

Module 04

Enumeration

Learning Objectives

- 01** Explain Enumeration Concepts
- 02** Demonstrate Different Techniques for NetBIOS Enumeration
- 03** Demonstrate Different Techniques for SNMP Enumeration and LDAP Enumeration
- 04** Use Different Techniques for NTP and NFS Enumeration
- 05** Demonstrate Different Techniques for SMTP and DNS Enumeration
- 06** Demonstrate IPsec, VoIP, RPC, Unix/Linux, and SMB Enumeration
- 07** Explain Enumeration Countermeasures

Objective **01**

Explain Enumeration Concepts

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

Objective **02**

Demonstrate Different Techniques for NetBIOS Enumeration

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

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

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

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

NetBIOS Enumeration (Cont'd)

Nbtstat Utility

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

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.11

Ethernet 2:
Node IpAddress: [10.10.1.19] Scope Id: []

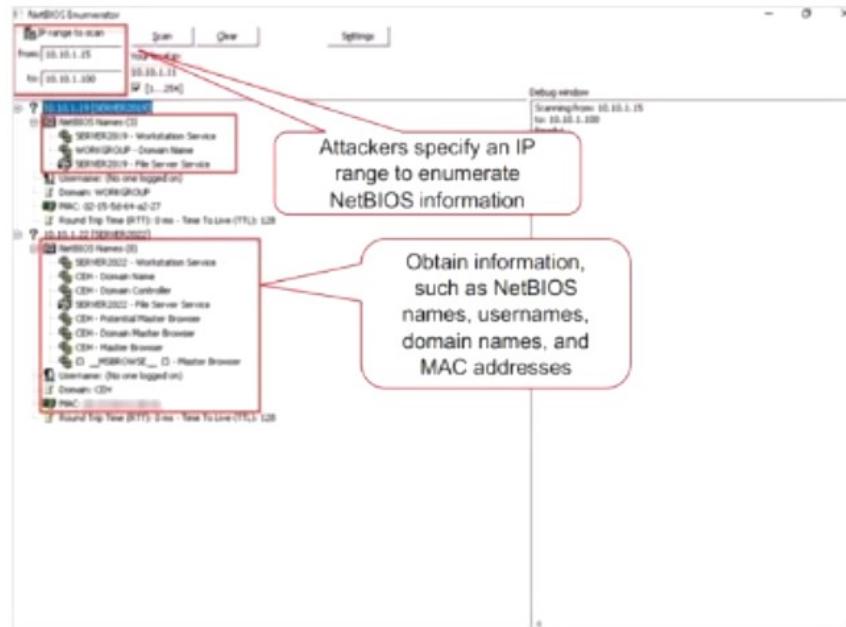
NetBIOS Remote Machine Name Table

Name          Type      Status
WINDOWS$11    <00>    UNIQUE   Registered
WORKGROUP     <00>    GROUP    Registered
WINDOWS$11    <20>    UNIQUE   Registered
WORKGROUP     <1E>    GROUP    Registered
WORKGROUP     <1D>    UNIQUE   Registered
00_MSBBROWSE_<01> GROUP    Registered

MAC Address = 00-0c-29-00-00-00
```

<https://learn.microsoft.com>

NetBIOS Enumerator



<https://nbtenum.sourceforge.net>

Other NetBIOS Enumeration Tools:

Nmap

<https://nmap.org>

Global Network Inventory

<https://magnetosoft.com>

Advanced IP Scanner

<http://www.advanced-ip-scanner.com>

Hyena

<https://www.systemtools.com>

Enumerating Shared Resources Using Net View

- The Net View utility is used to obtain a list of all the **shared resources of a remote host or workgroup**

Net View Commands

- `net view \\<computername>`
- `net view /domain:<domain name>`

A screenshot of a Windows Command Prompt window titled "Select Administrator: Command Prompt". The window shows the command `net view \\10.10.1.22 /ALL` being run, followed by a list of shared resources on the remote host \\\10.10.1.22. The output is as follows:

Share name	Type	Used as	Comment
ADMIN\$	Disk		Remote Admin
C\$	Disk		Default share
IPC\$	IPC		Remote IPC
NETLOGON	Disk		Logon server share
SYSVOL	Disk		Logon server share
Users	Disk		

The command completed successfully.

C:\Users\Administrator>

NetBIOS Enumeration using AI

- Attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using appropriate prompt such as
"Perform NetBIOS enumeration on target IP 10.10.1.11"
"Get NetBIOS info for IP 10.10.1.11 and display the associated names"
"Enumerate NetBIOS on target IP 10.10.1.22 with nmap"

```
[attacker@parrot:~]
--> $sgpt --shell 'Perform NetBIOS enumeration on target IP 10.10.1.11'
Please enter your OpenAI API key:
[!]token: 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Doing NBT name scan for addresses from 10.10.1.11

IP address      NetBIOS Name      Server      User      MAC address
-----          -----          -----          -----          -----
10.10.1.11      WIND0WS11      <server>    <unknown>  00:15:5d:01:88:00
```

```
[attacker@parrot:~]
--> $sgpt --shell "Get NetBIOS info for IP 10.10.1.11 and display the associated names"
[!]token: 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Looking up status of 10.10.1.11
  WIND0WS11  <00> -      B <ACTIVE>
  WORKGROUP  <00> - <GROUP> B <ACTIVE>
  WIND0WS11  <20> -      B <ACTIVE>
  WORKGROUP  <1e> - <GROUP> B <ACTIVE>
  WORKGROUP  <1d> -      B <ACTIVE>
  ..._MSBROWSE_ <01> - <GROUP> B <ACTIVE>

  MAC Address = 00:15:5d:01:88:00
```

```
[root@parrot:~/home/attacker]
--> #sgpt --shell 'Enumerate NetBIOS on target IP 10.10.1.22 with nmap'
nmap -sU -A -T4 -oN /tmp/nmap_out.txt 10.10.1.22
(E)execute, (D)escribe, (A)bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 07:58 EDT
Nmap scan report for 10.10.1.22
Host is up (0.0012s latency).

PORT      STATE SERVICE
137/udp  open  netbios-ns
MAC Address: 00:15:5d:01:88:02 (Microsoft)

PORT      STATE SERVICE
137/udp  open  netbios-ns
MAC Address: 00:15:5d:01:88:02 (Microsoft)

Host script results:
nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:88:02 (Microsoft)
)
Names:
  CEH<00>                Flags: <group><active>
  CEH<1c>                Flags: <group><active>
  SERVER2022<00>          Flags: <unique><active>
  SERVER2022<20>          Flags: <unique><active>
  CEH<1e>                Flags: <group><active>
  CEH<1b>                Flags: <unique><active>
  CEH<1d>                Flags: <unique><active>
  \x01\x02__MSBROWSE_\x02\x01> Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Objective **03**

Demonstrate Different Techniques for SNMP Enumeration and LDAP Enumeration

SNMP (Simple Network Management Protocol)

Enumeration

- Attackers use SNMP **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

Enumerating SNMP using SnmpWalk and Nmap

```
snmpwalk -v1 -c public 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot ~]$
$ sudo su
[sudo] password for attacker
[attacker@parrot ~]# /home/attacker
[attacker@parrot ~]# snmpwalk -v1 -c public 10.10.1.22
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel(R) Dual Band Wireless-AC 7265"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (2889990469) 334 days, 11:45:04.69
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Sezver2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
```

<https://ezfive.com>

```
nmap -sU -p 161 --script=snmp-processes 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot ~]#
$ sudo su
[sudo] password for attacker
[attacker@parrot ~]# /home/attacker
[attacker@parrot ~]# nmap -sU -p 161 --script=snmp-processes 10.10.1.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 05:24 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00077s latency).

PORT      STATE SERVICE
161/udp    open  snmp

snmp-processes:
  1:
    Name: System Idle Process
  4:
    Name: System
  72:
    Name: svchost.exe
    Path: C:\Windows\system32\
    Params: -k DcomLaunch -p -s LS
  96:
    Name: Registry
  376:
    Name: smss.exe
```

<https://nmap.org>

Other SNMP
Enumeration Tools:

snmp-check
<https://www.nothink.org>

SoftPerfect Network Scanner
<https://www.softperfect.com>

Network Performance Monitor
<https://www.solarwinds.com>

OpUtils
<https://www.manageengine.com>

SNMP Enumeration with SnmpWalk and Nmap using AI

- Attacker can also leverage AI powered ChatGPT or other generative AI technology to perform this task by using appropriate prompt such as
 - “Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here”
 - “Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here“

```
→ #sgpt --chat enum --shell " Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here "
nmap -sU -p 161 --script snmp-info 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:11 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00028s latency).

PORT      STATE SERVICE
161/udp    open   snmp
MAC Address: 00:15:5D:01:80:02 (Microsoft)
```

LDAP Enumeration

Lightweight directory access protocol (LDAP) is an **Internet protocol** for accessing distributed directory services

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

Attackers query the LDAP service to gather information, such as **valid usernames, addresses**, and **departmental details**, which can be further used to perform attacks

Other LDAP Enumeration Tools:

Softerra LDAP Administrator
<https://www.ldapadministrator.com>

ldapsearch

AD Explorer
<https://docs.microsoft.com>

LDAP Admin Tool
<https://www.ldapsoft.com>

Manual LDAP Enumeration

Automated LDAP Enumeration

Objective **04**

Use Different Techniques for NTP and NFS Enumeration

NTP Enumeration and NTP Enumeration Commands

Attackers query the NTP server to gather valuable information, such as list of **connected hosts** and **Clients' IP addresses** in a network, their system names, and OSs

- **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] [...]**

```
ubuntu@ubuntu-Virtual-Machine: ~
ubuntu@ubuntu-Virtual-Machine: ~ $ ntpdc
ntpdc> ?
ntpdc commands:
addpeer    controlkey   fudge      keytype    quit      timeout
addrefclock  ctlsstats   help       listpeers  readkeys  timerstats
addserver   debug       host       loopinfo   requestkey traps
addtrap     delay       hostnames  memstats  reset     trustedkey
authinfo    delrestrict ifreload  monlist   reslist   unconfig
broadcast   disable     ifstats   passwd   restrict  unrestrict
clkbug     dmpeers    iostats   peers     showpeer untrustedkey
clockstat  enable     kerninfo  preset    sysinfo  version
clrtrap    exit       keyid    pstats   sysstats
```

These ntpdc queries can be used to obtain additional NTP server information

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

```
ubuntu@ubuntu-Virtual-Machine: ~
ubuntu@ubuntu-Virtual-Machine: ~ $ ntpq
ntpq> ?
ntpq commands:
cconfig    drefid    mreadlist  readvar
addvars   exit      mreadvar  reslist
speers    help      mrl        rl
associations  host    mrulist  rmvars
authenticate hostnames  mrv      rv
authinfo   ifstats  opeers    showvars
cl        iostats  passassociations  saveconfig
clearvars  kerninfo  peers    showvars
clocklist  keyid   passwd   sysinfo
clockvar   keytype  peers    timeout
config-from-file lassociations  poll   timerstats
cooked    lpeers   pstats   version
cv        lpassociations  quit   writelist
debug    lpairs   raw     writevar
delay    monstats  readlist
```

These ntpq queries can be used to obtain additional NTP server information

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

Attackers use tools such as **RPSCan** and **SuperEnum** to perform NFS enumeration

showmount command

```
showmount -e 10.10.1.9 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot] -| ~
$showmount -e 10.10.1.9
Export list for 10.10.1.9:
/home * <----- Shared folder
```

rpcinfo command

```
ubuntu@ubuntu-Virtual-Machine: ~ $ rpcinfo -p 10.10.1.13
program vers proto port service
100000 4 tcp 111 portmapper
100000 3 tcp 111 portmapper
100000 2 tcp 111 portmapper
100000 4 udp 111 portmapper
100000 3 udp 111 portmapper
100000 2 udp 111 portmapper
100024 1 udp 50883 status
100024 1 tcp 41813 status
100005 1 udp 59085 mountd
100005 1 tcp 38127 mountd
100005 2 udp 48885 mountd
100005 2 tcp 39347 mountd
100005 3 udp 42995 mountd
100005 3 tcp 48399 mountd
100003 3 tcp 2849 nfs
100003 4 tcp 2849 nfs
100227 3 tcp 2849 nlockmgr
100021 1 udp 55478 nlockmgr
100021 3 udp 55478 nlockmgr
100021 4 udp 55478 nlockmgr
100021 1 tcp 42867 nlockmgr
100021 3 tcp 42867 nlockmgr
100021 4 tcp 42867 nlockmgr
```

Objective **05**

Demonstrate Different Techniques for SMTP and DNS Enumeration

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

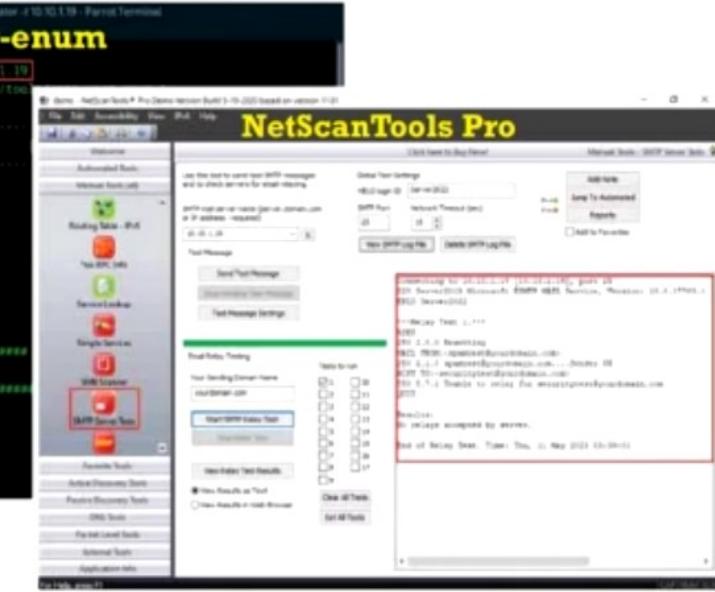
```
$ telnet 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder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

SMTP Enumeration (Cont'd)

```
nmap -p 25 --script=smtp-enum-users  
File Edit View Search Terminal Help  
attacker@parrot:~$ sudo su  
[sudo] password for attacker:  
root@parrot:~# /home/attacker/nmap  
# nmap -p 25 --script=smtp-enum-users  
Starting Nmap 7.94SN ( https://nmap.org )  
Nmap scan report for www.goodshopping.com (127.0.0.1)  
Host is up (0.00058s latency).  
  
PORT      STATE SERVICE  
25/tcp    open  smtp  
| smtp-enum-users  
|_ root  
|_ admin  
|_ administrato  
|_ webadmin  
|_ sysadmin  
|_ netadmin  
|_ guest  
|_ user  
|_ web  
|_ test  
MAC Address 02:15:5D:64:A2:27 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned
```

<https://www.metasploit.com>

<https://pentestmonkey.net>



SMTP Enumeration using AI

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using appropriate prompt such as

- “Perform SMTP enumeration on target IP 10.10.1.19.”
- “Perform SMTP enumeration on target IP 10.10.1.19 with metasploit”

```
$sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19"
nmap -p25 --script smtp-enum-users --script-args smtp-enum-users.methods=(VRFY,EXPN,F
PT) 10.10.1.19 -oN ./enumeration_results/smtp_enum_10.10.1.19.txt
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SNN ( https://nmap.org ) at 2024-03-15 06:38 EDT
Failed to resolve "smtp-enum-users.methods=EXPN".
Failed to resolve "smtp-enum-users.methods=RCPT".
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00059s latency).

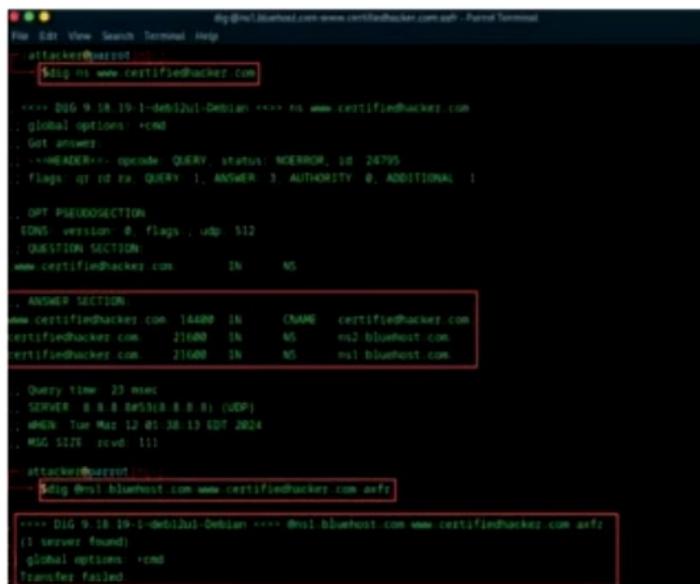
PORT      STATE SERVICE
25/tcp    open  smtp
|_ SMTP-ENUM-USERS:
    root
    admin
    administrator
    webadmin
    sysadmin
    netadmin
    guest
    user
    web
    test
```

```
[attacker@parrot] ~
$sgpt --shell "Perform SMTP enumeration on target IP 10.10.1.19 with metasploit"
msfconsole -q -x "use auxiliary/scanner/smtp/smtp_enum; set RHOSTS 10.10.1.19; run; exit"
[E]xecute, [D]escribe, [A]bort: E
RHOSTS => 10.10.1.19
[*] 10.10.1.19:25      - 10.10.1.19:25 Skipping microsoft (220 Server2019 Microsoft ESMTP MAIL Ser
vice, Version: 10.0.17763.1 ready at Fri, 15 Mar 2024 05:36:00 -0700 )
[*] 10.10.1.19:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[attacker@parrot] ~
$
```

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 transfer using dig command

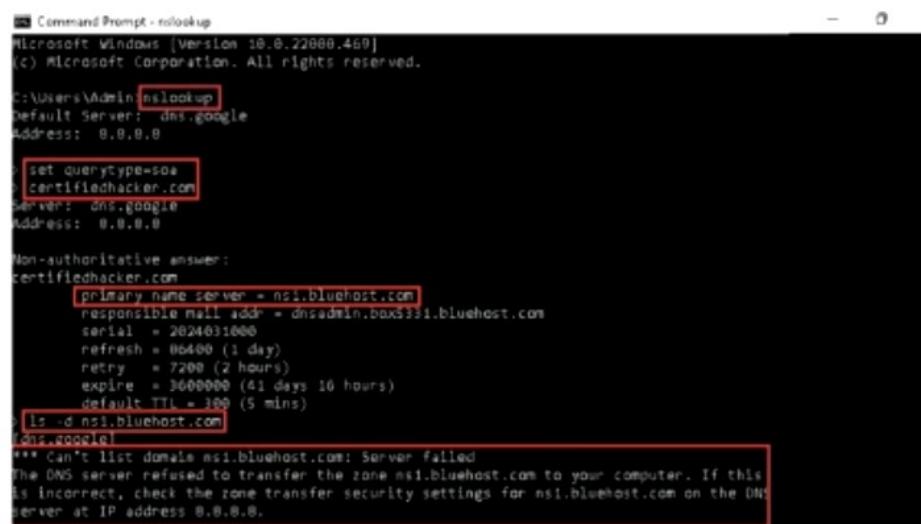


```
dig ns www.certifiedhacker.com
...
ANSWER SECTION
www.certifiedhacker.com. IN      CNAME   certifiedhacker.com.
certifiedhacker.com. 21600 IN      NS       ns1.bluehost.com.
certifiedhacker.com. 21600 IN      NS       ns2.bluehost.com.
certifiedhacker.com. 21600 IN      NS       ns3.bluehost.com.

Query time: 23 msec
SERVER: 8.8.8.8 (dns321) (UDP)
WHEN: Tue Mar 12 05:38:13 EDT 2024
MSG SIZE rcvd: 111

dig ns1.bluehost.com www.certifiedhacker.com axfr
...
*** DIG 9.18.19-1-debian-Debian *** @ns1.bluehost.com www.certifiedhacker.com axfr
(1 servers found)
global options: +rdns
Transfer failed
```

Windows DNS zone transfer using nslookup command



```
nslookup
Default Server: dns.google
Address: 8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box3331.bluehost.com
    serial = 2024031800
    refresh = 06400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
> ls -d ns1.bluehost.com
(dns.google)

*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer. If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on the DNS
server at IP address 8.8.8.8.
```

DNS Cache Snooping

- DNS cache snooping is a **DNS enumeration** technique whereby an **attacker queries the DNS server** for a specific cached DNS record

Non-recursive Method

Attackers send a **non-recursive query** by setting the **Recursion Desired (RD)** bit in the query header to zero

```
dig @162.159.25.175 certifiedhacker.com A +nosecuse -Parrot Terminal
attacker@parrot: ~%
```

```
dig @162.159.25.175 certifiedhacker.com A +nosecuse

;;> QD=1, RD=0, RA=0, Z=0, NXRRSIG=0, NSEC3=0, NSEC3PARAM=0, CNAME=0
;;> OPT PSEUDOSECTION
;;> EDNS version 0, flags: rd 1282
;;> QUESTION SECTION:
certifiedhacker.com. IN A

;; ANSWER SECTION:
certifiedhacker.com. 14400 IN A 162.243.236.11

Query time: 19 msec
SERVER: 162.159.25.175#53(162.159.25.175) (UDP)
AREN: Tue May 12 02:36:28 EDT 2024
MSG: 532B, DLEN: 64
```

Indicates that the query is accepted, but the site is not cached

Recursive Method

Attackers send a recursive query to **determine the time** the **DNS record** resides in the cache

```
dig @162.159.25.175 certifiedhacker.com A +recuse -Parrot Terminal
attacker@parrot: ~%
```

```
dig @162.159.25.175 certifiedhacker.com A +recuse

;;> QD=1, RD=1, RA=1, Z=0, NXRRSIG=0, NSEC3=0, NSEC3PARAM=0, CNAME=0
;;> OPT PSEUDOSECTION
;;> EDNS version 0, flags: rd 1282
;;> QUESTION SECTION:
certifiedhacker.com. IN A

;; ANSWER SECTION:
certifiedhacker.com. 14400 IN A 162.243.236.11

Query time: 18 msec
SERVER: 162.159.25.175#53(162.159.25.175) (UDP)
AREN: Tue May 12 02:36:28 EDT 2024
MSG: 532B, DLEN: 64
```

A high TTL value indicates that the record was not in the cache

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

```
ubuntu@ubuntu-Virtual-Machine: ~ $ ldns-walk @8.8.8.8 nlnetlabs.nl
nlnetlabs.nl. nlnetlabs.nl. A NS SOA MX TXT AAAA NAPTR RRSIG NSEC DNSKEY
l.nlnetlabs.nl. TXT RRSIG NSEC
mail.onion.nlnetlabs.nl. AAAA RRSIG NSEC
acme-challenge.nlnetlabs.nl. CNAME RRSIG NSEC
j.1.1._dane.nlnetlabs.nl. RRSIG NSEC TLSA
j.1.1._dane-gs.nlnetlabs.nl. RRSIG NSEC TLSA
_dmarc.nlnetlabs.nl. TXT RRSIG NSEC
bela._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
default._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
google._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
rbo0001._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
rbo0002._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
rbo0003._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
rbo0004._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
soverin._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
github-challenge-nlnetlabs.nl.netlabs.nl. TXT RRSIG NSEC
77fa5113ab6a532ce2e6901f3bd3351c0db5845e0b1b5fb09907888d._openpgpkey.nlnetlabs.
nl. CNAME RRSIG NSEC
9fe0ccb9e933ad0b8b4fa94066474e091ee8be696c224b1c1678fcce._openpgpkey.nlnetlabs.
nl. RRSIG NSEC OPENPGPKEY
77fa5113ab6a532ce2e6901f3bd3351c0db5845e0b1b5fb09907888d._otrfpingerprint.nlnet
abs.nl. TXT RRSIG NSEC
0suwy3dfnu=====._otrfp.nlnetlabs.nl. TXT RRSIG NSEC
olaf._pka.nlnetlabs.nl. TXT RRSIG NSEC
williem._pka.nlnetlabs.nl. TXT RRSIG NSEC
25._tcp.nlnetlabs.nl. CNAME RRSIG NSEC
https://www.nlnetlabs.nl
```

Enumerated DNS record file

DNSRecon

```
dnsrecon -d www.certifiedhacker.com -z - Parrot Terminal
[attacker@parrot] ~
$ dnsrecon -d www.certifiedhacker.com -z
[*] std: Performing General Enumeration against: www.certifiedhacker.com...
[*] DNSSEC is not configured for www.certifiedhacker.com
[*] SOA ns1.bluehost.com 162.159.24.88
[*] NS ns1.bluehost.com 162.159.24.88
[*] Bind Version for 162.159.24.88 "2024.2.2"
[*] NS ns2.bluehost.com 162.159.25.175
[*] Bind Version for 162.159.25.175 "2024.2.2"
[*] MX mail.certifiedhacker.com 162.241.216.11
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[*] TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[*] 0 Records Found
[*] Performing NSEC Zone Walk for www.certifiedhacker.com
[*] Getting SOA record for www.certifiedhacker.com
[*] Name Server 162.159.24.88 will be used
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[*] 2 records found
https://www.github.com
```

DNS Enumeration Using OWASP Amass

OWASP Amass is a DNS enumeration tool that allows attackers to map the target network and discover potential attack surfaces

```
File Edit View Search Terminal Help
[!] -[root@parrot -] /home/attacker/amass
# docker run caffix/amass enum -d certifiedhacker.com
certifiedhacker.com (FQDN) --> mx_record --> mail.certifiedhacker.com (FQDN)
certifiedhacker.com (FQDN) --> ns_record --> ns2.bluehost.com (FQDN)
certifiedhacker.com (FQDN) --> ns_record --> ns1.bluehost.com (FQDN)
www.certifiedhacker.com (FQDN) --> cname_record --> certifiedhacker.com (FQDN)
ns2.bluehost.com (FQDN) --> a_record --> 162.159.25.175 (IPAddress)
soc.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
www.itf.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
sftp.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
162.241.216.0/24 (Netblock) --> contains --> 162.241.216.11 (IPAddress)
162.159.25.0/24 (Netblock) --> contains --> 162.159.25.175 (IPAddress)
26337 (ASN) --> managed_by --> OISI - Oso Grande IP Services, LLC (RIROrganization)
26337 (ASN) --> announces --> 162.241.216.0/24 (Netblock)
13335 (ASN) --> managed_by --> CLOUDFLARENET - Cloudflare, Inc. (RIROrganization)
13335 (ASN) --> announces --> 162.159.25.0/24 (Netblock)
mail.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
ns1.bluehost.com (FQDN) --> a_record --> 162.159.24.80 (IPAddress)
zpccontacts.demo.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
www.events.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
```

OWASP Amass commands for DNS Enumeration

- Command to perform a passive enumeration:
`amass enum -passive -d <Target Domain> -src`
- Command to perform an active enumeration through brute-forcing :
`amass enum -active -d <Target Domain> -brute -w /usr/share/wordlists/amass/all.txt`
- Command to track or compare the last two enumeration scans :
`amass track -config /root/amass/config.ini -dir
amass4owasp -d <Target Domain> -last 2`

DNS and DNSSEC Enumeration Using Nmap

DNS Enumeration

Attackers use Nmap for scanning domains and obtaining a **list of subdomains, records, IP addresses**, and other valuable information from the target host

```
nmap --script=broadcast-dns-service-discovery certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help
[+] attackert@parrot:~[ - ]
--> # nmap --script=broadcast-dns-service-discovery certifiedhacker.com
Starting Nmap 7.945VN ( https://nmap.org ) at 2024-03-12 03:07 EDT
Pre-scan script results:
| broadcast-dns-service-discovery:
  224.0.0.251
  |_ 5555/tcp adb
    |_ Address=10.10.1.14 fe80::9bab:4253%3:tid:7473
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.092s latency).
DNS record for 162.241.216.11: box533.bluehost.com
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp   filtered  smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https


```

DNSSEC Enumeration

Attackers enumerate DNSSEC using Nmap **dns-nsec-enum.nse** or **dns-nsec3-enum.nse** scripts to obtain information related to domains and their sub-domains

```
nmap -sU -p 53 --script dns-nsec-enum --script-args dns-nsec-enum.domain=certifiedhacker.com 162.159.25.175
File Edit View Search Terminal Help
[+] attackert@parrot:~/home/attackert[ - ]
--> # nmap -sU -p 53 --script dns-nsec-enum --script-args dns-nsec-enum.domain=certifiedhacker.com 162.159.25.175
Starting Nmap 7.945VN ( https://nmap.org ) at 2024-03-12 03:12 EDT
Nmap scan report for ns2.bluehost.com (162.159.25.175)
Host is up (0.0025s latency).

PORT      STATE SERVICE
53/udp  open  domain
| dns-nsec-enum:
|_ No NSEC records found

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds


```

DNS Enumeration Tools

Knock
<https://github.com>

Raccoon
<https://github.com>

Subfinder
<https://github.com>

Turbolist3r
<https://github.com>

DNS Enumeration with Nmap Using AI

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

- “Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com”

```
[attacker@parrot]:~$ 
[attacker@parrot]:~$ ssgpt --chat enum --shell "Use Nmap to perform DNS enumeration on target domain www.certifiedhacker.com"
nmap -script dns brute --script dns brute domain=certifiedhacker.com -oN ./enumeration_results/dns_brute_certifiedhacker.txt && nmap --script dns-zone-transfer -p 53 certifiedhacker.com -oN ./enumeration_results/dns_zonetransfer_certifiedhacker.txt
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:31 EDT
Pre-scan script results:
| dns-brute:
|_ DNS Brute-force hostnames:
  www.certifiedhacker.com - 162.241.216.11
  mail.certifiedhacker.com - 162.241.216.11
  www.certifiedhacker.com - 162.241.216.11
  blog.certifiedhacker.com - 162.241.216.11
  ftp.certifiedhacker.com - 162.241.216.11
  smtp.certifiedhacker.com - 162.241.216.11
  demo.certifiedhacker.com - 162.241.216.11
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 8.33 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:31 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
```

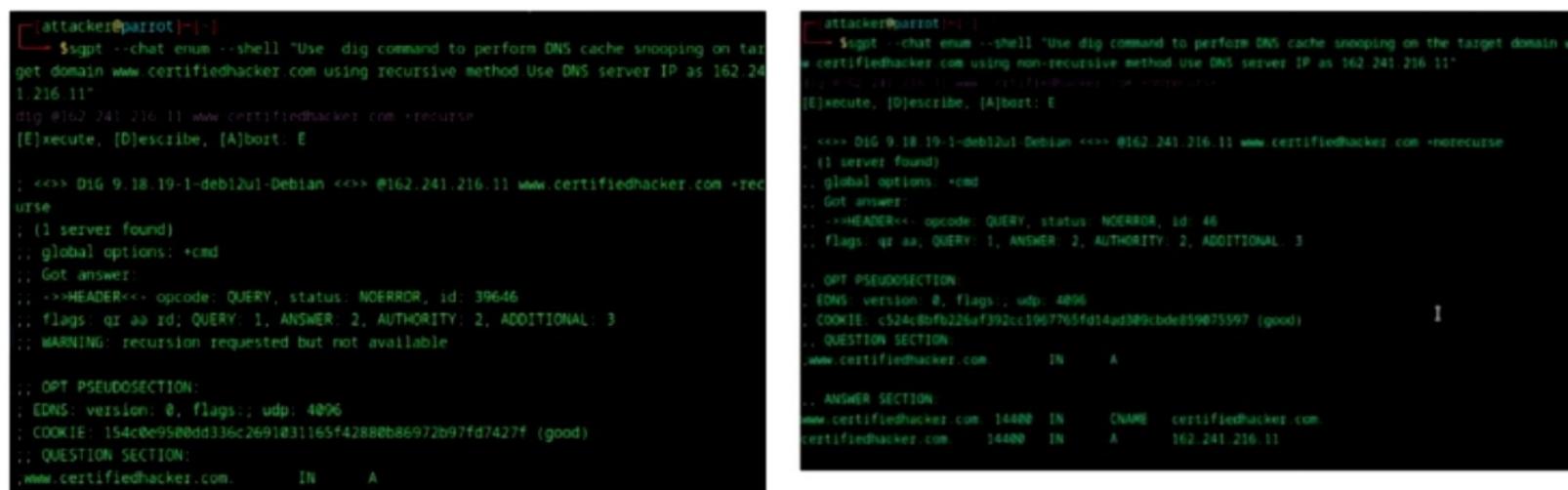
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:31 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.058s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE SERVICE
53/tcp    open  domain
```

DNS Cache Snooping using AI

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

- "Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as <DNS server IP>"*
- "Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method. Use DNS server IP as <DNS server IP>"*



The image shows two terminal windows side-by-side. Both windows have a black background and white text. The left window shows the command being issued: \$sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method Use DNS server IP as 162.241.216.11". The right window shows the output of the command, which includes the dig command itself and its results. The results show a query for www.certifiedhacker.com, an answer section with an A record pointing to 162.241.216.11, and a CNAME record pointing to certifiedhacker.com.

```
[attacker@parrot:~] $sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method Use DNS server IP as 162.241.216.11"
dig @162.241.216.11 www.certifiedhacker.com +recuse
[E]xecute, [D]escribe, [A]bort: E

; <>> DIG 9.18.19-1-deb12u1-Debian <>> @162.241.216.11 www.certifiedhacker.com +recuse
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 39646
; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
; WARNING: recursion requested but not available

; OPT PSEUDOSECTION
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c524c8fb226af392cc1967765fd14ad389cbde859875597 (good)
; QUESTION SECTION:
www.certifiedhacker.com. IN A

; ANSWER SECTION:
www.certifiedhacker.com. 14400 IN CNAME certifiedhacker.com
certifiedhacker.com. 14400 IN A 162.241.216.11

[attacker@parrot:~] $sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method Use DNS server IP as 162.241.216.11"
dig @162.241.216.11 www.certifiedhacker.com +noexecuse
[E]xecute, [D]escribe, [A]bort: E

; <>> DIG 9.18.19-1-deb12u1-Debian <>> @162.241.216.11 www.certifiedhacker.com +noexecuse
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 46
; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3
; OPT PSEUDOSECTION
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c524c8fb226af392cc1967765fd14ad389cbde859875597 (good)
; QUESTION SECTION:
www.certifiedhacker.com. IN A

; ANSWER SECTION:
www.certifiedhacker.com. 14400 IN CNAME certifiedhacker.com
certifiedhacker.com. 14400 IN A 162.241.216.11
```

Objective **06**

Demonstrate IPsec, VoIP, RPC, Unix/Linux, and SMB Enumeration

IPsec Enumeration

Most IPsec based **VPNs use ISAKMP**, a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment

A simple **scanning for ISAKMP at UDP port 500** can indicate the presence of a VPN gateway

Attackers can probe further using a tool, such as **ike-scan**, to enumerate sensitive information, including encryption and hashing algorithm, authentication type, key distribution algorithm, and SA LifeDuration

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as "**Perform IPsec enumeration on target IP 10.10.1.22 with nmap**"

The image displays three terminal windows from a Parrot OS environment, each showing the output of different network scanning tools:

- Top Terminal:** Shows the output of the **nmap -sU -p 500** command. It identifies port 500 as open/filtered and associated with the service isakmp.
- Middle Terminal:** Shows the output of the **#ike-scan -M** command. It performs an IKE scan and finds a Notify message 14 (NO-PROPOSAL-CHosen) with HDR=(CKY-R=f161f1d5ea32a456).
- Bottom Terminal:** Shows the output of the **#sgpt --shell** command, which performs IPsec enumeration on the target IP 10.10.1.22 using nmap. It lists the MAC Address of the target host as 00:15:5D:01:00:02 (Microsoft).

VoIP Enumeration

```
svmap 151.50.106.225 - Parrot Terminal
File Edit View Search Terminal Help
$svmap 151.50.106.225
+-----+
| SIP Device | User Agent |
+-----+
| 151.50.106.225:5060 | DLink VoIP Stack |
+-----+
```

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] (Jobs: 0 Agents: 0) >> use auxiliary/scanner/sip/enum
[*] (Jobs: 0 Agents: 0) auxiliary(scanner/sip/enum) >> use auxiliary/scanner/sip/options
[*] (Jobs: 0 Agents: 0) auxiliary(scanner/sip/options) >> set RHOSTS 192.168.0.1/24
[*] RHOSTS => 192.168.0.1/24
[*] (Jobs: 0 Agents: 0) auxiliary(scanner/sip/options) >> run
[*] Sending SIP UDP OPTIONS requests to 192.168.0.0->192.168.0.255 (256 hosts)
[*] 192.168.0.54:5060 udp SIP/2.0 200 OK {"User-Agent":>"Grandstream GXP1620 1.0.2.27", "Allow":>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.87:5060 udp SIP/2.0 200 OK {"User-Agent":>"Grandstream GXP1620 1.0.2.27", "Allow":>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.109:5060 udp SIP/2.0 200 OK {"User-Agent":>"Grandstream GXP1620 1.0.2.27", "Allow":>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.113:5060 udp SIP/2.0 200 OK {"User-Agent":>"Grandstream GXP1620 1.0.2.27", "Allow":>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] 192.168.0.167:5060 udp SIP/2.0 200 OK {"User-Agent":>"Grandstream GXP1620 1.0.2.27", "Allow":>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE"}
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

VoIP uses **Session Initiation Protocol (SIP)** protocol to enable voice and video calls over an IP network

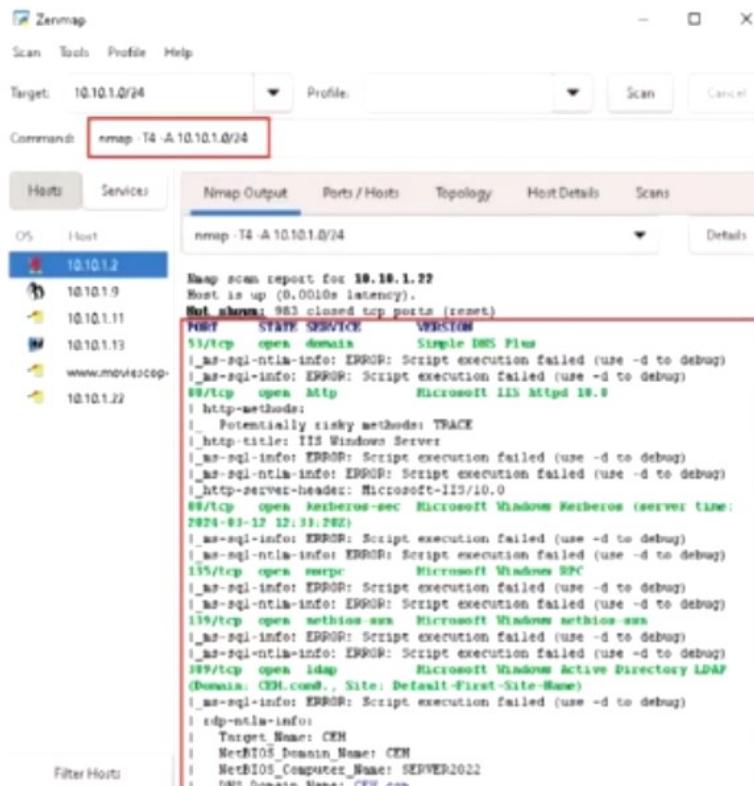
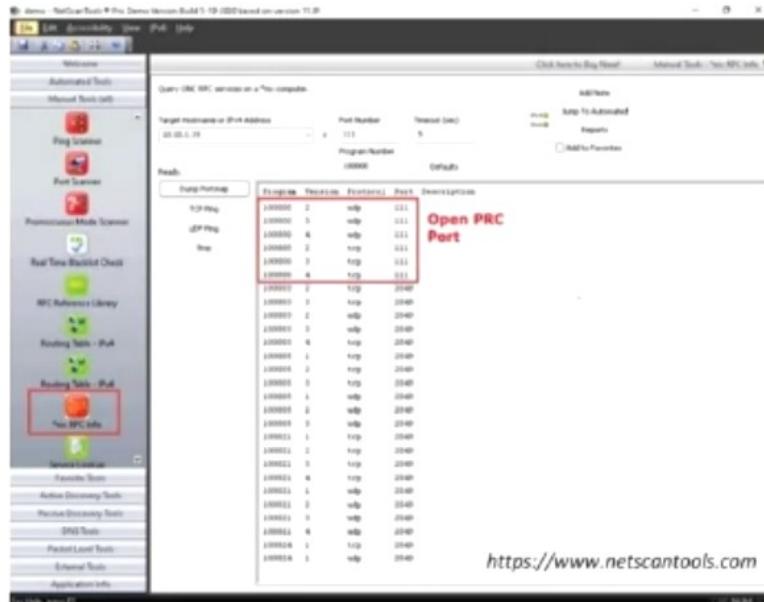
SIP service generally uses UDP/TCP ports 2000, 2001, 5060, and 5061

VoIP enumeration provides sensitive information, such as VoIP gateway/servers, IP-PBX systems, client software (softphones)/VoIP phones, User-agent IP addresses, and user extensions

This information can be used to launch various VoIP attacks, such as Denial-of-Service (DoS), Session Hijacking, Caller ID spoofing, Eavesdropping, Spamming over Internet Telephony (SPIT), and VoIP phishing (Vishing)

RPC Enumeration

- Remote Procedure Call (RPC) allows clients and servers to communicate in **distributed client/server programs**
- Enumerating RPC endpoints enables attackers to **identify any vulnerable services** on these service ports



Unix/Linux User Enumeration

rusers

Displays a list of users who are logged on to remote machines or machines on local network

Syntax: /usr/bin/rusers [-a] [-l] [-u] [-h] [-i] [Host ...]

rwho

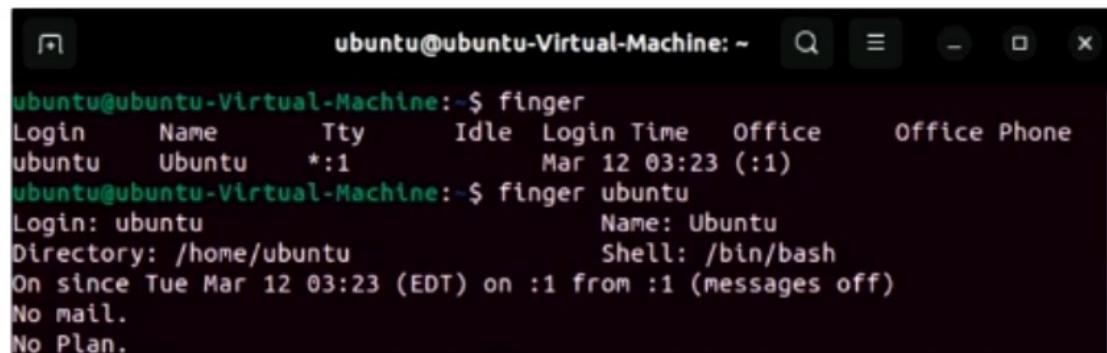
Displays a list of users who are logged on to hosts on the local network

Syntax: rwho [-a]

finger

Displays information about system users, such as login name, real name, terminal name, idle time, login time, office location, and office phone numbers

Syntax: finger [-l] [-m] [-p] [-s] [user ...] [user@host ...]



The screenshot shows a terminal window titled "ubuntu@ubuntu-Virtual-Machine:~". The user has run the "finger" command twice. The first run shows a header and a single entry for the user "ubuntu". The second run shows detailed information for the user "ubuntu", including their login name, real name, directory, shell, and a message indicating they have been on since March 12, 2023, at 03:23 EDT.

```
ubuntu@ubuntu-Virtual-Machine:~$ finger
Login      Name      Tty      Idle  Login Time   Office      Office Phone
ubuntu    Ubuntu      *:1              Mar 12 03:23 (:1)
ubuntu@ubuntu-Virtual-Machine:~$ finger ubuntu
Login: ubuntu                           Name: Ubuntu
Directory: /home/ubuntu                 Shell: /bin/bash
On since Tue Mar 12 03:23 (EDT) on :1 from :1 (messages off)
No mail.
No Plan.
```

SMB Enumeration

- Attackers use SMB enumeration tools, such as **Nmap**, **SMBMap**, **enum4linux**, and **nullinux**, to perform a directed scan on the SMB service running on port 445
- SMB enumeration helps attackers to perform **OS banner grabbing** on the target

```

nmap -p 445 -A 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 09:15 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00075s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds
MAC Address: 02:15:50:64:A2:27 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2019
OS details: Microsoft Windows Server 2019
Network Distance: 1 hop

Host script results:
  smb2-security-mode:
    3.1.1
    - Message signing enabled but not required
  _clock-skew: -1s
  _restat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC: 02:15:50:64:a2:27 (unknown)
  _smb2-time:
    date: 2024-03-15T13:15:26
    start_date: N/A

NMAPROUTE

```

SMB details

SMB Enumeration with AI

- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as
"Scan the target IP 10.10.1.22 for the port using SMB with nmap"

```

attacker@parrot:~$ 
attacker@parrot:~$ !sgpt --shell "Scan the target IP 10.10.1.22 for the port using SMB with nmap"
nmap -p 445 -A 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 01:50 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00005s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
  smb-enum-shares:
    note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
    account_used: <blank>
    \\\10.10.1.22\ADMIN$:
      warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
      Anonymous access: <none>
    \\\10.10.1.22\C$:
      warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
      Anonymous access: <none>
    \\\10.10.1.22\IPC$:
      warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
      Anonymous access: READ
    \\\10.10.1.22\NETLOGON

```

Create and Run Custom Script to Automate Network Enumeration Tasks with AI

- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to automate various network enumeration tasks by create custom script that will run automatically and fetch the desired result. They can use appropriate prompts to create custom scripts, such as the one below:
 - "Develop and execute a script which will automate network enumeration tasks on target IP range 10.10.1.0/24"*

```
[-] (attacker@parrot)[-]
→ $sgpt --chat enum --shell " develop and execute a script which will automate
network enumeration tasks on target IP range 10.10.1.0/24"
#!/bin/bash
$target_range='10.10.1.0/24'

# Update system and install necessary tools
sudo apt-get update && sudo apt-get install -y nmap

# Create a directory for the enumeration outputs
mkdir -p ~/enumeration_results

# Perform a ping sweep to find live hosts
nmap -sn $target_range -oN ~/enumeration_results/ping_sweep.txt
I

# Perform a quick scan on discovered hosts
nmap -T4 -F $target_range -oN ~/enumeration_results/quick_scan.txt

# Perform a detailed scan on discovered hosts
```

```
# Perform a detailed scan on discovered hosts
nmap -T4 -A $target_range -oN ~/enumeration_results/detailed_scan.txt

# Perform a version detection scan on discovered hosts
nmap -sV $target_range -oN ~/enumeration_results/version_detection.txt

# Execute the script
chmod +x network_enumeration.sh && ./network_enumeration.sh

[E]xecute, [D]escribe, [A]bort: E
[sudo] password for attacker:
Get:1 https://deb.parrot.sh/parrot lory InRelease [29.8 kB]
Get:2 https://deb.parrot.sh/direct/parrot lory-security InRelease [29.4 kB]
Get:3 https://deb.parrot.sh/parrot lory-backports InRelease [29.6 kB]
Get:4 https://deb.parrot.sh/parrot lory/contrib Sources [76.8 kB]
Get:5 https://deb.parrot.sh/parrot lory/main Sources [15.6 MB]
Get:6 https://deb.parrot.sh/parrot lory/main Free Sources [126 kB]
```

Create and Run Custom Script to Automate Network Enumeration Tasks with AI (Cont'd)

```
_Not valid after: 2024-09-13T08:50:47
rdp-ntlm-info:
  Target_Name: WINDOWS11
  NetBIOS_Domain_Name: WINDOWS11
  NetBIOS_Computer_Name: WINDOWS11
  DNS_Domain_Name: Windows11
  DNS_Computer_Name: Windows11
  Product_Version: 10.0.22000
  System_Time: 2024-03-15T07:57:56+00:00
  _ssl-date: 2024-03-15T07:58:38+00:00; 0s from scanner time.
  service Info: Host: WINDOWS11; OS: Windows; CPE: cpe:/o:microsoft:windows

  lost script results:
  _clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
  smb-security-mode:
    account_used: guest           I
    authentication_level: user
    challenge_response: supported
  _ message_signing: disabled (dangerous, but default)
  smb-os-discovery:
    OS: Windows 10 Enterprise 22000 (Windows 10 Enterprise 6.3)
    OS CPE: cpe:/o:microsoft:windows_10::-
    Computer_name: Windows11
```

```
_http-title: goodshopping
  http-methods:
    _ Potentially risky methods: TRACE
  135/tcp open msrpc Microsoft Windows RPC
  139/tcp open netbios-ssn Microsoft Windows netbios-ssn
  445/tcp open microsoft-ds?
  1801/tcp open msmq?
  2103/tcp open msrpc Microsoft Windows RPC
  2105/tcp open msrpc Microsoft Windows RPC
  2107/tcp open msrpc Microsoft Windows RPC
  3389/tcp open ms-wbt-server Microsoft Terminal Services
  _ssl-date: 2024-03-15T07:58:38+00:00; 0s from scanner time.
  _ssl-cert: Subject: commonName=Server2019
  Not valid before: 2024-03-14T07:50:45
  Not valid after: 2024-09-13T07:50:45
  rdp-ntlm-info:
    Target_Name: SERVER2019
    NetBIOS_Domain_Name: SERVER2019
    NetBIOS_Computer_Name: SERVER2019
    DNS_Domain_Name: Server2019
    DNS_Computer_Name: Server2019
    Product_Version: 10.0.17763
    System_Time: 2024-03-15T07:57:56+00:00
```

Create and Run Custom Script to Automate Network Enumeration Tasks with AI (Cont'd)

```
host script results:  
_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s  
smb-security-mode:  
 account_used: guest  
 authentication_level: user  
 challenge_response: supported  
 message_signing: disabled (dangerous, but def  
_smb-os-discovery:  
 OS: Windows 10 Enterprise 22000 (Windows 10 E  
 OS CPE: cpe:/o:microsoft:windows_10::  
 Computer name: Windows11  
 NetBIOS computer name: WINDOWS11\x00  
 Workgroup: WORKGROUP\x00  
 System time: 2024-03-15T00:57:58-07:00  
smb2-security-mode:  
 3:1:1:  
 _ Message signing enabled but not required  
_nbstat: NetBIOS name: WINDOWS11, NetBIOS user:  
01:00:00 (Microsoft)  
smb2-time:
```

```
smb2-time:  
 date: 2024-03-15T07:57:57  
 start_date: N/A  
clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s  
nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d  
1:00:02 (Microsoft)  
smb-os-discovery:  
 OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)  
 Computer name: Server2022  
 NetBIOS computer name: SERVER2022\x00  
 Domain name: CEH.com  
 Forest name: CEH.com  
 FQDN: Server2022.CEH.com  
 System time: 2024-03-15T00:57:57-07:00
```

```
host script results:  
smb-enum-users:  
 CEH\Guest (RID: 501)  
 Description: Built-in account for guest access to the computer/domain  
 Flags: Password does not expire, Account disabled, Normal user account  
 Password not required  
 CEH\Martin (RID: 1104)  
 Full name: Martin J.  
 Flags: Password does not expire, Normal user account  
 CEH\Shiela (RID: 1105)  
 Full name: Shiela D.  
 Flags: Password does not expire, Normal user account
```

Objective **07**

Explain Enumeration Countermeasures

Enumeration Countermeasures

SNMP

- Remove the **SNMP agent** or turn off the SNMP service
- If turning 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**"

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 **NT LAN Manager (NTLM)**, **Kerberos**, or any basic authentication mechanism to limit access to legitimate users

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 the requests** to access the system files on the NFS server

Enumeration Countermeasures (Cont'd)

SMTP

Configure SMTP servers to

- 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
- Provide **limited information** in error messages

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**

DNS

- Ensure that the resolver can be accessed only by the hosts **inside the network**
- Ensure that the request packets exiting the network use **random ports**
- Audit **DNS zones** to identify vulnerabilities in domains and subdomains
- Update and **patch nameservers** with the most recent versions of software

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, AD, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, and SMB 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