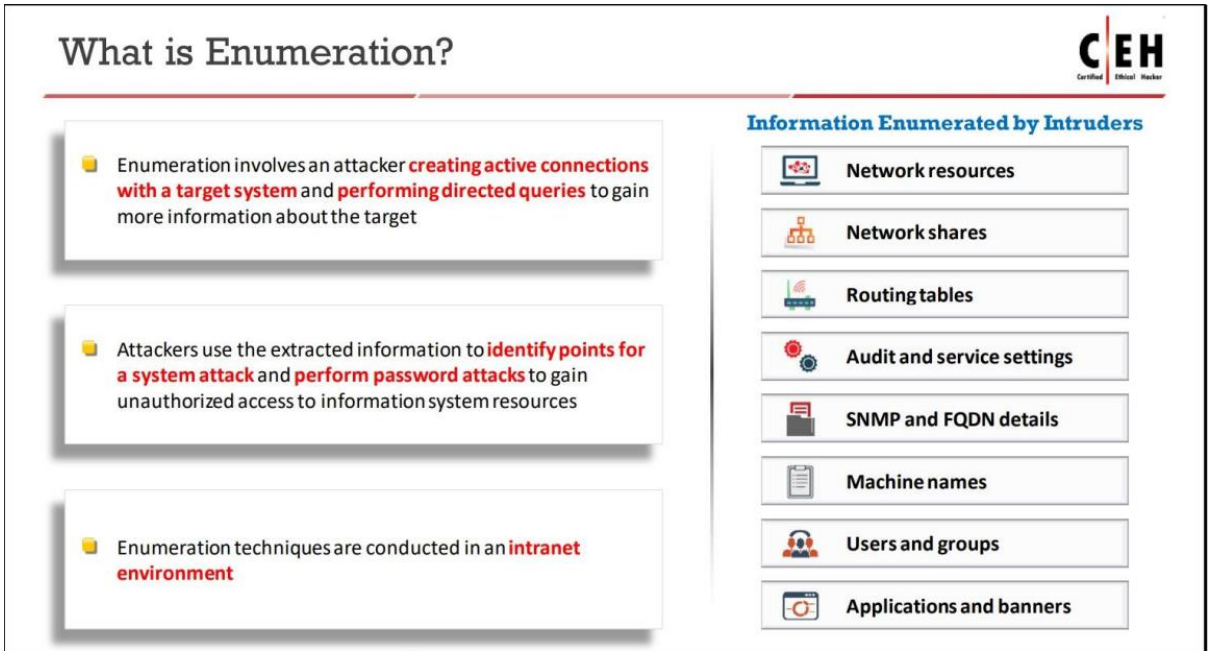
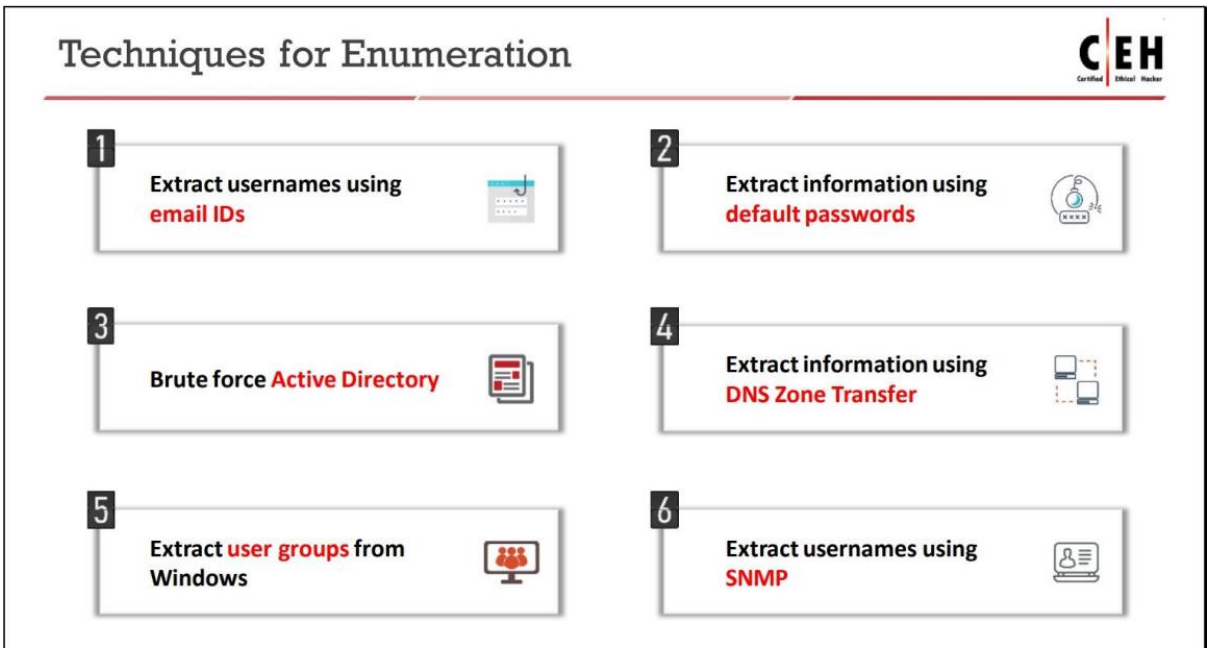
ENUMERATION

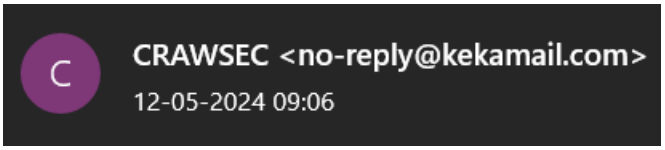


- Enumeration is a process of extracting usernames, machine name, network resources and services from a network or a system. It is a process to check the current user. Configure IP address (default gateway, subnet, DNS, domain controller).

Techniques for Enumeration



1) Extract username using Email IDs – Every email address contains of two parts, a username and a domain name.

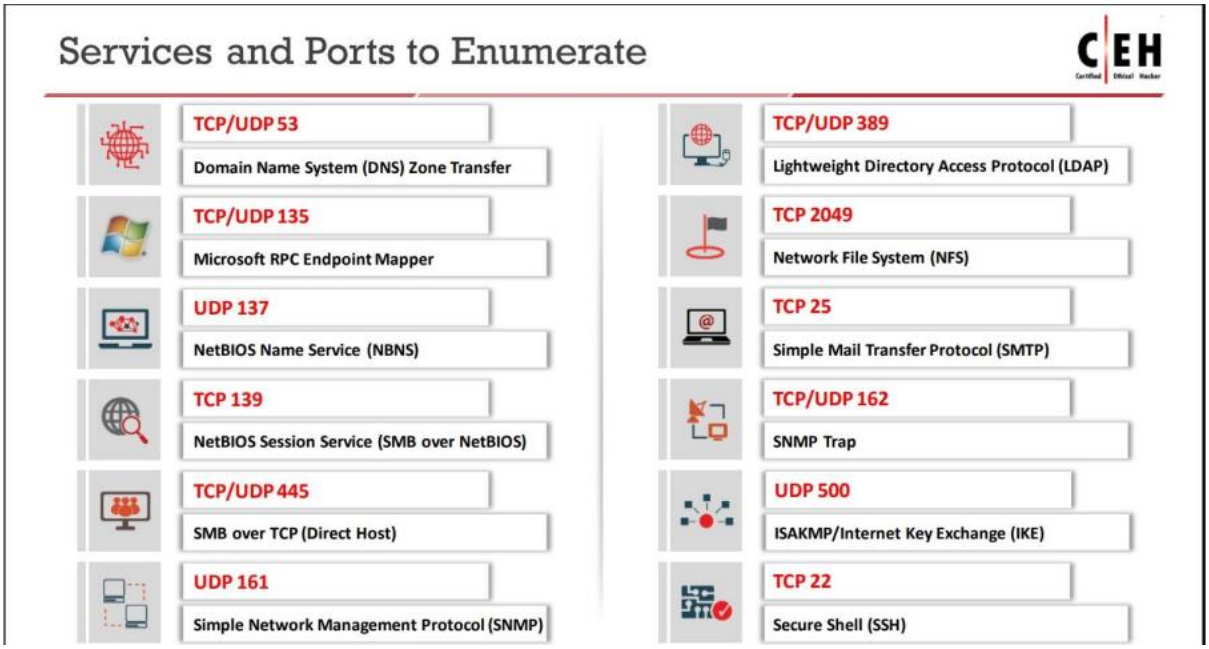


2) Extract information using default passwords - There are many online resources that publish many default passwords assigned by the manufacturer for their products. Often users forget to change the default passwords that help an attacker to enumerate their data easily.

3) Brute force active directory - Brute force directory guessing attacks are very common attacks used against websites and web servers. They are used to find hidden and often forgotten directories on a site to try to compromise.

4) Extract Information Using DNS Zone Transfer - An Attacker can get valuable topological information about the target's internal network using DNS zone transfer. Services and ports to enumerate: TCP 53: DNS Zone Transfer: DNS zone transfer relies on TCP 53 port rather than UDP 53.

5) Extract username using SNMP - By using SNMP APIs, attackers can guess the strings through which they can extract required username.



Net BIOS Enumeration

NetBIOS is an acronym that stands for Network Basic Input Output System. It enables computer communication over a LAN and the sharing of files and printers. TCP/IP network devices are identified using NetBIOS names (Windows). It must be network-unique and limited to 16 characters, with 15 reserved for the device name and the 16th reserved for identifying the type of service running or name record type.

NetBIOS Enumeration

- A NetBIOS name is a unique 16 ASCII character string used to **identify the network devices** over TCP/IP; fifteen characters are used for the **device name**, and the sixteenth character is reserved for the **service or name record type**

Attackers use the NetBIOS enumeration to obtain

- The list of computers that belong to a domain
- The list of shares on the individual hosts in the network
- Policies and passwords

NetBIOS name list

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the primary domain controller (PDC) for the domain

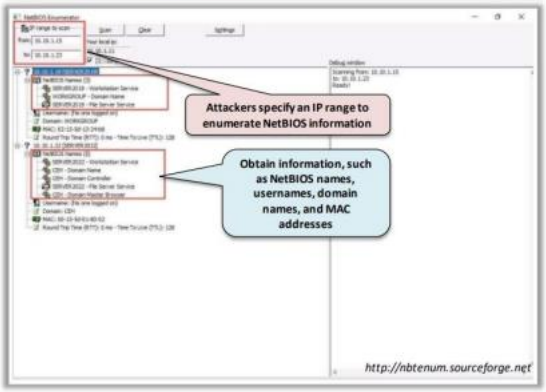
Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

Net BIOS Enumeration Tools

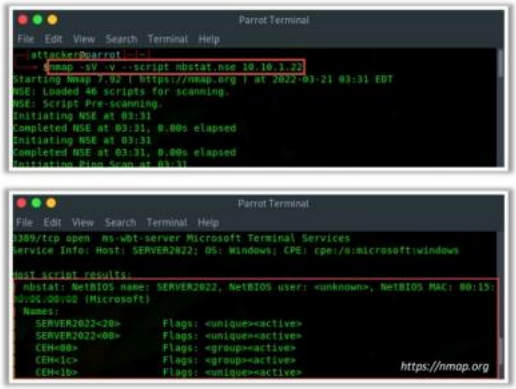
- Netbios enumerator
- Nmap
- Advance IP scanner

NetBIOS Enumeration Tools

NetBIOS Enumerator NetBIOS Enumerator helps to enumerate details, such as **NetBIOS names**, **Usernames**, **Domain names**, and **MAC addresses**, for a given range of IP addresses



Nmap Nmap's nbstat NSE script allow attackers to retrieve targets' **NetBIOS names** and **MAC addresses**

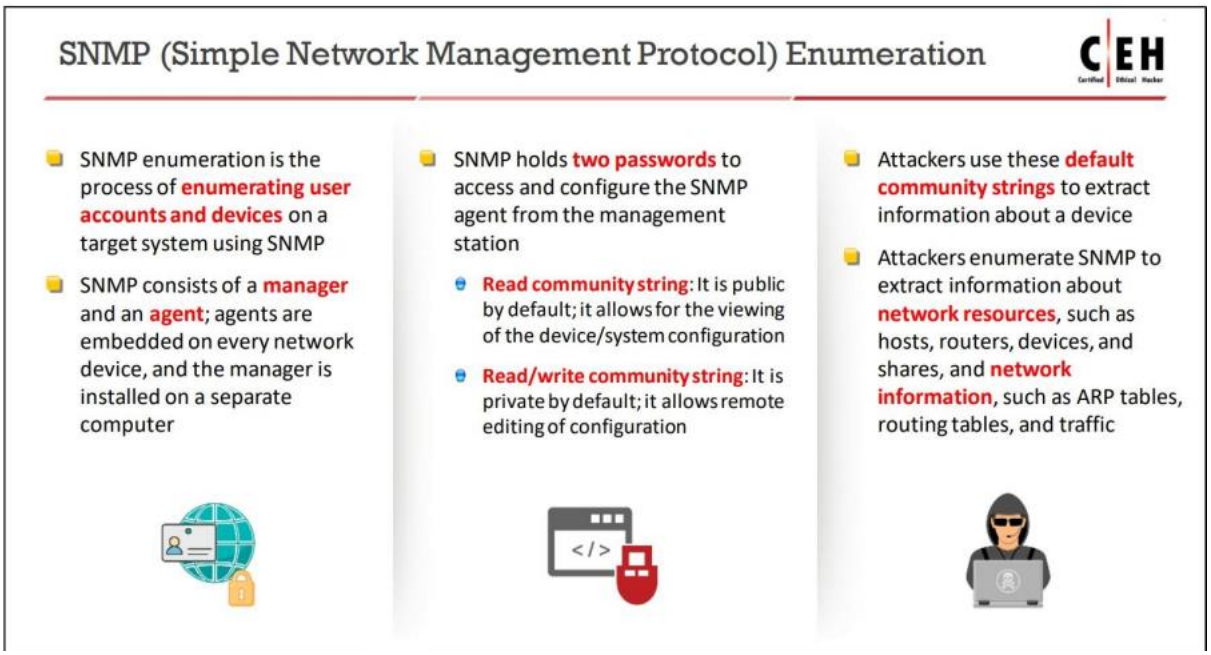


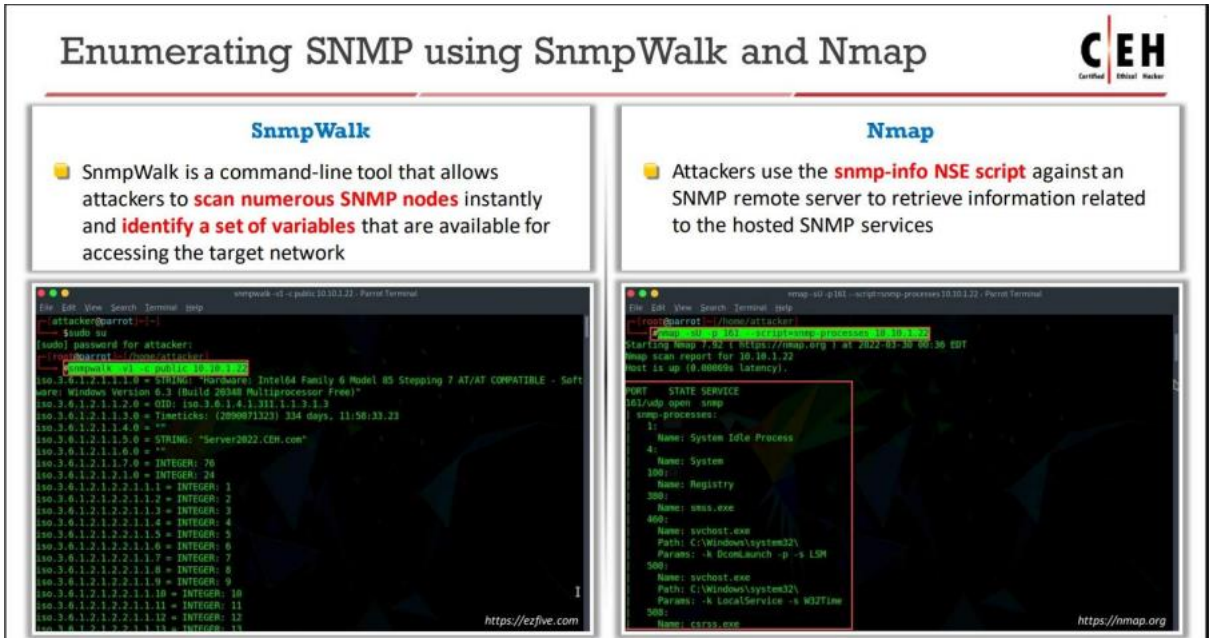
Other NetBIOS Enumeration Tools:

- **Global Network Inventory** *http://www.magnetosoft.com*
- **Advanced IP Scanner** *http://www.advanced-ip-scanner.com*
- **Hyena** *https://www.systemtools.com*
- **Nsauditor Network Security Auditor** *https://www.nsauditor.com*

SNMP enumeration

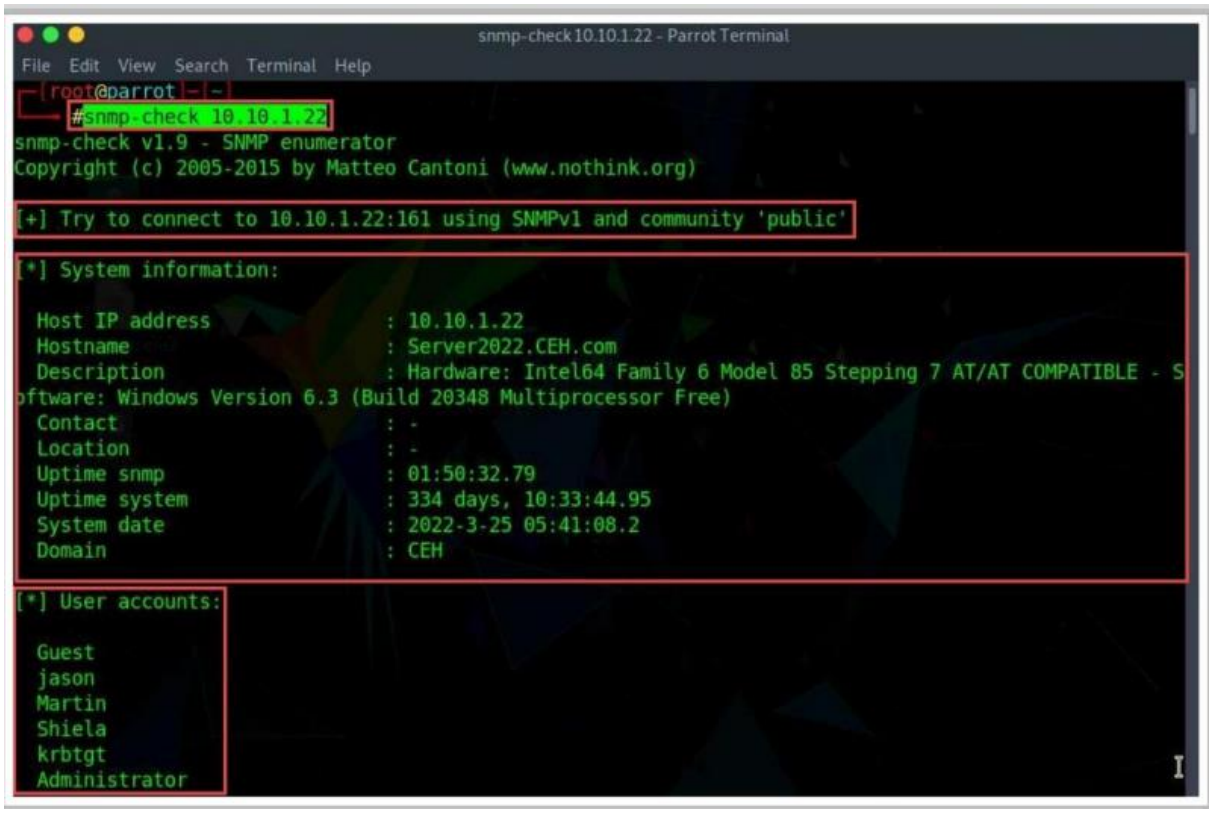
Simple Network Management Protocol (SNMP) is an application layer protocol that runs on UDP and maintains and manages IP network routers, hubs, and switches. SNMP agents run on networking devices in Windows and UNIX networks. SNMP enumeration is process of enumeration user account and device on a target system using SNMP. SNMP consist manager and agent on every network and manager is installed on separate computer.



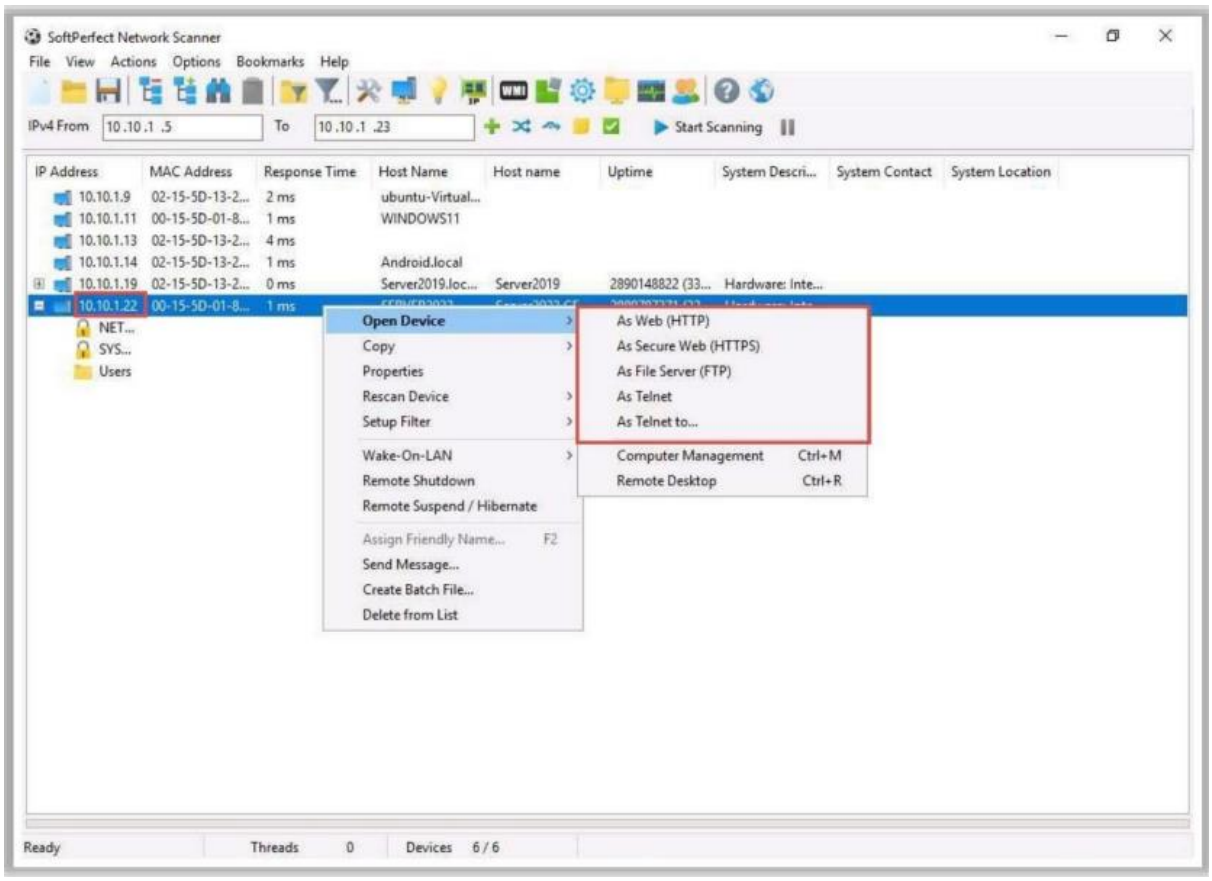


SNMP Enumeration Tools

1) snmp-check



2) SoftPerfect Network Scanner



LDAP Enumeration

Lightweight Directory Access Protocol (LDAP) is an internet protocol that works on TCP/IP, used to access information from directories. The LDAP protocol is used to access an active directory. LDAP enumeration is a technique used to enumerate the active directory. This service mainly runs on TCP ports 389 and 636 as default. LDAP enumeration can help enumerate usernames, addresses, and much juicy information that can be later used for other attacks including social engineering attacks.

LDAP Enumeration

1. Lightweight directory access protocol (LDAP) is an **Internet protocol** for accessing distributed directory services
2. Directory services may provide any organized set of records, often in a **hierarchical** and **logical structure**, such as a corporate email directory
3. A client starts a LDAP session by connecting to a **directory system agent** (DSA) on TCP port 389 and then sends an operation request to the DSA
4. Information is transmitted between the client and server using **basic encoding rules** (BER)
5. Attackers query the LDAP service to gather information, such as **valid usernames, addresses,** and **departmental details**, which can be further used to perform attacks

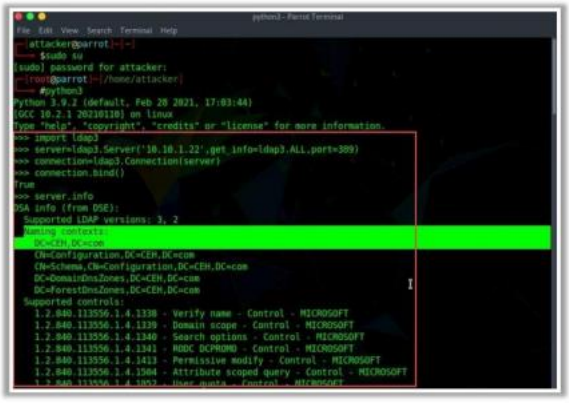
Manual and Automated LDAP Enumeration

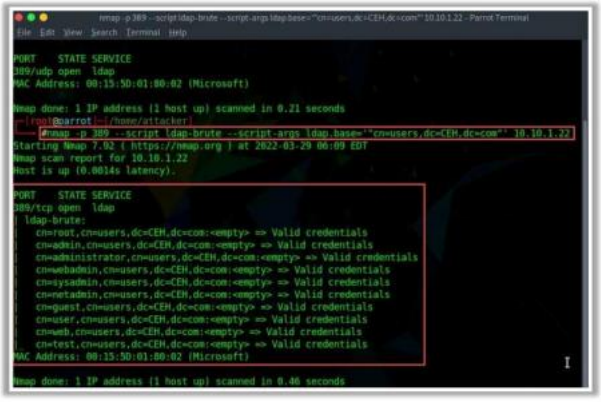
Manual LDAP Enumeration

- Attackers perform manual LDAP enumeration using **Python to fetch information** such as the domain name, naming context, and directory objects

Automated LDAP Enumeration

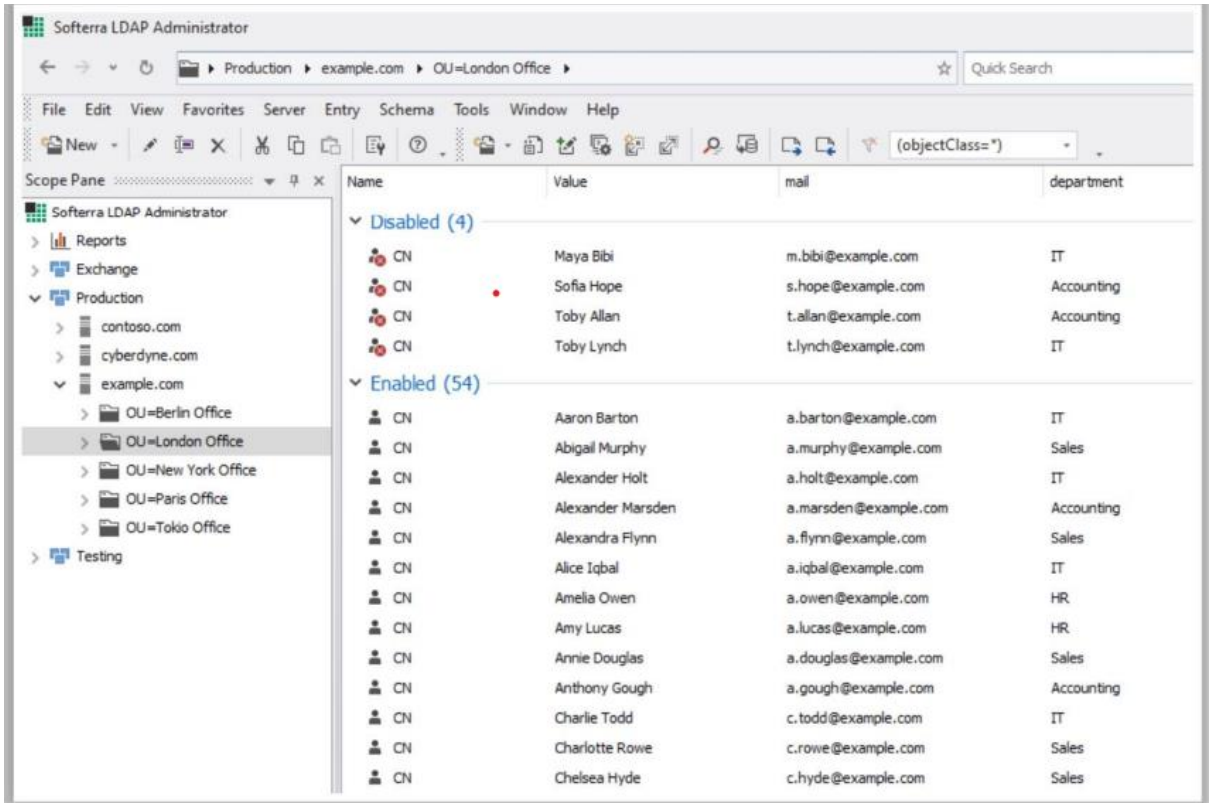
- Attackers use the **ldap-brute NSE script** to brute-force LDAP authentication





LDAP Enumeration Tools –

1) Softerra LDAP Administrator



2) ldap Search

```
ldapsearch -h 10.10.1.22 -x -s base namingcontexts - Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #ldapsearch -h 10.10.1.22 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=CEH,DC=com
namingcontexts: CN=Configuration,DC=CEH,DC=com
namingcontexts: CN=Schema,CN=Configuration,DC=CEH,DC=com
namingcontexts: DC=DomainDnsZones,DC=CEH,DC=com
namingcontexts: DC=ForestDnsZones,DC=CEH,DC=com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

NTP Enumeration

NTP (Network Time Protocol) Enumeration is a process by which an attacker can discover NTP servers on the network. This information can be used to find vulnerable NTP servers, or simply to further enumerate the network. Servers that are allowed access from the internet usually have a much higher chance of being exploitable. An attacker will often use both DNS and brute force methods to find these servers, as well as using Shodan.io or Censys to find unprotected devices.

NTP Enumeration

Network Time Protocol (NTP) is designed to **synchronize the clocks of networked computers**

It uses **UDP port 123** as its primary means of communication

NTP can maintain time to within **10 milliseconds (1/100 second)** over the public Internet

It can achieve accuracies of **200 microseconds** or better in local area networks under ideal conditions

Attackers query the NTP server to gather valuable information, such as

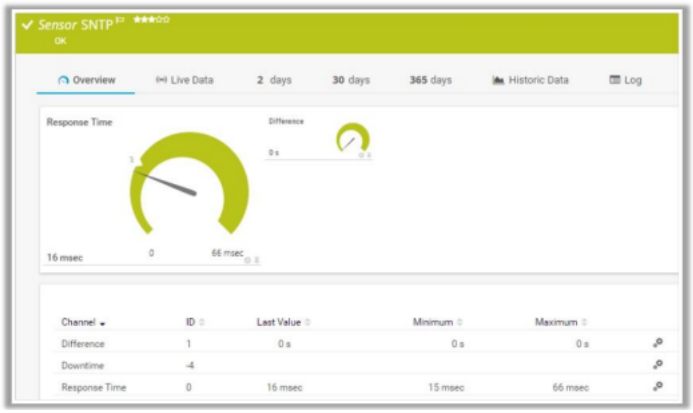
- List of **connected hosts**
- **Clients IP addresses** in a network, their system names, and OSs
- **Internal IPs** can also be obtained if the NTP server is in the demilitarized zone (DMZ)

NTP Enumeration Tools

1) PRTG Network Monitor

NTP Enumeration Tools

- **PRTG Network Monitor** includes **SNTP Sensor monitor**, a simple network time protocol (SNTP) server that shows the response time of the server and time difference in comparison to the local system time



NTP Enumeration Tools

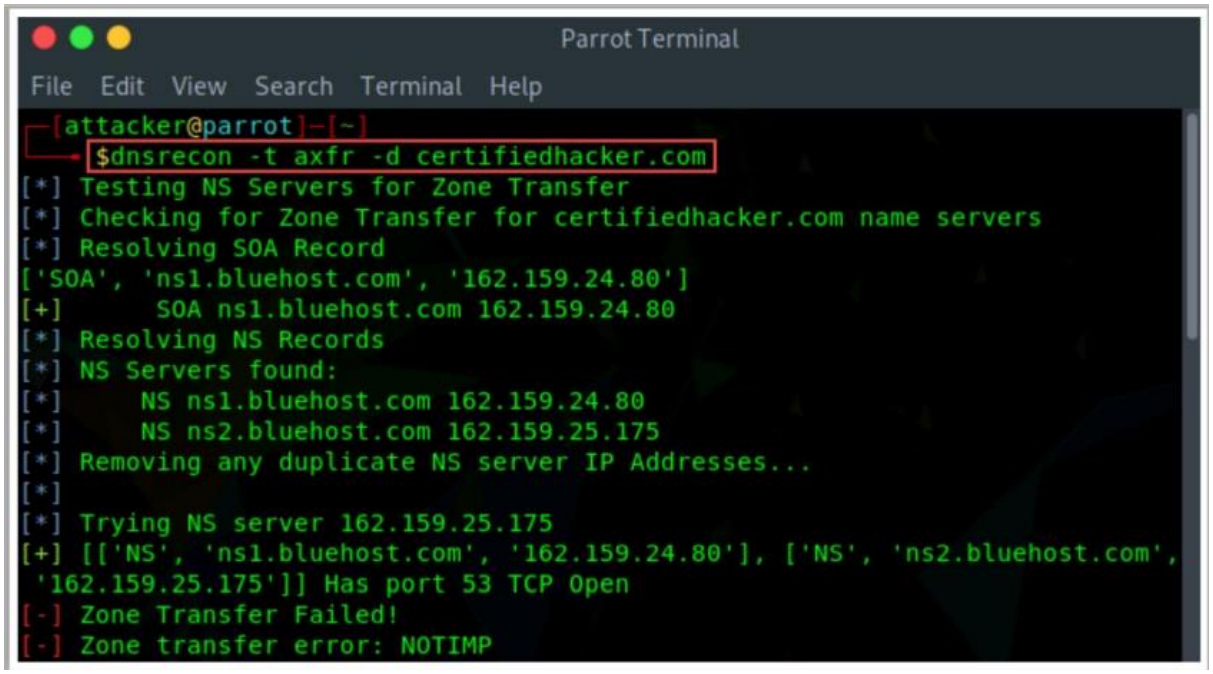
- Nmap (*https://nmap.org*)
- Wireshark (*https://www.wireshark.org*)
- udp-proto-scanner (*https://labs.portcullis.co.uk*)
- NTP Server Scanner (*http://www.bytefusion.com*)

DNS Enumeration

Domain Name System (DNS) is nothing but a program that converts or translates a website name into an IP address and vice versa.
Example: A user enters www.omg.org in a browser, now the DNS will intercept this request and will fetch the corresponding IP address and connect the user to that fetched IP address. The process of DNS Enumeration returns various important information about the target like DNS record types, host names, IP addresses and much more depending upon the configuration of that target system.

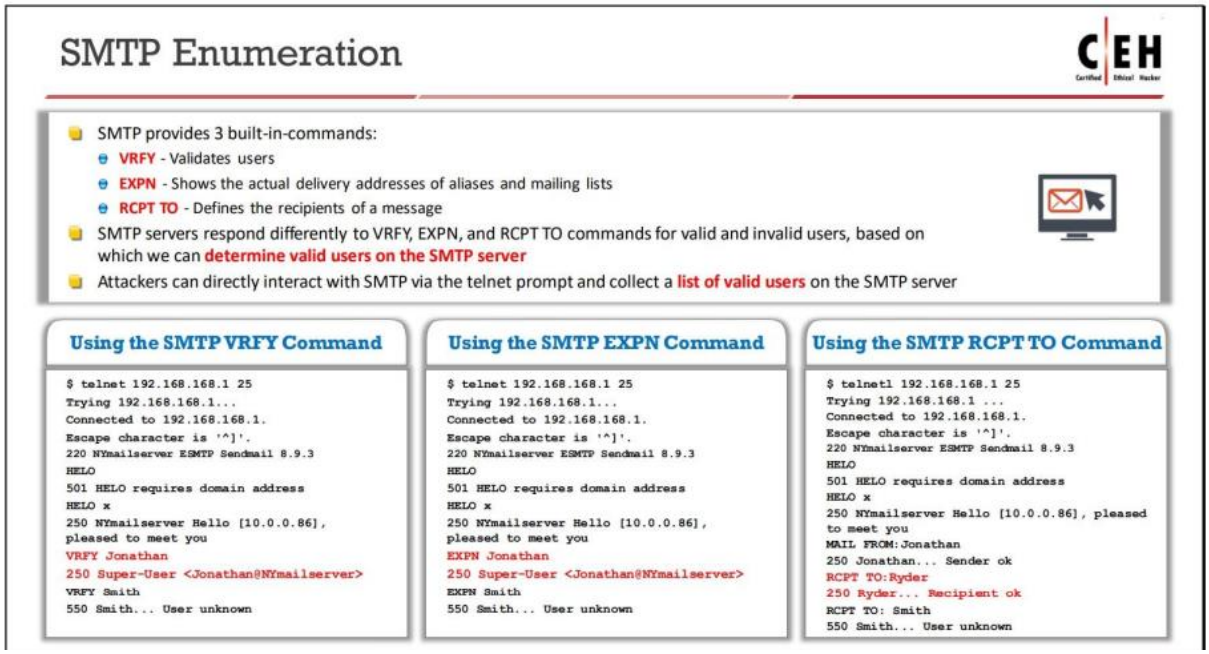
DNS Enumeration Tools

- dnsrecon



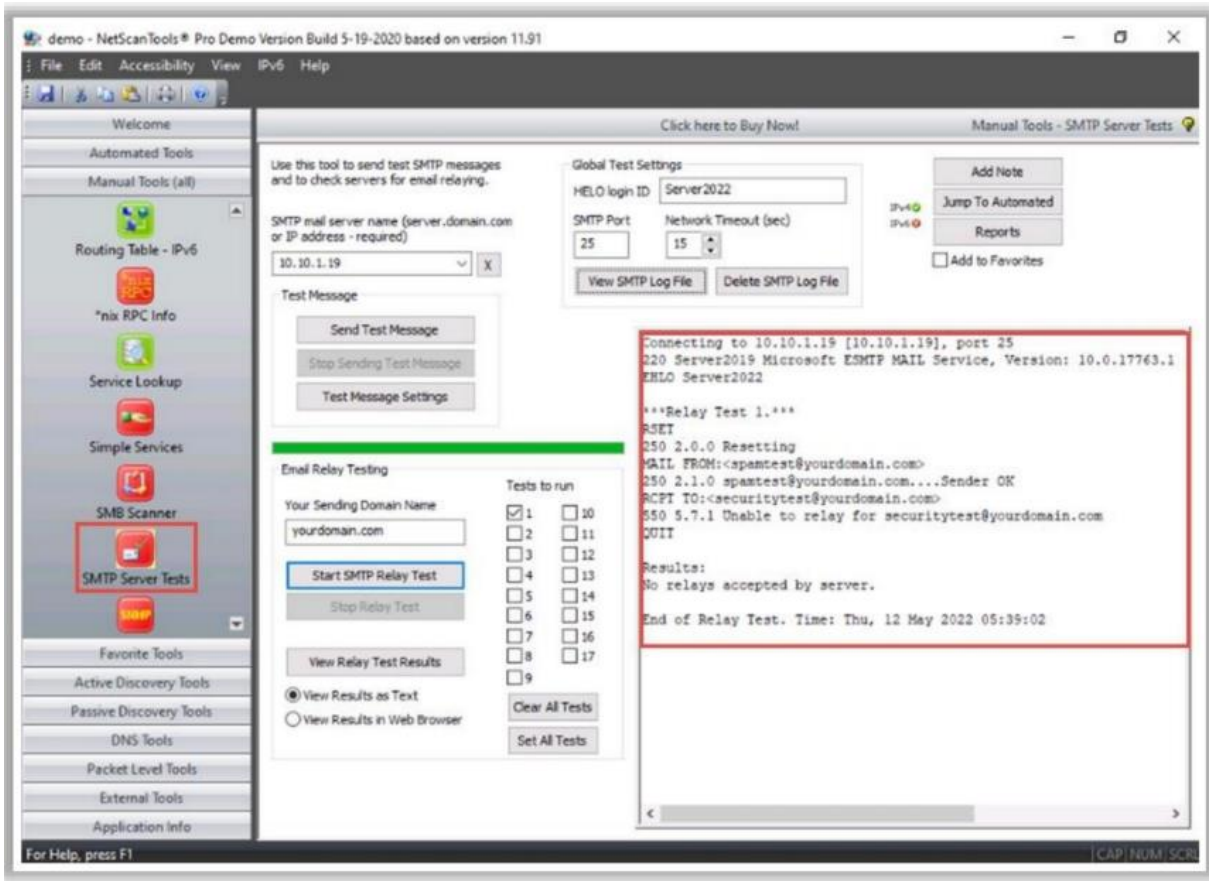
SMTP Enumeration

SMTP (Simple Mail Transfer Protocol) is a set of communication guidelines that allow web applications to perform communication tasks over the internet, including emails. It is a part of the TCP/IP protocol and works on moving emails across the network. SMTP enumeration allows us to identify valid users on the SMTP server. This is done with the built-in SMTP commands using them. VRFY – This command is used to authenticate the user. EXPN – This command displays the actual mailing address for aliases and mailing lists.



SMTP Enumeration Tools

1) Netscan tools pro


demo - NetScanTools® Pro Demo Version Build 5-19-2020 based on version 11.91
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Routing Table - IPv6
*nix RPC Info
Service Lookup
Simple Services
SMB Scanner
SMTP Server Tests
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Click here to Buy Now!
Manual Tools - SMTP Server Tests
Use this tool to send test SMTP messages and to check servers for email relaying.
SMTP mail server name (server.domain.com or IP address - required)
10.10.1.19
Test Message
Send Test Message
Stop Sending Test Message
Test Message Settings
Global Test Settings
HELO login ID
Server2022
SMTP Port
25
Network Timeout (sec)
15
View SMTP Log File
Delete SMTP Log File
Add Note
Jump To Automated
Reports
Add to Favorites
Email Relay Testing
Your Sending Domain Name
yourdomain.com
Start SMTP Relay Test
Stop Relay Test
View Relay Test Results
View Results as Text
View Results in Web Browser
Tests to run
Clear All Tests
Set All Tests
Connecting to 10.10.1.19 [10.10.1.19], port 25
220 Server2019 Microsoft ESMTP MAIL Service, Version: 10.0.17763.1
EHLO Server2022
Relay Test 1.
RSET
250 2.0.0 Resetting
MAIL FROM:<spamtest@yourdomain.com>
250 2.1.0 spamtest@yourdomain.com....Sender OK
RCPT TO:<securitytest@yourdomain.com>
550 5.7.1 Unable to relay for securitytest@yourdomain.com
QUIT
Results:
No relays accepted by server.
End of Relay Test. Time: Thu, 12 May 2022 05:39:02
For Help, press F1
CAP NUM SCRL