall, the penetration test serves as a valuable exercise in identifying and addressing security gaps, ultimately contributing to the enhancement of the organization's cybersecurity resilience and preparedness.

Lia Potikyan

liapotikyan006@gmail.com