Cyber Public School

LDAP ENUMERATION

https://cyberpublicschool.com/

LDAP ENUMERATION

LDAP Enumeration

Introduction

LDAP (Lightweight Directory Access Protocol) is a protocol used for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. LDAP is commonly used for managing user authentication and authorization, as well as storing other types of directory information such as email addresses, phone numbers, and organizational units.

LDAP enumeration refers to the process of querying an LDAP server to extract information about its directory structure and contents. Enumeration can be used by attackers to gather information about potential targets, such as user account names, email addresses, and organizational unit names, which can then be used for further attacks such as password guessing or social engineering.

LDAP Enumeration

LDAP Enumeration using Nmap

Nmap is a powerful network exploration and security auditing tool that can be used to scan and enumerate different types of systems and services. When it comes to LDAP enumeration, Nmap can be used to discover and map out LDAP-enabled servers and identify potential vulnerabilities.

To scan for LDAP servers using Nmap, you can use the following command:

```
css

nmap -p 389 --script ldap-search <target_IP>
```

This command instructs Nmap to scan for LDAP servers on port 389 and run the LDAP-search script to query the server for information. The output will show a list of LDAP objects and their attributes, which can be used to identify usernames, groups, and other information that could be used for further attacks.

You can also use Nmap to scan for other LDAP-related ports, such as 636 (for SSL/TLS encrypted LDAP traffic) and 3268/3269 (for global catalog servers):

```
css

nmap -p 636 --script ldap-search <target_IP>
nmap -p 3268,3269 --script ldap-search <target_IP>
```

LDAP Enumeration

It's important to note that LDAP enumeration should only be performed on systems that you have permission to access and test. Unauthorized scanning and enumeration can lead to legal consequences and damage to systems and networks.

```
$ nmap -p 389 --script ldap-search --script-args
'ldap.username="cn=ldaptest,cn=users,dc=cqure,
dc=net",ldap.password=ldaptest,
ldap.qfilter=users,ldap.attrib=sAMAccountName' <IP
address>

$ nmap -p 389 --script ldap-search --script-args
'ldap.username="cn=ldaptest,cn=users,
dc=cqure,dc=net",ldap.password=ldaptest,
ldap.qfilter=custom,ldap.searchattrib="operatingSystem
",
ldap.searchvalue="Windows *Server*",ldap.attrib=
{operatingSystem,whencreated,OperatingSystemService
Pack}' <host>
```

LDAP Enumeration

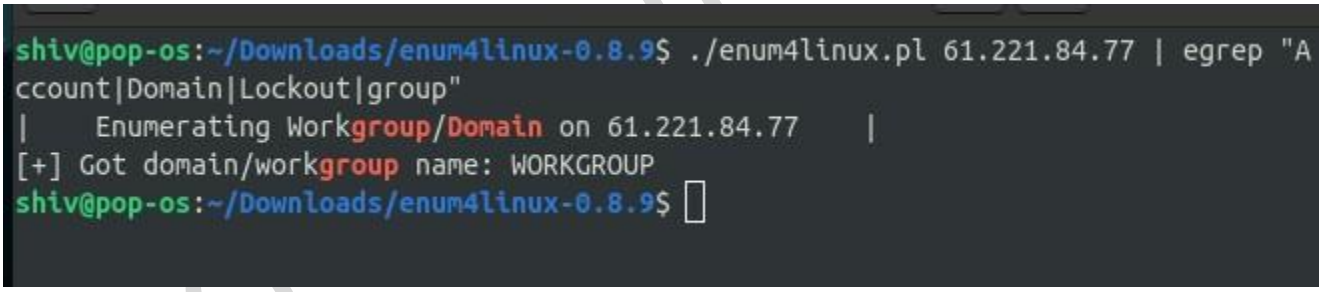
```
shiv@pop-os:~$ nmap -p 389 --script ldap-search --script-args 'ldap.username="cn=
ldaptest,cn=users,dc=cqure,dc=net",ldap.password=ldaptest,
ldap.qfilter=users,ldap.attrib=sAMAccountName' 61.221.84.77
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-08 17:48 IST
Nmap scan report for mail.chyuanuei.com.tw (61.221.84.77)
Host is up (0.13s latency).

PORT    STATE SERVICE
389/tcp open  ldap

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
shiv@pop-os:~$
```

LDAP Enumeration

LDAP Enumeration Using enum4linux:

Enum4linux is a great tool that is used in windows enumeration, hence we are going to look at this tool's usage. Using the below command, you can enumerate the accounts and groups.

```
$ enum4linux <IP address> |
egrep "Account|Domain|Lockout|group"
```



LDAP Enumeration

LDAP Enumeration Using Windapsearch:

Windapsearch is a python script that is used to enumerate users, groups, and computers from a windows domain by taking the leverage of LDAP queries.

```
#for computers
python3 windapsearch.py --dc-ip
<IP address> -u <username>
-p <password> --computers

#for groups
python3 windapsearch.py --dc-ip <IP address>
-u <username> -p <password> --groups

#for users
python3 windapsearch.py --dc-ip <IP address>
-u <username> -p <password> --da

#for privileged users
python3 windapsearch.py --dc-ip <IP address>
-u <username> -p <password> --privileged-users
```

LDAP Enumeration

LDAP Enumeration Using Ldapsearch:

LDAP search makes a connection to an LDAP server, and it executes a search by using different paraments. The filter conforms to the string representation for search filters as defined in RFC 4515 else it uses (objectClass=*).

Below are some commands that can be used for checking and verifying the credentials.

```
#To check null credentials
$ ldapsearch -x -H ldap://<IP address>
 -D '' -w '' -b "DC=<1_SUBDOMAIN>,DC=<TLD>"
```

```
#to validate the credentials
$ ldapsearch -x -H ldap://<IP address>
-D '<DOMAIN>\<username>' -w '<password>'
-b "DC=<1_SUBDOMAIN>,DC=<TLD>"
```

LDAP Enumeration

An LDAP based Active Directory object (users, groups, and computers) enumeration tool.

About

ad-ldap-enum is a Python script developed to collect users/computers and their group memberships from Active Directory. In large Active Directory environments, tools such as NBTEnum were not performing fast enough. By executing LDAP queries against a domain controller, ad-ldap-enum is able to target specific Active Directory attributes and quickly build out group membership. ad-ldap-enum outputs three tab delimited files:

- Domain_Group_Membership.csv
- Extended_Domain_User_Information.csv
- Extended_Domain_Computer_Information.csv

The first file contains users, computers, groups, and their memberships. The second file contains users and extra information about the users from Active Directory (e.g. a user's home folder or email address). The third file contains computers in the 'Domain Computers' group and extra information about them from Active Directory (e.g. operating system type and service pack version). ad-ldap-enum supports both authenticated and unauthenticated LDAP connections. Additionally, ad-ldap-enum can process nested groups and display a user's actual group membership. This tool also supports password and Pass-the-Hash (PtH) **LM:NTLM** style authentication. ad-ldap-enum also supports LDAP over SSL/TLS connections, IPv4, and IPv6 networks.

LDAP Enumeration

Requirements

The package primarily uses the ldap3 Python package to execute the LDAP connections and queries. To install all requirements, please run the below command:

```
python -m pip install -r 'requirements.txt'
```

LDAP Enumeration

LDAP Enumeration Tool

LDAP enumeration is the process of gathering information about an LDAP directory, such as the structure, users, groups, and other directory objects. This can be useful for auditing and testing the security of an LDAP directory.

There are several LDAP enumeration tools available that can be used for this purpose. Here are some popular ones:

ldapsearch - a command-line tool included in most LDAP implementations that can be used for querying an LDAP directory and retrieving information.

Enum4linux - a tool that can be used for enumerating information from Windows and Samba systems, including information about the LDAP directory.

LDAPenum - a Python script that can be used for enumerating users and groups from an LDAP directory.

LDAP Recon - a tool that can be used for enumerating information about an LDAP directory, including users, groups, and attributes.

Nmap - a network exploration and security auditing tool that includes scripts for scanning and enumerating LDAP directories.

LDAP Enumeration

Dirsearch - a web-based directory scanning tool that includes a module for enumerating LDAP directories.

These tools can help you gather information about an LDAP directory and identify potential vulnerabilities and security issues. However, it's important to use these tools responsibly and with permission, as unauthorized LDAP enumeration can be considered a security breach.

LDAP Enumeration

LDAP ENU4LINUX ALL COMMAND

Enum4linux is a tool that can be used for enumerating information from Windows and Samba systems, including information about the LDAP directory. Here are some of the commands that can be used with Enum4linux for LDAP enumeration:

enum4linux -a: This command will perform a complete enumeration of the target system, including users, shares, services, and password policy information.

enum4linux -U <username> -P <password> -G <domain>: This command will perform a targeted enumeration of the specified username and password for the specified domain.

enum4linux -S <IP address>: This command will perform a scan of the specified IP address for available shares.

enum4linux -u <username> -p <password> -d <domain> -D: This command will dump the user and password hashes for the specified domain.

enum4linux -k: This command will dump the Kerberos tickets from the target system.

enum4linux -M: This command will perform a brute force attack on the target system's password policy.

LDAP Enumeration

enum4linux -N: This command will perform a null session enumeration of the target system.

These commands can be used to gather information about the LDAP directory and identify potential security vulnerabilities. However, it's important to use these tools responsibly and with permission, as unauthorized LDAP enumeration can be considered a security breach.

LDAP Enumeration

LDAP ENU4LINUX ALL COMMAND WITH EXAMPLE

Here are some examples of how to use the various commands available in Enum4linux for LDAP enumeration:

enum4linux -a

This command performs a complete enumeration of the target system, including users, shares, services, and password policy information. For example:

```
css

enum4linux -a 192.168.1.10
```

enum4linux -U <username> -P <password> -G <domain>

This command performs a targeted enumeration of the specified username and password for the specified domain. For example:

```
css

enum4linux -U user -P password -G domain 192.168.1.10
```

enum4linux -S <IP address>

This command performs a scan of the specified IP address for available shares. For example:

```

enum4linux -S 192.168.1.10
```

LDAP Enumeration

enum4linux -u <username> -p <password> -d <domain> -D
This command dumps the user and password hashes for the specified domain. For example:

```
css
```

```
enum4linux -u user -p password -d domain -D 192.168.1.10
```

enum4linux -k
This command dumps the Kerberos tickets from the target system. For example:

```
```

```
enum4linux -k 192.168.1.10
```

enum4linux -M
This command performs a brute force attack on the target system's password policy. For example:

```
```

```
enum4linux -M 192.168.1.10
```

LDAP Enumeration

enum4linux -N

This command performs a null session enumeration of the target system. For example:

```mathematica
enum4linux -N 192.168.1.10
```

Note that these commands are just examples and should not be used to perform unauthorized LDAP enumeration. It's important to use these tools responsibly and with permission, as unauthorized LDAP enumeration can be considered a security breach.

LDAP Enumeration

Dumping LAPS Passwords from Linux

ldapsearch

```
-x -h -D "@" -w -b "dc=<>,dc=<>,dc=<>"
"(&(objectCategory=computer)(ms-MCS-AdmPwd=*))" ms-
MCS-AdmPwd
```

LDAP Enumeration

Search Specific Base DN and Scope

ldapsearch

```
h master.example.com -D
"cn=manager,dc=example,dc=com" -w "slappasswd" -b
"ou=users,ou=department,dc=example,dc=com" -s base
```

Contacts us

https://cyberpublicschool.com/

https://www.instagram.com/cyberpublicschool/

Phone no.: +91 9631750498 India
+61 424866396 Australia

Our Successful Oscp Student.