

## UNIT - II

### **UNIT - II: Gathering Network and Host Information**

CEH Scanning Methodology, Ping Sweep Techniques, nmap Command Switches, Enumeration, Covering Your Tracks and Erasing Evidence.

Scanning is the process of locating systems that are alive and responding on the network. Ethical hackers use scanning to identify target systems' IP addresses. Scanning is also used to determine whether a system is on the network and available. Scanning tools are used to gather information about a system such as IP addresses, the operating system, and services running on the target computer.

Table 3.1 lists the three types of scanning.

**TABLE 3.1** Types of scanning

Scanning type	Purpose
Port scanning	Determines open ports and services
Network scanning	Identifies IP addresses on a given network or subnet
Vulnerability scanning	Discovers presence of known weaknesses on target systems

**Port Scanning** Port scanning is the process of identifying open and available TCP/IP ports on a system. Port-scanning tools enable a hacker to learn about the services available on a given system. Each service or application on a machine is associated with a *well-known* port number. Port Numbers are divided into three ranges:

Well-Known Ports: 0-1023

Registered Ports: 1024-49151

Dynamic Ports: 49152-65535

For example, a port-scanning tool that identifies port 80 as open indicates a web server is running on that system. Hackers need to be familiar with well-known port numbers.

### Common port Numbers

On Windows systems, well-known port numbers are located in the C:\windows\system32\drivers\etc\services file. Services is a hidden file. To view it, show hidden files in Windows Explorer, and double-click the filename to open it with Notepad. The CEH exam expects you to know the well-known port numbers for common applications; familiarize yourself with the port numbers for the following applications:

FTP, 21

Telnet, 23

HTTP, 80

SMTP, 25

POP3, 110

HTTPS, 443

The following list contains additional port numbers not necessarily on the CEH exam but useful for real-world penetration testing:

Global Catalog Server (TCP), 3269 and 3268

LDAP Server (TCP/UDP), 389

LDAP SSL (TCP/UDP), 636

IPsec ISAKMP (UDP), 500

NAT-T (UDP), 4500

RPC (TCP), 135

ASP.NET Session State (TCP), 42424

NetBIOS Datagram Service (UDP), 137 and 138

NetBIOS Session Service (TCP), 139

DHCP Server (UDP), 67

LDAP Server (TCP/UDP), 389

SMB (TCP), 445

RPC (TCP), 135

DNS (TCP/UDP), 53

IMAP (TCP), 143

IMAP over SSL (TCP), 993

POP3 (TCP), 110

POP3 over SSL (TCP), 995

RPC (TCP), 135

RPC over HTTPS (TCP), 443 or 80

SMTP (TCP/UDP), 25

**Network Scanning** Network scanning is a procedure for identifying active hosts on a network, either to attack them or as a network security assessment. Hosts are identified by their individual IP addresses. Network-scanning tools attempt to identify all the *live*

or responding hosts on the network and their corresponding IP addresses.

**Vulnerability Scanning** Vulnerability scanning is the process of proactively identifying the vulnerabilities of computer systems on a network. Generally, a vulnerability scanner first identifies the operating system and version number, including service packs that may be installed. Then, the scanner identifies weaknesses or vulnerabilities in the operating system. During the later attack phase, a hacker can exploit those weaknesses in order to gain access to the system.

Although scanning can quickly identify which hosts are listening and active on a network, it is also a quick way to be identified by an intrusion detection system (IDS). Scanning tools probe TCP/IP ports looking for open ports and IP addresses, and these probes can be recognized by most security intrusion detection tools. Network and vulnerability scanning can usually be detected as well, because the scanner must interact with the target system over the network.

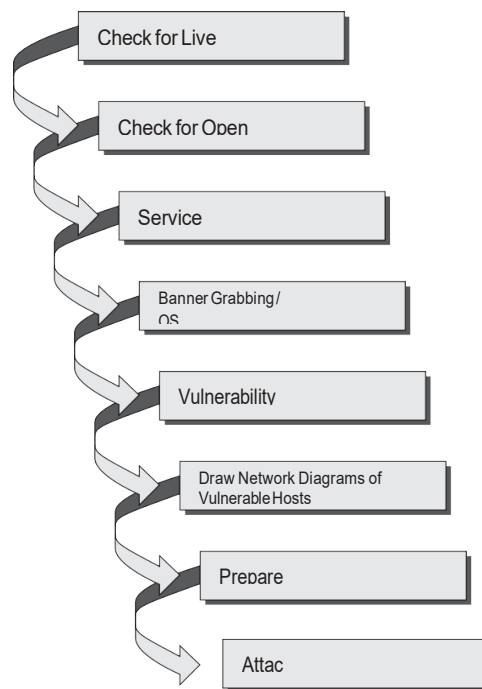
Depending on the type of scanning application and the speed of the scan, an IDS will detect the scanning and flag it as an IDS event. Some of the tools for scanning have different modes to attempt to defeat an IDS and are more likely to be able to scan undetected. As a CEH it is your job to gather as much information as possible and try and remain undetected.

## The CEH Scanning Methodology

As a CEH, you're expected to be familiar with the scanning methodology presented in Figure 3.1. This methodology is the process by which a hacker scans the network. It ensures that no system or vulnerability is overlooked and that the hacker gathers all necessary information to perform an attack.

We'll look at the various stages of this scanning methodology, starting with the first three steps checking for systems that are live and for open ports and service identification in the following section.

**Figure 3.1** CEH scanning methodology



## Ping Sweep Techniques

The CEH scanning methodology starts with checking for systems that are live on the network, meaning that they respond to probes or connection requests. The simplest, although not necessarily the most accurate, way to determine whether systems are live is to perform a *ping sweep* of the IP address range. All systems that respond with a ping reply are considered live on the network. A ping sweep is also known as Internet Control Message Protocol (ICMP) scanning, as ICMP is the protocol used by the ping command.

ICMP scanning, or a ping sweep, is the process of sending an ICMP request or ping to all hosts on the network to determine which ones are up and responding to pings. ICMP began as a protocol used to send test and error messages between hosts on the Internet. It has evolved as a protocol utilized by every operating system, router, switch or Internet Protocol (IP)-based device. The ability to use the ICMP Echo request and Echo reply as a connectivity test between hosts is built into every IP enabled device via the ping command. It is a quick and dirty test to see if two hosts have connectivity and is used extensively for troubleshooting.

A benefit of ICMP scanning is that it can be run in *parallel*, meaning all systems are scanned at the same time; thus it can run quickly on an entire network. Most hacking tools include a ping sweep option, which essentially means performing an ICMP request to every

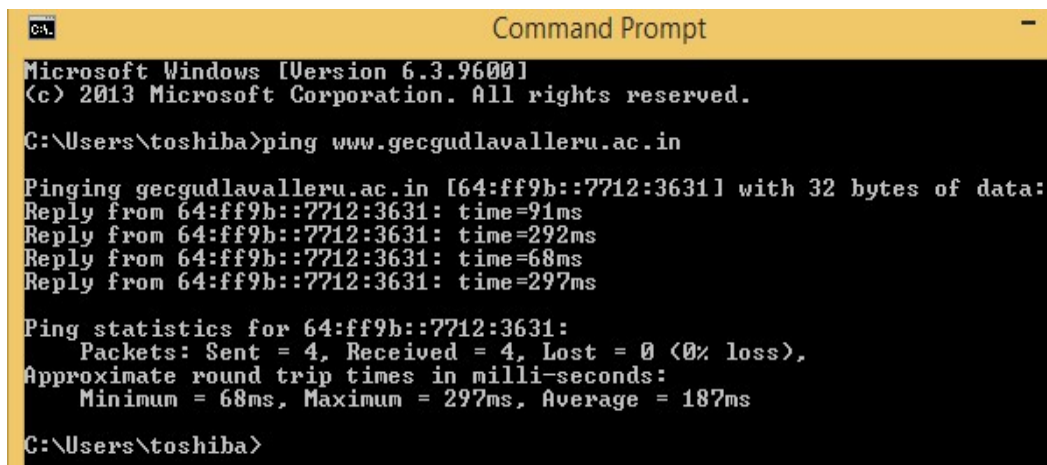
host on the network. Systems that respond with a ping response are alive and listening on the network.

One considerable problem with this method is that personal firewall software and network-based firewalls can block a system from responding to ping sweeps. More and more systems are configured with firewall software and will block the ping attempt and notify the user that a scanning program is running on the network. Another problem is that the computer must be on to be scanned.

## Using a Windows ping

To use the built-in ping command in Windows to test connectivity to another system:

1. Open a command prompt in Windows.
2. Type **ping www.microsoft.com**.



```
C:\> Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\toshiba>ping www.gecgudlavalley.ac.in

Pinging gecgudlavalley.ac.in [64:ff9b::7712:3631] with 32 bytes of data:
Reply from 64:ff9b::7712:3631: time=91ms
Reply from 64:ff9b::7712:3631: time=292ms
Reply from 64:ff9b::7712:3631: time=68ms
Reply from 64:ff9b::7712:3631: time=297ms

Ping statistics for 64:ff9b::7712:3631:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 68ms, Maximum = 297ms, Average = 187ms

C:\Users\toshiba>
```



A timeout indicates that the remote system is not responding or turned off or that the ping was blocked. A reply indicates that the system is alive and responding to ICMP requests.

### **Detecting Ping Sweeps**

Almost any IDS or Intrusion Prevention System (IPS) system will detect and alert the security administrator to a ping sweep occurring on the network. Most firewall and proxy servers block ping responses so a hacker can't accurately determine whether systems are available using a ping sweep alone. More intense port scanning must be used if systems don't respond to a ping sweep. Just because a ping sweep doesn't return any active hosts on the network doesn't mean they aren't available—you need to try an alternate method of identification.

Remember, hacking takes time, patience, and persistence.

### **Scanning Ports and Identifying Services**

Checking for open ports is the second step in the CEH scanning methodology. *Port scanning* is the method used to check for open ports. The process of port scanning involves probing each port on a host to determine which ports are open. Port scanning generally yields more valuable information than a ping sweep about the host and vulnerabilities on the system.

Service identification is the third step in the CEH scanning methodology; it's usually performed using the same tools as port scanning. By identifying open ports, a hacker can

usually also identify the services associated with that port number.

### **Port-Scan Countermeasures**

Countermeasures are processes or tool sets used by security administrators to detect and possibly thwart port scanning of hosts on their network. The following list of countermeasures should be implemented to prevent a hacker from acquiring information during a port scan:

Proper security architecture, such as implementation of IDS and firewalls, should be followed.

Ethical hackers use their toolset to test the scanning countermeasures that have been implemented. Once a firewall is in place, a port-scanning tool should be run against hosts on the network to determine whether the firewall correctly detects and stops the port-scanning activity.

The firewall should be able to detect the probes sent by port-scanning tools. The fire wall should carry out *stateful inspections*, which means it examines the data of the packet and not just the TCP header to determine whether the traffic is allowed to pass through the firewall.

Network IDS should be used to identify the OS detection method used by some common hackers tools.

Only needed ports should be kept open. The rest should be filtered or blocked.

The staff of the organization using the systems should be given appropriate training on security awareness. They

should also know the various security policies they're required to follow.

### ***nmap* Command Switches**

Nmap is a free, open source tool that quickly and efficiently performs ping sweeps, port scanning, service identification, IP address detection, and operating system detection.

Nmap has the benefit of scanning a large number of machines in a single session. It's supported by many operating systems, including Unix, Windows, and Linux.

The state of the port as determined by an nmap scan can be open, filtered, or unfiltered. *Open* means that the target machine accepts incoming request on that port. *Filtered* means a firewall or network filter is screening the port and preventing nmap from discovering whether it's open. *Unfiltered* mean the port is determined to be closed, and no firewall or filter is interfering with the nmap requests.

Nmap supports several types of scans. Table 3.2 details some of the common scan methods.

**Table 3.2** Nmap scan types

Nmap scan type	Description
TCP connect	The attacker makes a full TCP connection to the target system. The most reliable scan type but also the most detectable. Open ports reply with a SYN/ACK while closed ports reply with a RST/ACK.

- XMAS tree scan**      The attacker checks for TCP services by sending XMAS-tree packets, which are named as such because all the “lights” are on, meaning the FIN, URG, and PSH flags are set (the meaning of the flags will be discussed later in this chapter). Closed ports reply with a RST flag.
- SYN stealth scan**      This is also known as *half-open scanning*. The hacker sends a SYN packet and receives a SYN-ACK back from the server. It’s stealthy because a full TCP connection isn’t opened. Open ports reply with a SYN/ACK while closed ports reply with a RST/ACK.
- Null scan**      This is an advanced scan that may be able to pass through firewalls undetected or modified. Null scan has all flags off or not set. It only works on Unix systems. Closed ports will return a RST flag.
- Windows scan**      This type of scan is similar to the ACK scan and can also detect open ports.
- ACK scan**      This type of scan is used to map out firewall rules. ACK scan only works on Unix. The port is considered filtered by firewall rules if an ICMP destination unreachable message is received as a result of the ACK scan.

---

The nmap command has numerous switches to perform different types of scans. The common command switches are listed in Table 3.3.

**Table 3 . 3**      Common nmap command switches

<b>nmap command switch    Scan performed</b>	
-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan
-sX	XMAS tree scan
-sN	Null scan
-sP	Ping scan
-sU	UDP scan
-sO	Protocol scan
-sA	ACK scan
-sW	Windows scan
-sR	RPC scan

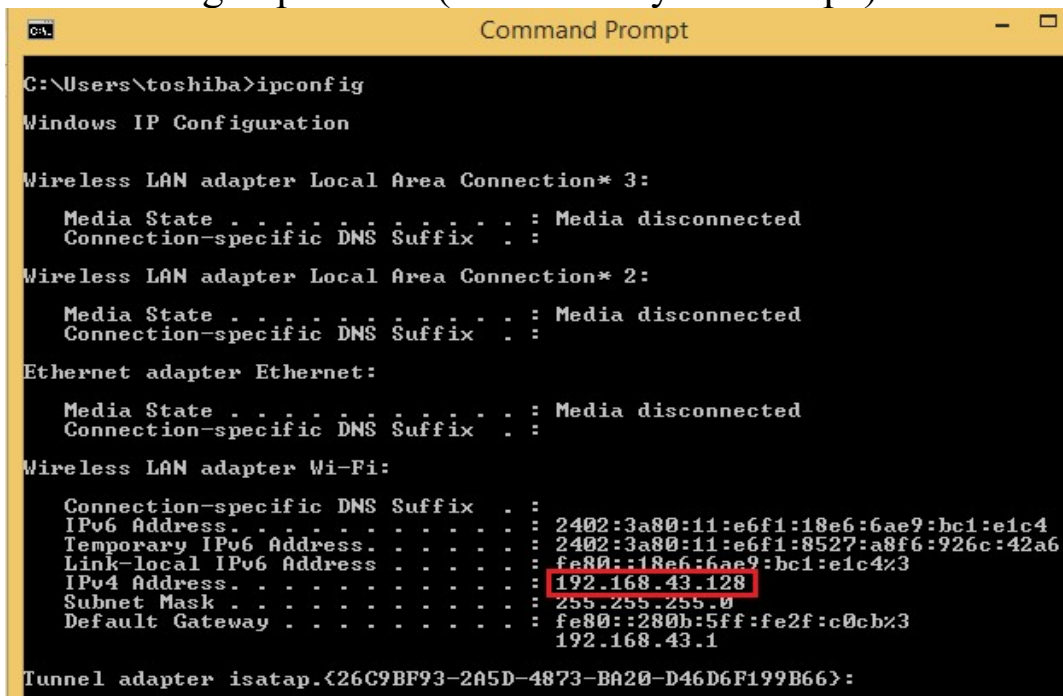
-sL	List/DNS scan
-sI	Idle scan
-Po	Don't ping
-PT	TCP ping
-PS	SYN ping
-PI	ICMP ping
-PB	TCP and ICMP ping
-PB	ICMP timestamp
-PM	ICMP netmask
-oN	Normal output
-oX	XML output
-oG	Grepable output
-oA	All output
-T Paranoid	Serial scan; 300 sec between scans
-T Sneaky	Serial scan; 15 sec between scans
-T Polite	Serial scan; .4 sec between scans

- T Normal          Parallel scan
- T Aggressive      Parallel scan, 300 sec timeout, and 1.25 sec/probe
- T Insane           Parallel scan, 75 sec timeout, and .3 sec/probe

To perform an nmap scan, find download and install nmap from <https://nmap.org/download.html> and then at the Windows command prompt type **Nmap IPaddress** followed by any command switches used to perform specific type of scans. For example, to scan the host with the IP address 192.168.0.1 using a TCP connect scan type, enter this command:

Nmap 192.168.0.1 -sT

Find the target ip address(in this case your own pc)



```
C:\Users\toshiba>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi:

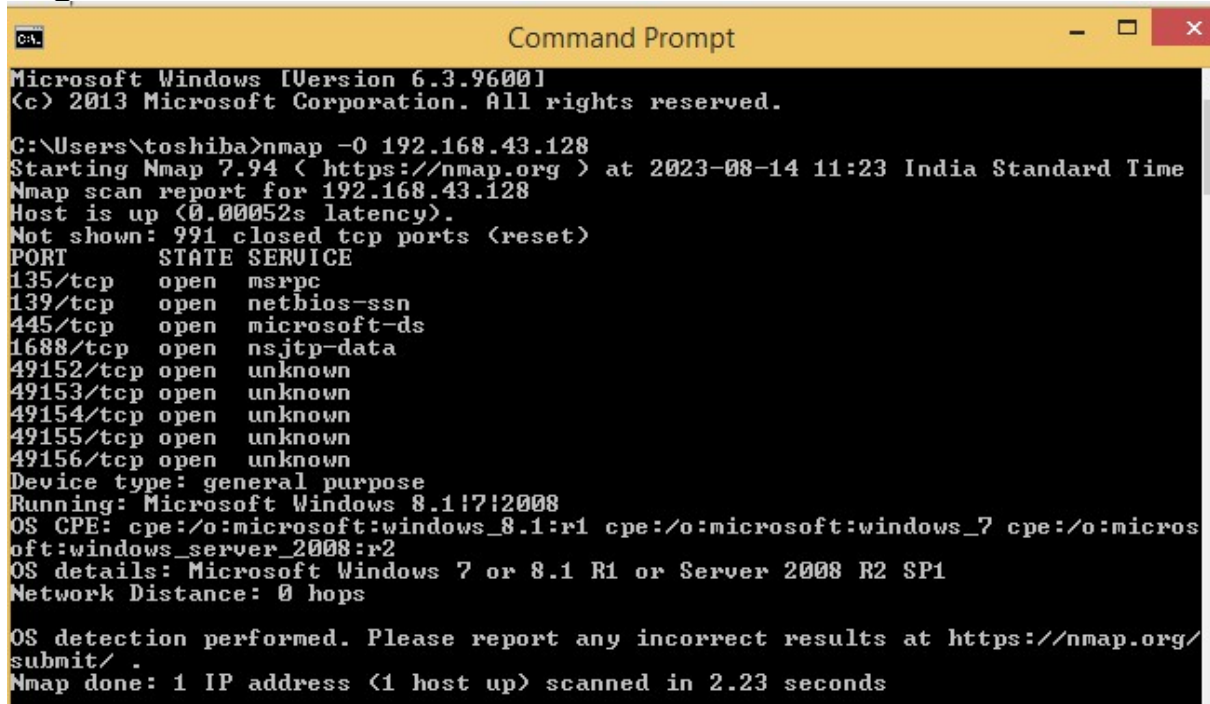
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2402:3a80:11:e6f1:18e6:6ae9:bc1:e1c4
    Temporary IPv6 Address. . . . . : 2402:3a80:11:e6f1:8527:a8f6:926c:42a6
    Link-local IPv6 Address . . . . . : fe80::18e6:6ae9:bc1:e1c4%3
    IPv4 Address. . . . . : 192.168.43.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::280b:5ff:fe2f:c0cb%3
                                192.168.43.1

Tunnel adapter isatap.{26C9BF93-2A5D-4873-BA20-D46D6F199B66}:

```

OS Detection: `nmap -O 192.168.43.128`

This command will try to guess the operating system the target host is running and also all the services that are running in the target.

A screenshot of a Windows Command Prompt window titled "Command Prompt". The window shows the output of the command `nmap -O 192.168.43.128`. The output includes the Nmap version (7.94), the scan time (2023-08-14 11:23 India Standard Time), and a list of open ports with their corresponding services. The OS is detected as Microsoft Windows 8.1. The window has a yellow title bar and standard Windows window controls (minimize, maximize, close).

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\toshiba>nmap -O 192.168.43.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-14 11:23 India Standard Time
Nmap scan report for 192.168.43.128
Host is up (0.00052s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1688/tcp  open  nsjtp-data
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows 8.1!7!2008
OS CPE: cpe:/o:microsoft:windows_8.1:r1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 or 8.1 R1 or Server 2008 R2 SP1
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.23 seconds
```

Get services and version information: `nmap -sV 192.168.43.128`

This is a great command to get version information on services running on the target hosts. For example, it will show what version is running on port 80, 443, and so on).



```
Command Prompt

C:\Users\toshiba>nmap -sU 192.168.43.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-14 11:28 India Standard Time
Nmap scan report for 192.168.43.128
Host is up (0.0012s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1688/tcp  open  msrpc        Microsoft Windows RPC
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: TOSHIBA; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 61.65 seconds
```

Port Scan (find specific open port): `nmap -p 445 192.168.43.128`

This will do a TCP port scan of the most popular 1000 ports. The ports are listed in the nmap services file. If you want to scan specific ports you can use the `-p` option, here is an example of scanning port 445.

```
Command Prompt

C:\Users\toshiba>nmap -p 445 192.168.43.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-14 11:31 India Standard Time
Nmap scan report for 192.168.43.128
Host is up (0.0020s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Find the target server ip address(in this case a website) using  
dnslookup

Merino Consulting Service

Getting The Right Solution Begins With The Right Consulting.

Choose Merino,

Enterprise Application Partner

Contact Us

DNS Server

Recursive Name Server

DNS Server IP or Hostname

8.8.8.8 - Google Public DNS

DNS Record

A (IPv4)

Domain Name or Hostname

www.gecgudlavalлерu.ac.in

☐ Advanced Mode ☐ DNSSEC

DNS Lookup

Answer

Type	Cname/Address	Name
CNAME	gecgudlavalлерu.ac.in	www.gecgudlavalлерu.ac.in
A	119.18.54.49	gecgudlavalлерu.ac.in

OS Detection: nmap -O 119.18.54.49

This command will try to guess the operating system the target host is running and also all the services that are running in the target.

```
Command Prompt

C:\Users\toshiba>nmap -O 119.18.54.49
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-14 11:52 India Standard Time
Nmap scan report for 119.18.54.49
Host is up (0.076s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
26/tcp    open  rsftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
139/tcp   filtered netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   filtered microsoft-ds
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
1720/tcp  filtered h323q931
2222/tcp  open  EtherNetIP-1
2525/tcp  filtered ms-v-worlds
3306/tcp  open  mysql
5060/tcp  filtered sip
Aggressive OS guesses: Linux 4.0 (90%), Linux 5.0 (90%), Linux 3.10 - 3.16 (90%)
, Linux 2.6.32 (88%), Linux 3.5 (88%), Linux 4.2 (88%), Linux 4.4 (88%), Synolog
y DiskStation Manager 5.1 (88%), WatchGuard Firewall 11.8 (88%), Linux 2.6.35 (8
8%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops


OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds
```

Netcraft and HTTrack are tools that fingerprint an operating system. Both are used to determine the OS and web server software version numbers.

Netcraft is a website that periodically polls web servers to determine the operating system version and the web server software version. Netcraft can provide useful information the hacker can use in identifying vulnerabilities in the web server software. In addition, Netcraft has an antiphishing toolbar and web server verification tool you can use to make sure you're using the actual web server rather than a spoofed web server.

← → ↻ https://sitereport.netcraft.com/?url=https://gecgudlavalleru.ac.in 150% ☆

**netcraft** ≡

Site	<a href="https://gecgudlavalleru.ac.in">https://gecgudlavalleru.ac.in</a>	Domain	<a href="https://gecgudlavalleru.ac.in">gecgudlavalleru.ac.in</a>
Netblock Owner	<a href="#">This is the second Websitedns.in IP pool.</a>	Nameserver	cns6001.hostgator.in
Hosting company	Newfold Digital	Domain registrar	registry.in
Hosting country	 IN	Nameserver organisation	whois.registry.in
IPv4 address	119.18.54.49 ( <a href="#">VirusTotal</a> )	Organisation	Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, India
IPv4 autonomous systems	<a href="#">AS394695</a>	DNS admin	root@cs3001.hostgator.in

← → ↻ https://sitereport.netcraft.com/?url=https://gecgudlavalleru.ac.in 150% ☆

**netcraft** ≡

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. [More information about Heartbleed detection.](#)

☒ **SSL Certificate Chain**

☒ **Hosting History**

Netblock owner	IP address	OS	Web server	Last seen
<a href="#">GoDaddy.com, LLC 2155 E GoDaddy Way Tempe AZ US 85284</a>	148.72.201.240	Linux	Apache	16-Dec-2019

**HTTrack(website copier)** arranges the original site's relative link structure. You open a page of the mirrored

website in your browser, and then you can browse the site from link to link as if you were viewing it online.



**Anonymous EMAIL service (sending email without ‘from’ address)**

anonymouse.org/anonemail.html

# Anonymouse.org

## AnonEmail

[AnonEmail](#)
[AnonWWW](#)
[AnonNews](#)

With AnonEmail it is possible to send e-mails without revealing your e-mail address or any information about your identity. Therefore you can communicate more freely and you do not have to worry that it might cause consequences for you.

This service allows you to send e-mails without revealing any personal information.

**Protect your privacy, protect your data, protect it for free.**

**To:** abinayamalar@gmail.com  
**Subject:** Hi students !!  
**Message:** Welcome to anonymousemail service but do use a ~~tor~~ browser for better security.

Send Anonymously

---

« [Back to Spam](#) Delete Forever Not Spam More Actions... Go 1 of hundreds [Older](#)

[Print](#) [New window](#)

**Hi students !!** [Spam](#)

★ [Nomen Nescio](#)<nobody@dizum.com> Mon, Aug 14, 2023 at 12:56 PM

**Why is this message in Spam?** It's similar to messages that were detected by our spam filters. [Learn More](#)

To: abinayamalar@gmail.com

[Reply](#) | [Reply to all](#) | [Forward](#) | [Print](#) | [Delete](#) | [Show original](#)

Welcome to anonymousemail service but do use a torr browser for better security.

## Enumeration

*Enumeration* occurs after scanning and is the process of gathering and compiling user names, machine names, network resources, shares, and services. It also refers to actively querying or connecting to a target system to acquire this information.

Hackers need to be methodical in their approach to hacking. The following steps are an example of those a

hacker might perform in preparation for hacking a target system:

1. Extract usernames using enumeration.
2. Gather information about the host using null sessions.
3. Perform Windows enumeration using the SuperScan tool.
4. Acquire the user accounts using the tool GetAcct.
5. Perform SNMP port scanning.

The object of enumeration is to identify a user account or system account for potential use in hacking the target system. It isn't necessary to find a system administrator account, because most account privileges can be escalated to allow the account more access than was previously granted.

Many hacking tools are designed for scanning IP networks to locate NetBIOS name information. For each responding host, the tools list IP address, NetBIOS computer name, logged-in username, and MAC address information.

On a Windows, net view can be used for NetBIOS enumeration. To enumerate NetBIOS names using the net view command, enter the following at the command prompt:

net view – will list all the computers/hosts connected in that network

```
C:\ Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\toshiba>net view
Server Name          Remark
-----
\\TOSHIBA
The command completed successfully.
```

net user – will list all the user accounts in that network

```
C:\ Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\toshiba>net user
User accounts for \\TOSHIBA
-----
Administrator      Guest              toshiba
The command completed successfully.
```

nbtstat -A [IP address of host] will display all the user accounts

```
C:\ Command Prompt
C:\Users\toshiba>nbtstat -A 192.168.43.128
Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []
Host not found.
Wi-Fi:
Node IpAddress: [192.168.43.128] Scope Id: []
NetBIOS Remote Machine Name Table
-----
Name          Type          Status
-----
TOSHIBA       <00>          UNIQUE       Registered
TOSHIBA       <20>          UNIQUE       Registered
WORKGROUP     <00>          GROUP        Registered
MAC Address = 24-EC-99-C2-EF-26
```

net user – view/add/remove users & change passwords of other users from admin account



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net user
User accounts for \TOSHIBA

Administrator      Guest              toshiba
The command completed successfully.

C:\WINDOWS\system32>net user Abinaya abi /add
The command completed successfully.

C:\WINDOWS\system32>net user
User accounts for \TOSHIBA

Abinaya            Administrator      Guest
toshiba
The command completed successfully.

C:\WINDOWS\system32>net user Abinaya *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.

C:\WINDOWS\system32>net user Abinaya /delete
The command completed successfully.
```

### **Hacking tools**

DumpSec is a NetBIOS enumeration tool. It connects to the target system as a null user with the net use command. It then enumerates users, groups, NTFS permissions, and file ownership information.

Hyena is a tool that enumerates NetBIOS shares and additionally can exploit the null session vulnerability to connect to the target system and change the share path or edit the Registry.

The SMB Auditing Tool is a password auditing tool for the Windows and Server Message Block (SMB) platforms. Windows uses SMB to communicate between the client and server. The SMB Auditing Tool is able to identify user names and crack passwords on Windows systems.

The NetBIOS Auditing Tool is another NetBIOS enumeration tool. It's used to perform various security checks on remote servers running NetBIOS file sharing services.

### **Null Sessions**

A null session occurs when you log in to a system with no username or password. NetBIOS null sessions are a vulnerability found in the Common Internet File System (CIFS) or SMB, depending on the operating system.

Once a hacker has made a NetBIOS connection using a null session to a system, they can easily get a full dump of all usernames, groups, shares, permissions, policies, services, and more using the Null user account. The SMB and NetBIOS standards in Windows include APIs that return information about a system via TCP port 139.

One method of connecting a NetBIOS null session to a Windows system is to use the hidden Inter-Process Communication share (IPC\$). This hidden share is accessible using the net use command. As mentioned earlier, the net use command is a built-in Windows command that connects to a share on another computer. The empty quotation marks ("" ) indicate that you want to connect with no username and no password. To make a NetBIOS null session to a system with the IP address 192.21.7.1 with the built-in anonymous user account and a null password using the net use command, the syntax is as follows:

```
C:\Users\toshiba>net use \\192.168.43.128\IPC$ "" /u:""
```

Once the net use command has been successfully completed, the hacker has a channel over which to use other hacking tools and techniques.

As a CEH, you need to know how to defend against NetBIOS enumeration and null sessions.

## **NetBIOS Enumeration and Null Session Countermeasures**

The NetBIOS null session uses specific port numbers on the target machine. Null sessions require access to TCP ports 135, 137,139, and/or 445. One countermeasure is to close

these ports on the target system. This can be accomplished by disabling SMB services on individual hosts by unbinding the TCP/IP WINS client from the interface in the network connection's properties. To implement this countermeasure, perform the following steps:

1. Open the properties of the network connection.
2. Click TCP/IP and then the Properties button.
3. Click the Advanced button.
4. On the WINS tab, select Disable NetBIOS Over TCP/IP.

A security administrator can also edit the Registry directly to restrict the anonymous user from login. To implement this countermeasure, follow these steps:

1. Open `regedt32` and navigate to `HKLM\SYSTEM\CurrentControlSet\LSA`.
2. Choose Edit ⇌ Add Value. Enter these values:

Value Name: **RestrictAnonymous**

Data Type: **REG\_WORD**

Value: **2**

Finally, the system can be upgraded to Windows XP and the latest Microsoft security patches, which mitigates the NetBIOS null session vulnerability from occurring.

## **SNMP Enumeration**

*SNMP enumeration* is the process of using SNMP to enumerate user accounts on a target system. SNMP employs two major types of software components for communication: the SNMP agent, which is located on the

networking device, and the SNMP management station, which communicates with the agent.

Almost all network infrastructure devices, such as routers and switches and including Windows systems, contain an SNMP agent to manage the system or device. The SNMP management station sends requests to agents, and the agents send back replies. The requests and replies refer to configuration variables accessible by agent software. Management stations can also send requests to set values for certain variables. Traps let the management station know that something significant has happened in the agent software, such as a reboot or an interface failure. Management Information Base (MIB) is the database of configuration variables that resides on the networking device.

SNMP has two passwords you can use to access and configure the SNMP agent from the management station. The first is called a *read community string*. This password lets you view the configuration of the device or system. The second is called the *read/write community string*; it's for changing or editing the configuration on the device. Generally, the default read community string is public and the default read/write community string is private. A common security loophole occurs when the community strings are left at the default settings: a hacker can use these default passwords to view or change the device configuration.

## Hacking tools

SNMPUtil and IP Network Browser are SNMP enumeration tools.

SNMPUtil gathers Windows user account information via SNMP in Windows systems. Some information—such as routing tables, ARP tables, IP addresses, MAC addresses, TCP and UDP open ports, user accounts, and shares—can be read from a Windows system that has SNMP enabled using the SNMPUtil tools.

IP Network Browser from the SolarWinds Toolset also uses SNMP to gather more information about a device that has an SNMP agent.

## **SNMP Enumeration Countermeasures**

The simplest way to prevent SNMP enumeration is to remove the SNMP agent on the potential target systems or turn off the SNMP service. If shutting off SNMP isn't an option, then change the default read and read/write community names.

## **Windows 2000 DNS Zone Transfer**

In a Windows 2000 domain, clients use service (SRV) records to locate Windows 2000 domain services, such as Active Directory and Kerberos. This means every Windows 2000 Active Directory domain must have a DNS server for the network to operate properly.

A simple zone transfer performed with the nslookup command can enumerate lots of interesting network information. The command to enumerate using the nslookup command is as follows:

```
nslookup ls -d domainname
```

```

C:\Users\toshiba>nslookup -type=ns www.gecgudlavalleru.ac.in
Server: UnKnown
Address: 192.168.43.1

Non-authoritative answer:
www.gecgudlavalleru.ac.in      canonical name = gecgudlavalleru.ac.in
gecgudlavalleru.ac.in        nameserver = cns6002.hostgator.in
gecgudlavalleru.ac.in        nameserver = cns6001.hostgator.in

C:\Users\toshiba>nslookup
Default Server: UnKnown
Address: 192.168.43.1

> server cns6001.hostgator.in
Default Server: cns6001.hostgator.in
Addresses: 64:ff9b::7712:362f
           119.18.54.47

> set type=any
> ls -d www.gecgudlavalleru.ac.in
[cns6001.hostgator.in]
*** Can't list domain www.gecgudlavalleru.ac.in: BAD ERROR VALUE
The DNS server refused to transfer the zone www.gecgudlavalleru.ac.in to your co
mputer. If this
is incorrect, check the zone transfer security settings for www.gecgudlavalleru.
ac.in on the DNS
server at IP address 64:ff9b::7712:362f.

```

Within the nslookup results, a hacker looks closely at the following records, because they provide additional information about the network services:

Global Catalog service (\_gc.\_tcp\_)

Domain controllers (\_ldap.\_tcp)

Kerberos authentication (\_kerberos.\_tcp)

As a countermeasure, zone transfers can be blocked in the properties of the Windows DNS server.

An Active Directory database is a Lightweight Directory Access Protocol (LDAP)-based database. This allows the



existing users and groups in the database to be enumerated with a simple LDAP query. The only thing required to perform this enumeration is to create an authenticated session via LDAP. A Windows 2000 LDAP client called the Active Directory Administration Tool (ldp.exe) connects to an Active Directory server and identifies the contents of the database. You can find ldp.exe on the Windows 2000 CD-ROM in the Support\Reskit\Netmgmt\Dstool folder.

To perform an Active Directory enumeration attack, a hacker performs the following steps:

1. Connect to any Active Directory server using ldp.exe on port 389. When the connection is complete, server information is displayed in the right pane.
2. On the Connection menu, choose Authenticate. Type the username, password, and domain name in the appropriate boxes. You can use the Guest account or any other domain account.
3. Once the authentication is successful, enumerate users and built-in groups by choosing the Search option from the Browse menu.

## **Covering Your Tracks and Erasing Evidence**

Once intruders have successfully gained administrator access on a system, they try to cover their tracks to prevent detection of their presence (either current or past) on the system.

A hacker may also try to remove evidence of their identity or activities on the system to prevent tracing of their identity or location by authorities. To prevent detection, the hacker usually erases any error messages or security events that have been logged. Disabling auditing and clearing the event log are two methods used by a hacker to cover their tracks and avoid detection.

The first thing intruders do after gaining administrator privileges is disable auditing. Windows auditing records certain events in a log file that is stored in the Windows Event Viewer. Events can include logging into the system, an application, or an event log. An administrator can choose the level of logging implemented on a system. Hackers want to determine the level of logging implemented to see whether they need to clear events that indicate their presence on the system.

Intruders can easily wipe out the security logs in the Windows Event Viewer. An event log that contains one

#### **Hacking tool**

Auditpol is a tool included in the Windows NT Resource Kit for system administrators. This tool can disable or enable auditing from the Windows command line. It can also be used to determine the level of logging implemented by a system administrator.

or just a few events is suspicious because it usually indicates that other events have been cleared. It's still necessary to clear the event log after disabling auditing,

because using the Auditpol tool places an entry in the event log indicating that auditing has been disabled. Several tools exist to clear the event log, or a hacker can do so manually in the Windows Event Viewer.

### **Hacking tools**

The `elsave.exe` utility is a simple tool for clearing the event log. It's command line based.

WinZapper is a tool that an attacker can use to erase event records selectively from the security log in Windows 2000. WinZapper also ensures that no security events are logged while the program is running.

Evidence Eliminator is a data-cleansing system for Windows PCs. It prevents unwanted data from becoming permanently hidden in the system. It cleans the Recycle Bin, Internet cache, system files, temp folders, and so on. Evidence Eliminator can also be used by a hacker to remove evidence from a system after an attack.