EC-Council

C|EH™
Certified Ethical Hacker

Module 04

Enumeration

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

What is Enumeration?

- Enumeration involves an attacker creating active connections with a target system and performing directed queries to gain more information about the target
- Attackers use the extracted information to identify points for a system attack and perform password attacks to gain unauthorized access to information system resources
- Enumeration techniques are conducted in an intranet environment

Information Enumerated by Intruders


Network resources


Network shares


Routing tables


Audit and service settings


SNMP and FQDN details


Machine names


Users and groups


Applications and banners

Techniques for Enumeration

1. Extract usernames using email IDs 
2. Extract information using default passwords 
3. Brute force Active Directory 
4. Extract information using DNS Zone Transfer 
5. Extract user groups from Windows 
6. Extract usernames using SNMP 

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

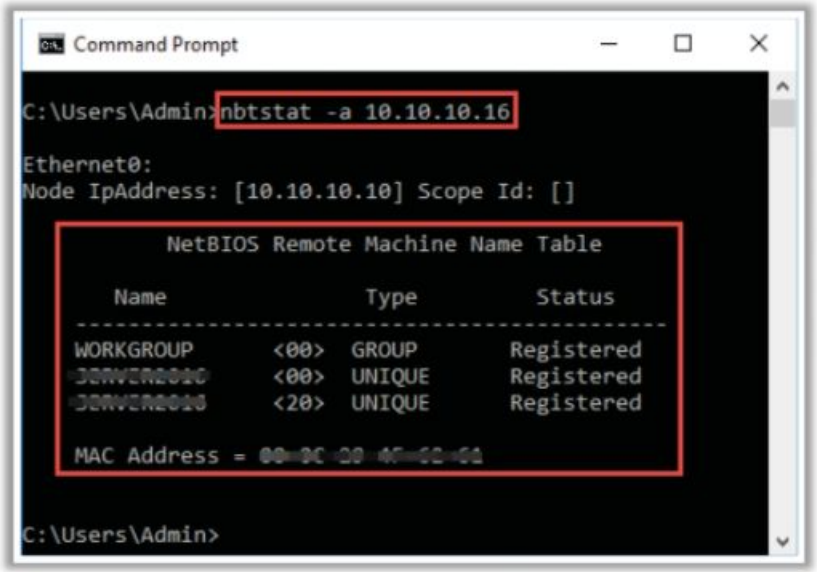
Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<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)

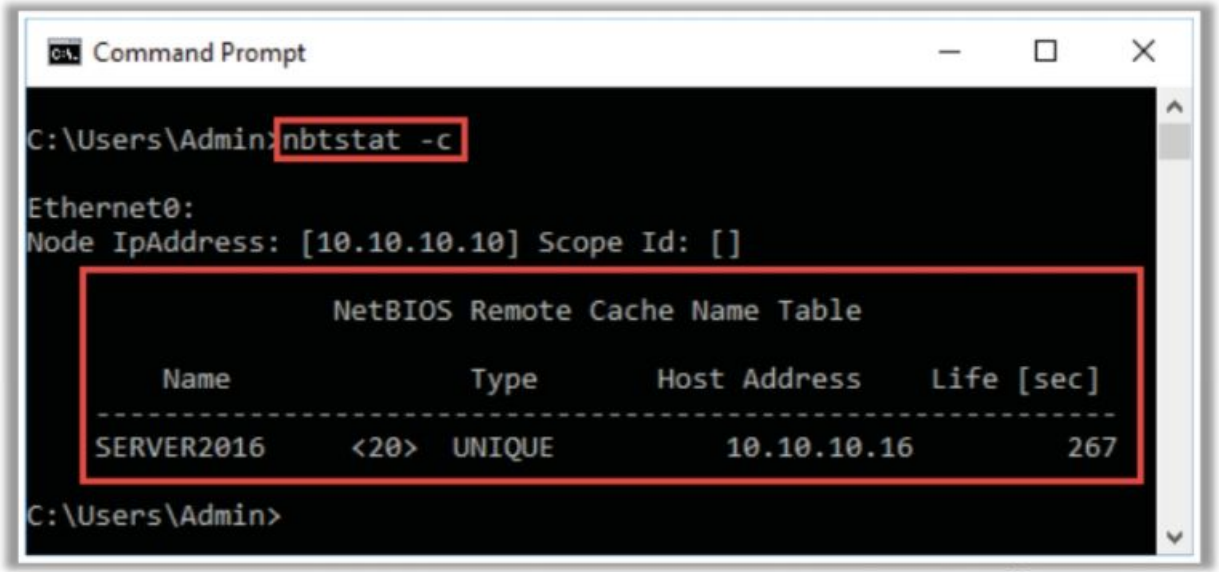
NetBIOS Enumeration (Cont'd)

- The nbtstat utility in Windows displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache

- Run the **nbtstat** command "**nbtstat -a <IP address of the remote machine>**" to obtain the NetBIOS name table of a remote computer



- Run the **nbtstat** command "**nbtstat -c**" to obtain the contents of the NetBIOS name cache, table of NetBIOS names, and their resolved IP addresses

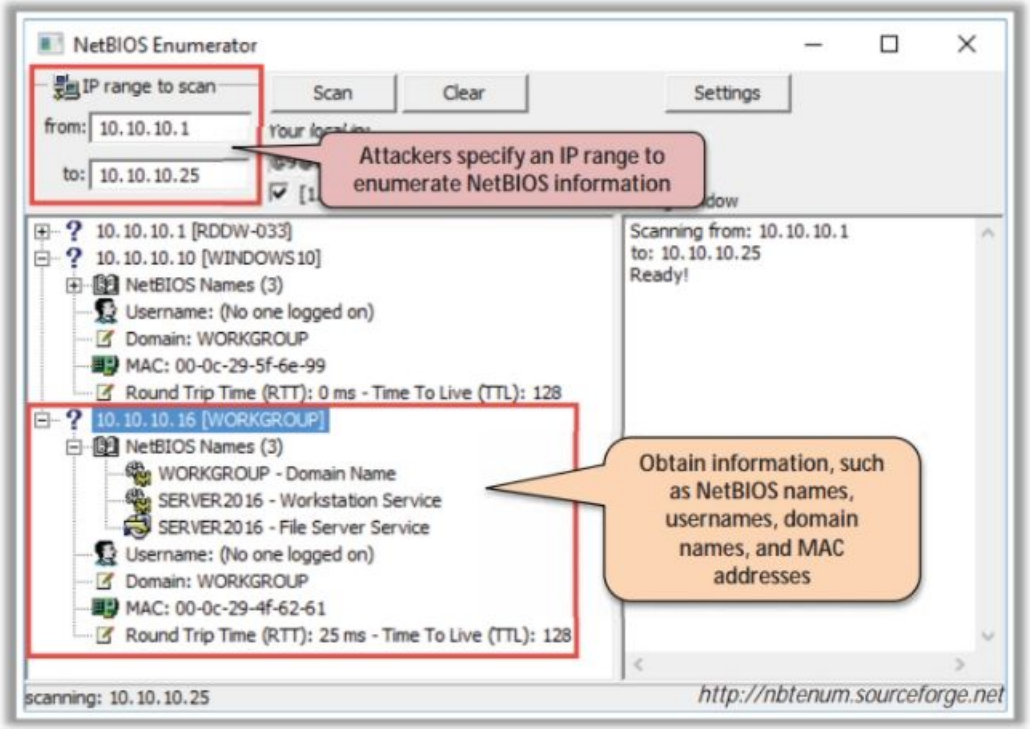


https://docs.microsoft.com

NetBIOS Enumeration Tools

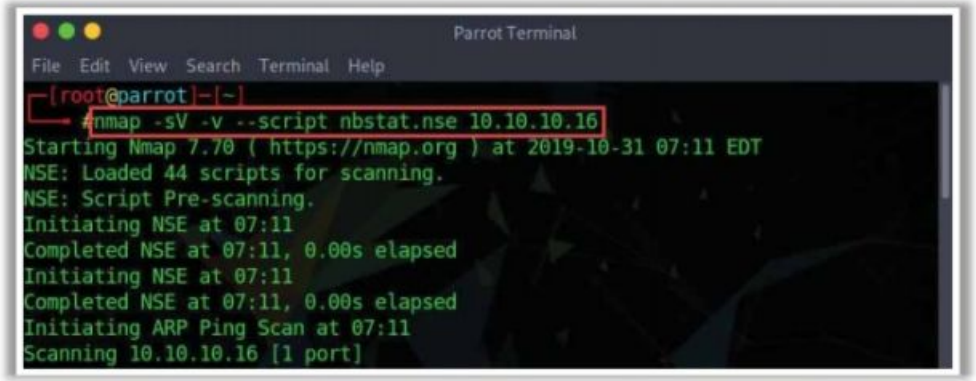
NetBIOS Enumerator

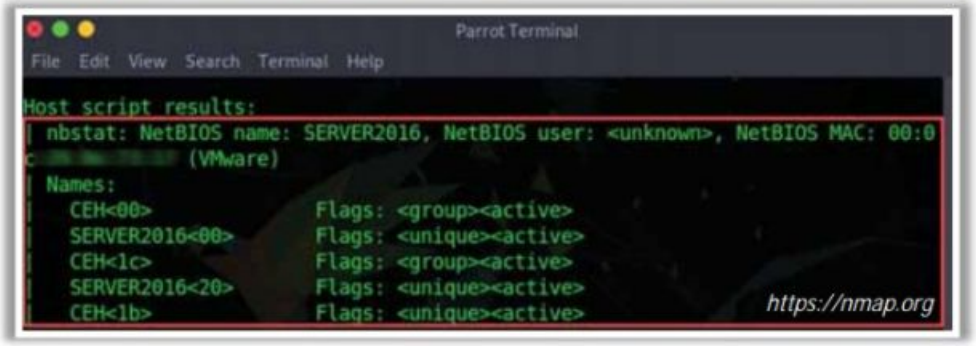
NetBIOS Enumerator helps to enumerate details, such as NetBIOS names, Usernames, Domain names, and MAC addresses, for a given range of IP addresses



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*

Services and Ports to Enumerate

TCP/UDP 53	Domain Name System (DNS) Zone Transfer
TCP/UDP 135	Microsoft RPC Endpoint Mapper
UDP 137	NetBIOS Name Service (NBNS)
TCP 139	NetBIOS Session Service (SMB over NetBIOS)
TCP/UDP 445	SMB over TCP (Direct Host)
UDP 161	Simple Network Management Protocol (SNMP)
TCP/UDP 389	Lightweight Directory Access Protocol (LDAP)
TCP 2049	Network File System (NFS)
TCP 25	Simple Mail Transfer Protocol (SMTP)
TCP/UDP 162	SNMP Trap
UDP 500	ISAKMP/Internet Key Exchange (IKE)
TCP 22	Secure Shell (SSH)

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

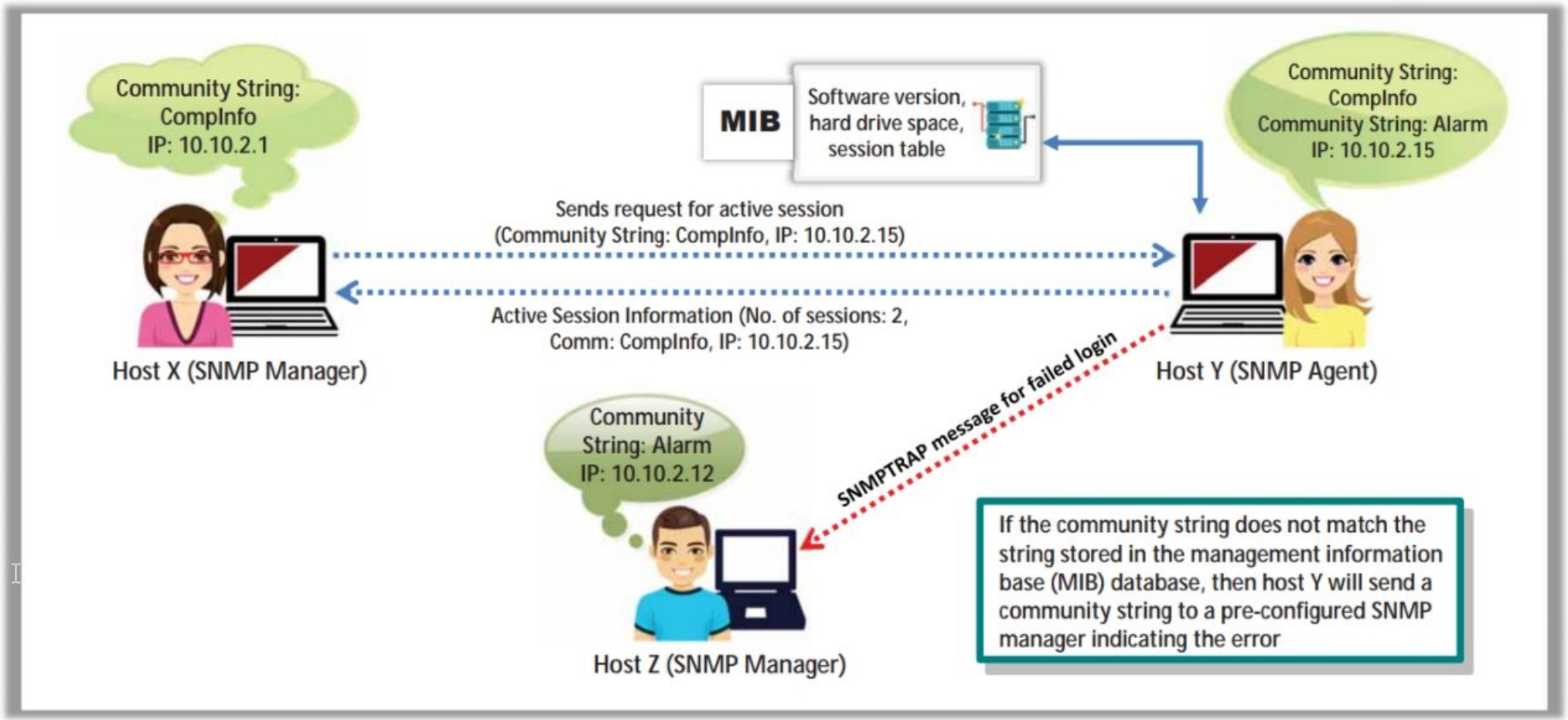
SNMP (Simple Network Management Protocol) Enumeration

- SNMP enumeration is the process of enumerating user accounts and devices on a target system using SNMP
- SNMP consists of a manager and an agent; agents are embedded on every network device, and the manager is installed on a separate computer

- SNMP holds two passwords to access and configure the SNMP agent from the management station
  - Read community string: It is public by default; it allows for the viewing of the device/system configuration
  - Read/write community string: It is private by default; it allows remote editing of configuration

- Attackers use these default community strings to extract information about a device
- Attackers enumerate SNMP to extract information about network resources, such as hosts, routers, devices, and shares, and network information, such as ARP tables, routing tables, and traffic

Working of SNMP



Management Information Base (MIB)

- MIB is a virtual database containing a formal description of all the network objects that can be managed using SNMP

- The MIB database is hierarchical, and each managed object in a MIB is addressed through Object Identifiers (OIDs)

- Two types of managed objects exist:
  - Scalar objects that define a single object instance
  - Tabular objects that define multiple related object instances and are grouped in MIB tables

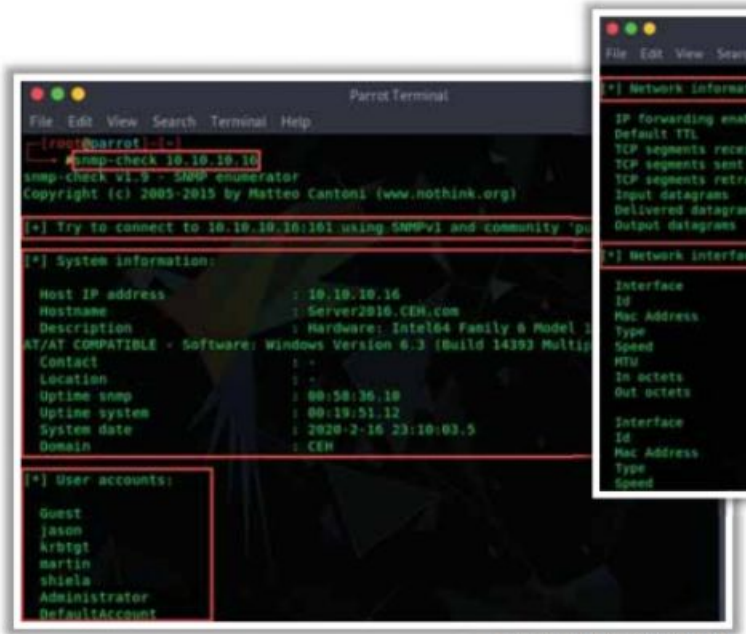
- OID includes the type of MIB object, such as counter, string, or address; access level, such as not-accessible, accessible-for-notify, read-only, or read-write; size restrictions; and range information

- SNMP uses the MIB's hierarchical namespace containing OIDs to translate the OID numbers into a human-readable display

SNMP Enumeration Tools

Snmpcheck

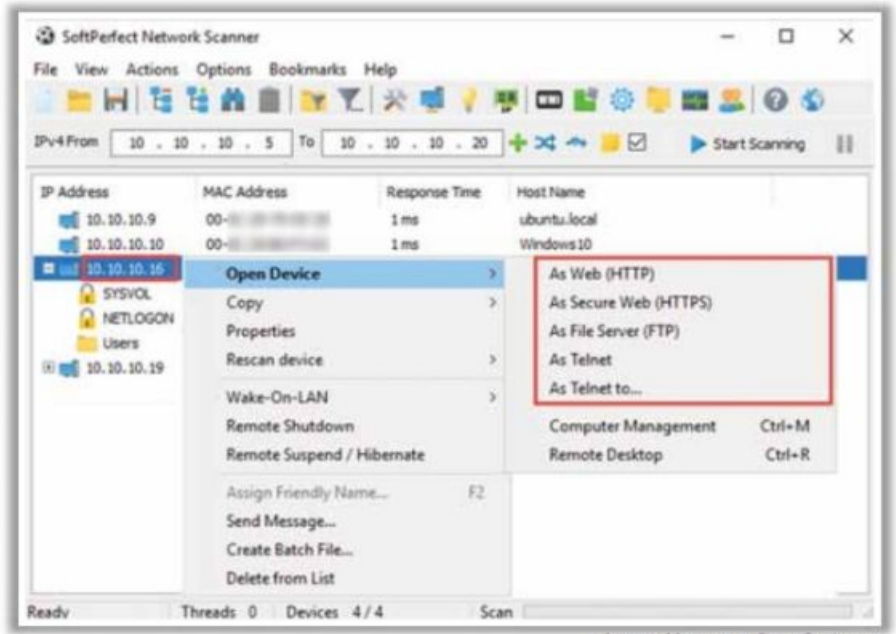
Snmpcheck allows one to enumerate the SNMP devices and place the output in a very human-readable and friendly format



http://www.nothink.org

SoftPerfect Network Scanner

SoftPerfect Network Scanner discovers shared folders and retrieves practically any information about network devices via WMI, SNMP, HTTP, SSH, and PowerShell



https://www.softperfect.com

Other SNMP Enumeration Tools:

Network Performance Monitor	OpUtils	PRTG Network Monitor	Engineer's Toolset
https://www.solarwinds.com	*https://www.manageengine.com*	*https://www.paessler.com*	*https://www.solarwinds.com*

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

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

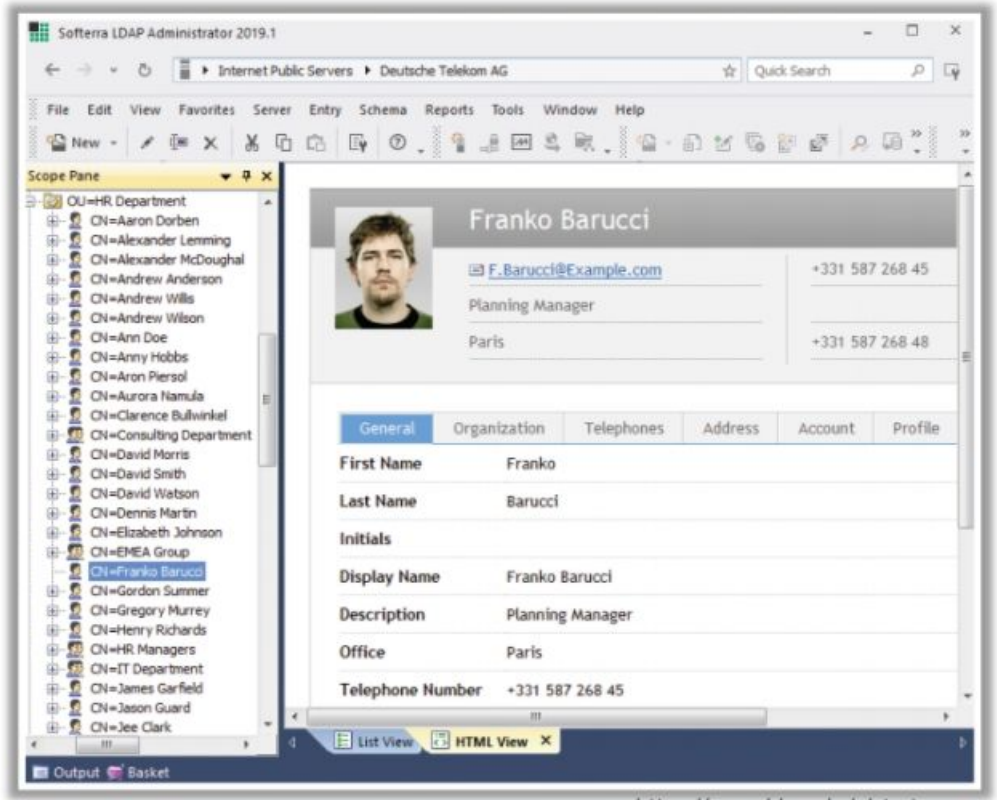
4. Information is transmitted between the client and server using basic encoding rules (BER)

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

LDAP Enumeration Tools

Softerra LDAP Administrator

Softerra LDAP Administrator provides various features essential for LDAP development, deployment, and administration of directories



https://www.ldapadministrator.com

- **LDAP Admin Tool**
  https://www.ldapsoft.com
- **LDAP Account Manager**
  https://www.ldap-account-manager.org
- **LDAP Search**
  https://securityxploded.com
- **JXplorer**
  http://www.jxplorer.org
- **Active Directory Explorer (AD Explorer)**
  https://docs.microsoft.com

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

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

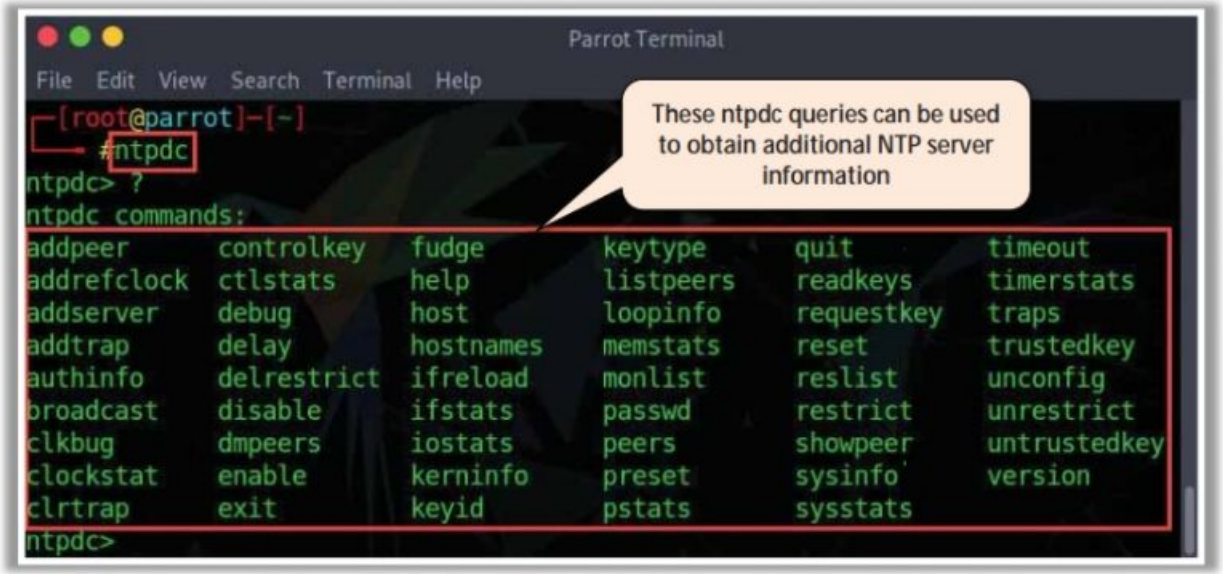
Attackers query the NTP server to gather valuable information, such as

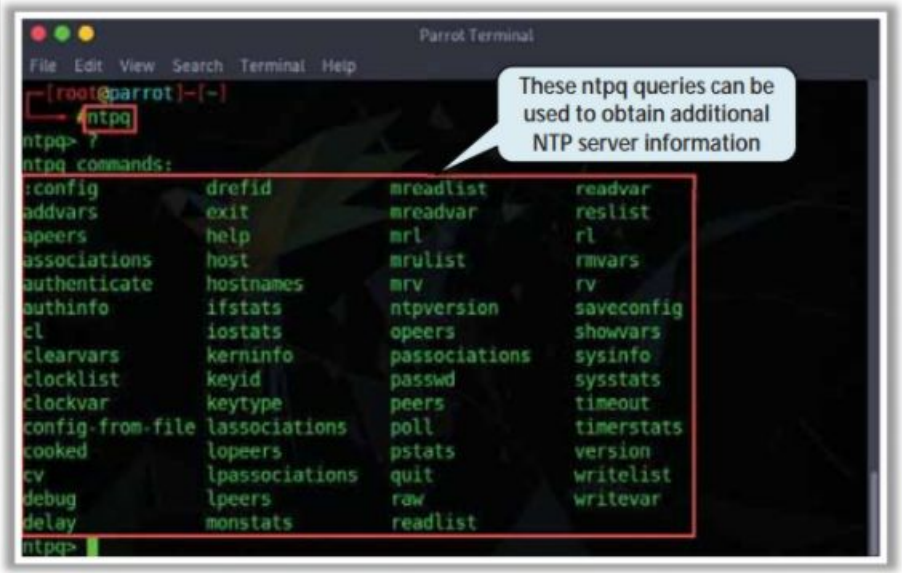
- List of connected hosts
- Clients IP addresses in a network, their system names, and OSs
- Internal IPs can also be obtained if the NTP server is in the demilitarized zone (DMZ)

NTP Enumeration Commands

- **ntptrace**
  - Traces a chain of NTP servers back to the primary source
  - `ntptrace [-n] [-m maxhosts] [servername/IP_address]`
- **ntpdc**
  - Monitors operation of the NTP daemon, ntpd
  - `ntpdc [-ilnps] [-c command] [host] [...]`

- **ntpq**
  - Monitors NTP daemon (ntpd) operations and determines performance
  - `ntpq [-inp] [-c command] [host] [...]`



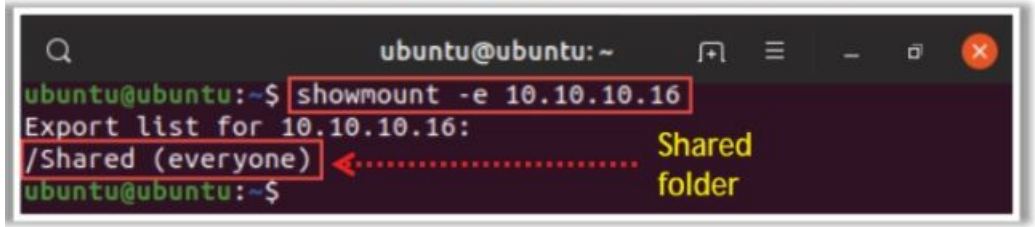


NFS Enumeration

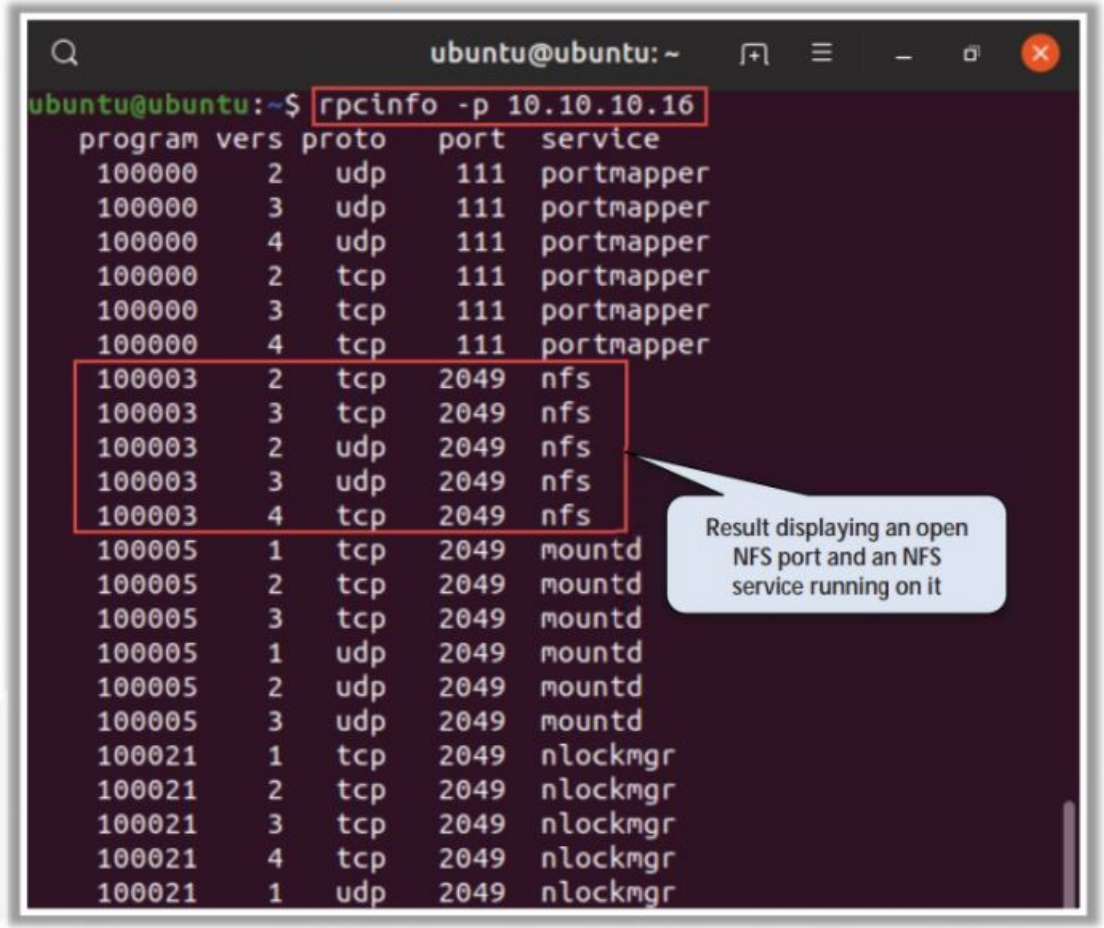
- The NFS system is generally implemented on the computer network, where the centralization of data is required for critical resources

- NFS enumeration enables attackers to identify the exported directories, list of clients connected to the NFS server along with their IP addresses, and the shared data associated with the IP addresses

showmountcommand



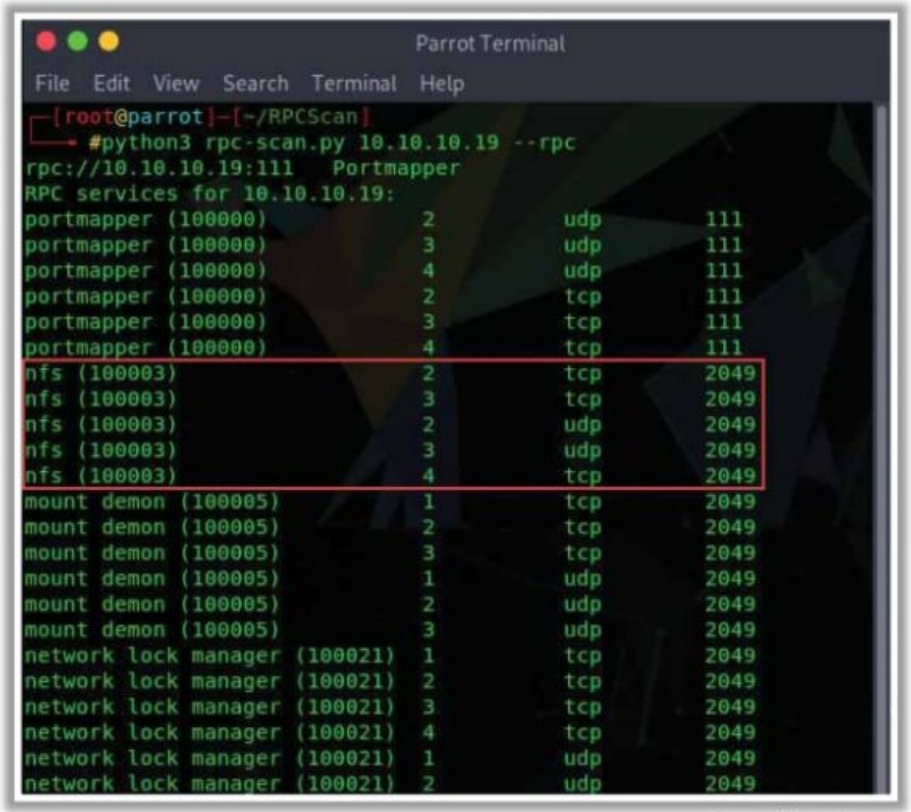
rpcinfo command



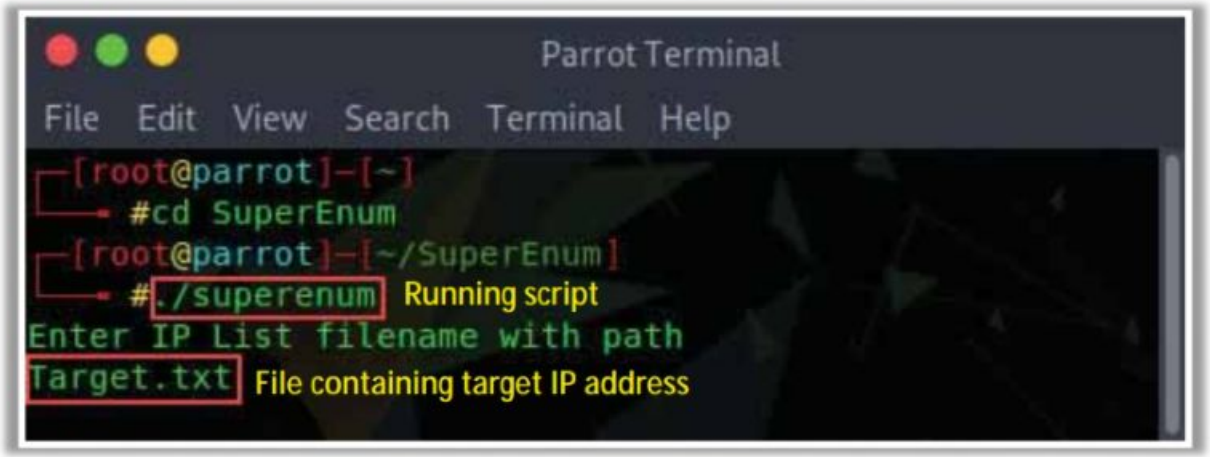
NFS Enumeration Tools

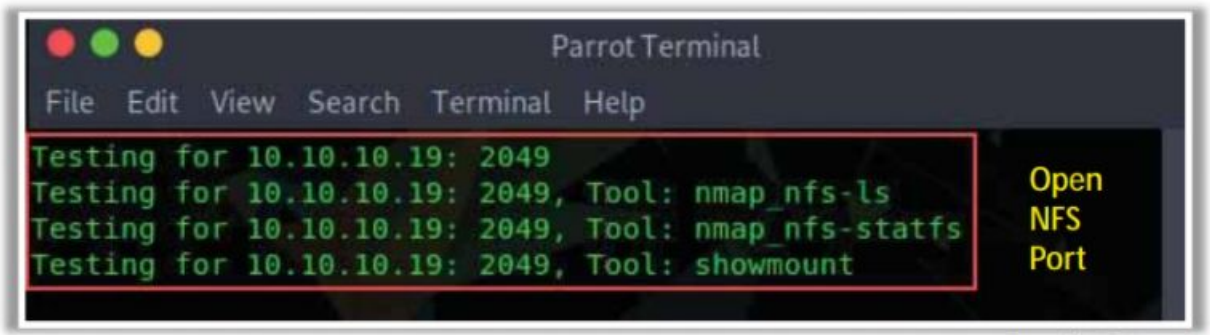
RPCScan — RPSCan communicates with RPC services and checks misconfigurations on NFS shares

SuperEnum — SuperEnum includes a script that does the basic enumeration of any open port



https://github.com





https://github.com

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

SMTP Enumeration

- SMTP provides 3 built-in-commands:
  - VRFY - Validates users
  - EXPN - Shows the actual delivery addresses of aliases and mailing lists
  - RCPT TO - Defines the recipients of a message
- SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users, based on which we can determine valid users on the SMTP server
- Attackers can directly interact with SMTP via the telnet prompt and collect a list of valid users on the SMTP server

Using the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Using the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

Using the SMTP RCPT TO Command

```
$ telnetl 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased
to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

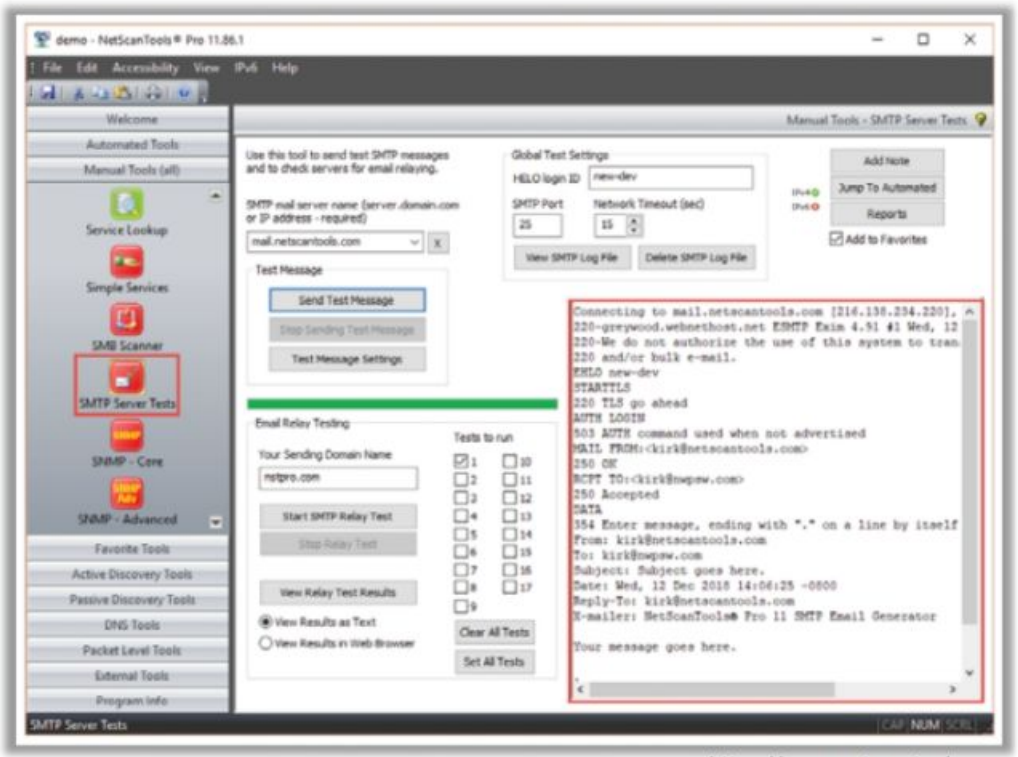
SMTP Enumeration Tools

NetScan Tools Pro

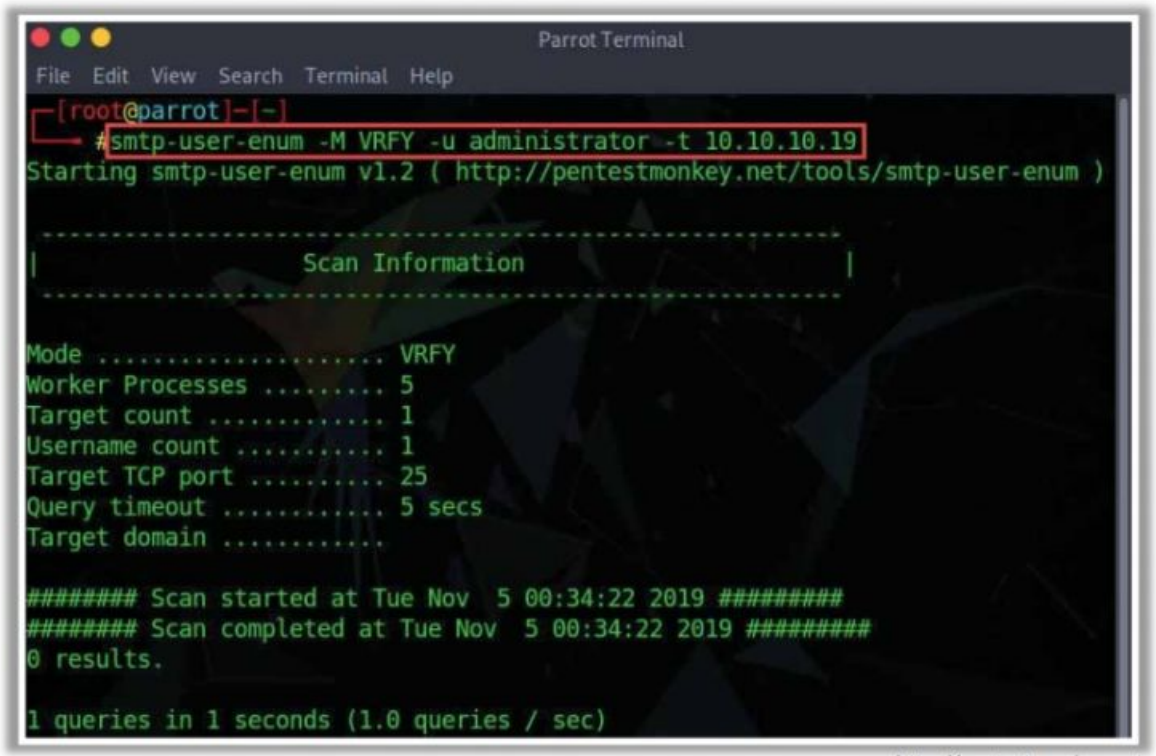
- NetScanTools Pro's SMTP Email Generator tool tests the process of sending an email message through an SMTP server

smtp-user-enum

- It is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail)
- Enumeration is performed by inspecting the responses to VRFY, EXPN, and RCPT TO commands



https://www.netscantools.com

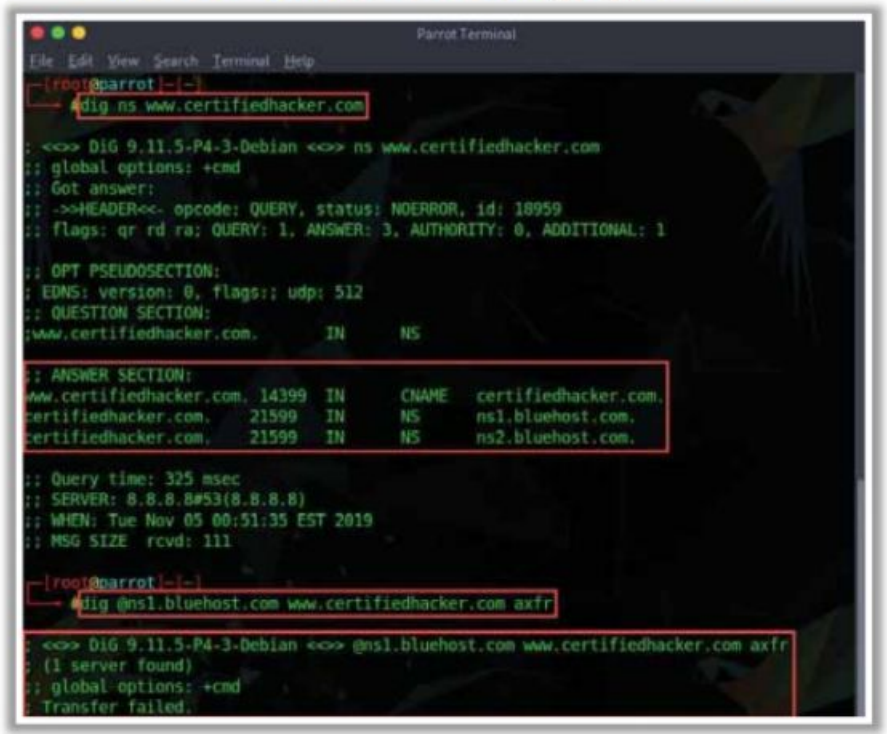


http://pentestmonkey.net

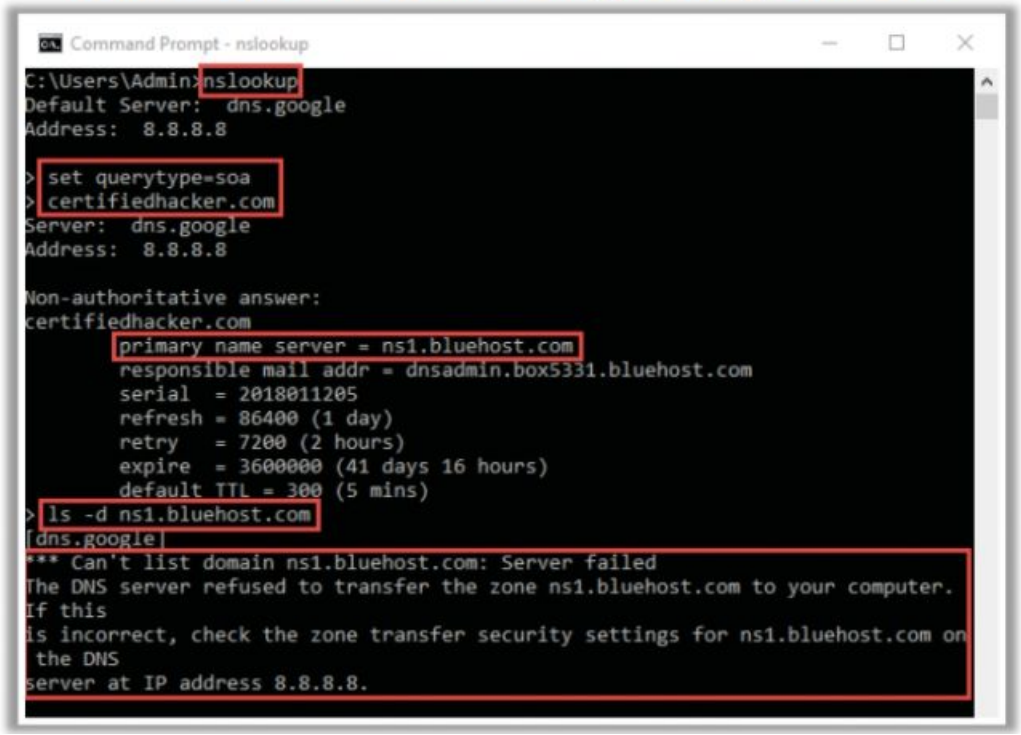
DNS Enumeration Using Zone Transfer

- If the target DNS server allows zone transfers, then attackers use this technique to obtain DNS server names, hostnames, machine names, usernames, IP addresses, aliases, etc. assigned within a target domain
- Attackers perform DNS zone transfer using tools, such as nslookup, dig, and DNSRecon; if DNS transfer setting is enabled on the target name server, it will provide DNS information, or else it will return an error saying it has failed or refuses the zone transfer

Linux DNS zone transferusing dig command



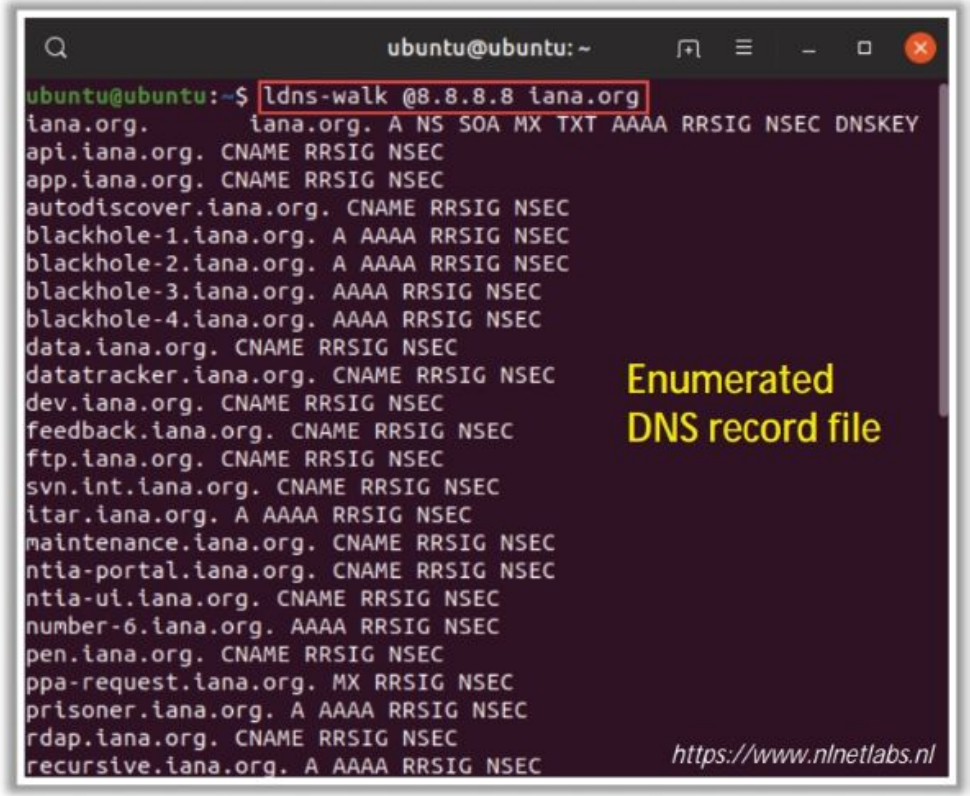
Windows DNS zone transferusing nslookup command



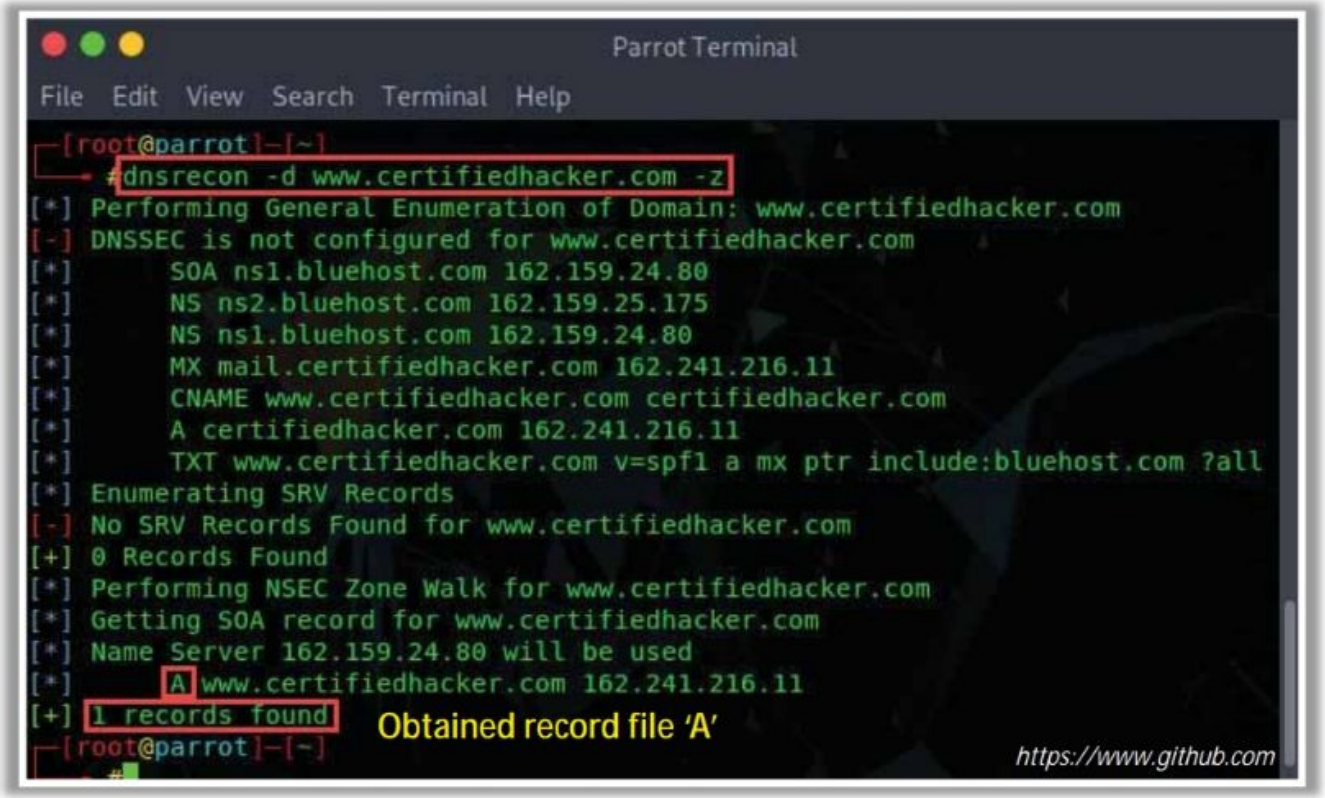
DNSSEC Zone Walking

- DNSSEC zone walking is a DNS enumeration technique where an attacker attempts to obtain internal records of the DNS server if the DNS zone is not properly configured
- Attackers use tools, such as LDNS and DNSRecon, to exploit this vulnerability and obtain the network information of a target domain and further launch Internet-based attacks

LDNS



DNSRecon



Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

Enumeration Countermeasures

SNMP

- Remove the SNMP agent or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default community string names
- Upgrade to SNMP3, which encrypts passwords and messages
- Implement the Group Policy security option called "Additional restrictions for anonymous connections"
- Ensure that the access to null session pipes, null session shares, and IPSec filtering is restricted
- Do not misconfigure SNMP service with read-write authorization

DNS

- Disable the DNS zone transfers to the untrusted hosts
- Ensure that the private hosts and their IP addresses are not published in DNS zone files of public DNS servers
- Use premium DNS registration services that hide sensitive information, such as host information (HINFO) from the public
- Use standard network admin contacts for DNS registrations to avoid social engineering attacks

Enumeration Countermeasures (Cont'd)

SMTP

Configure SMTP servers to

- Ignore email messages to unknown recipients
- Exclude sensitive mail server and local host information in mail responses
- Disable open relay feature
- Limit the number of accepted connections from a source to prevent brute-force attacks

LDAP

- By default, LDAP traffic is transmitted unsecured; use SSL or STARTTLS technology to encrypt the traffic
- Select a username different from your email address and enable account lockout
- Use NTLM or any basic authentication mechanism to limit access to legitimate users only

SMB

- Disable SMB protocol on Web and DNS Servers
- Disable SMB protocol on Internet facing servers
- Disable ports TCP 139 and TCP 445 used by the SMB protocol
- Restrict anonymous access through RestrictNullSessAccess parameter from the Windows Registry

Enumeration Countermeasures (Cont'd)

NFS

- Implement **proper permissions** (read/write must be restricted to specific users) on exported file systems
- Implement **firewall rules** to block NFS port 2049
- Ensure **proper configuration** of files, such as `/etc/smb.conf`, `/etc/exports` and `etc/hosts.allow`, to protect the data stored in servers
- **Log requests** to access system files on the NFS server
- Keep the `root_squash` option in `/etc/exports` file turned **ON**, so that no requests made as root on the client are trusted

FTP

- Implement **secure FTP** (SFTP, which uses SSH) or FTP secure (FTPS, which uses SSL) to encrypt the FTP traffic over the network
- Implement **strong passwords** or a certification-based authentication policy
- Ensure that **unrestricted uploading of files** on the FTP server is **not allowed**
- **Disable anonymous FTP accounts**; if not feasible, regularly monitor anonymous FTP accounts
- **Restrict access by IP or domain name** to the FTP server

Module Summary

- In this module, we have discussed the following:
  - Enumeration concepts along with techniques, services, and ports used for enumeration
  - How attackers perform enumeration using different techniques (NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration) to gather more information about a target
  - How organizations can defend against enumeration activities
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen testers, perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems