



University of Babylon College of
information Technology
Department of Information Security

Ethical Hacking

Lecture 4:Footprinting and Reconnaissance II and Scanning

Asst.Lect. Rasha Hussein



6- Whois Footprinting : Whois Lookup

- Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, which contain the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information regarding assignees, registrants, and administrative information (creation and expiration dates).

Two types of data models exist to store and lookup Whois information:

- **Thick Whois** - Stores the complete Whois information from all the registrars for a particular set of data.
- **Thin Whois** - Stores only the name of the Whois server of the registrar of a domain, which in turn holds complete details on the data being looked up.

Whois query returns the following information:

- Domain name details
- Contact details of the domain owner
- Domain name servers
- NetRange
- When a domain has been created
- Expiry records
- Records last updated

Whois Example

WHOIS Lookup

Search domain name registration records

Enter Domain Name or IP Address

SEARCH

Examples: qq.com, google.co.in, bbc.co.uk, ebay.ca

SmartWhois - Evaluation Version

File Query Edit View Settings Help

IP, host or domain: Query

certifiedhacker.com

certifiedhacker.com

162.241.216.11

PERFECT PRIVACY, LLC
12808 Gran Bay Parkway West
Jacksonville
FL
32258
United States
Phone: +1.5707088780
wf6j599s4d9@networksolutionsprivateregistration.com

PERFECT PRIVACY, LLC
12808 Gran Bay Parkway West
Jacksonville
FL
32258
United States
Phone: +1.5707088780
wf6j599s4d9@networksolutionsprivateregistration.com

PERFECT PRIVACY, LLC
12808 Gran Bay Parkway West
Jacksonville
FL
32258
United States
Phone: +1.5707088780
wf6j599s4d9@networksolutionsprivateregistration.com

NS1.BLUEHOST.COM
NS2.BLUEHOST.COM

Alexa Traffic Rank: 3 258 426

certifiedhacker.com - Source

```
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-08-22T09:05:36Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date:
2021-07-30T00:32:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 12808 Gran Bay Parkway West
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32258
Registrant Country: US
Registrant Phone: +1.5707088780
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:
wf6j599s4d9@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 12808 Gran Bay Parkway West
Admin City: Jacksonville
```

```
root@kali: ~
File Edit View Search Terminal Help
# available at: https://www.arin.net/whois_tou.html
#
root@kali:~# whois www.google.com
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.
Server Name: WWW.GOOGLE.COM.AR
Registrar: ENOM, INC.
Whois Server: whois.enom.com
Referral URL: http://www.enom.com
Server Name: WWW.GOOGLE.COM.AU
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Whois Server: whois.melbourneit.com
Referral URL: http://www.melbourneit.com
Server Name: WWW.GOOGLE.COM.BR
Registrar: ENOM, INC.
Whois Server: whois.enom.com
```

7- DNS Footprinting

- After collecting Whois records about the target, the next phase in the footprinting methodology is DNS footprinting. Attackers perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used by the target organization. This information helps attackers to identify the hosts connected in the target network and perform further exploitation on the target organization. This section describes how to extract DNS information, perform the reverse DNS lookup, and collect information from DNS zone transfers, as well as DNS interrogation tools. Extracting DNS Information DNS footprinting reveals information about domain names, computer names, IP addresses, and much more information about a network. An attacker uses DNS information to determine key hosts in the network and then performs social engineering attacks to gather even more information.
- DNS footprinting helps in determining the following records about the target DNS:

DNS Interrogation Tools:

1.DNSstuff (Professional Toolset)

2.DNS Records

3.Dig

Dig syntax : **dig <target domain> <record Type>**

Example

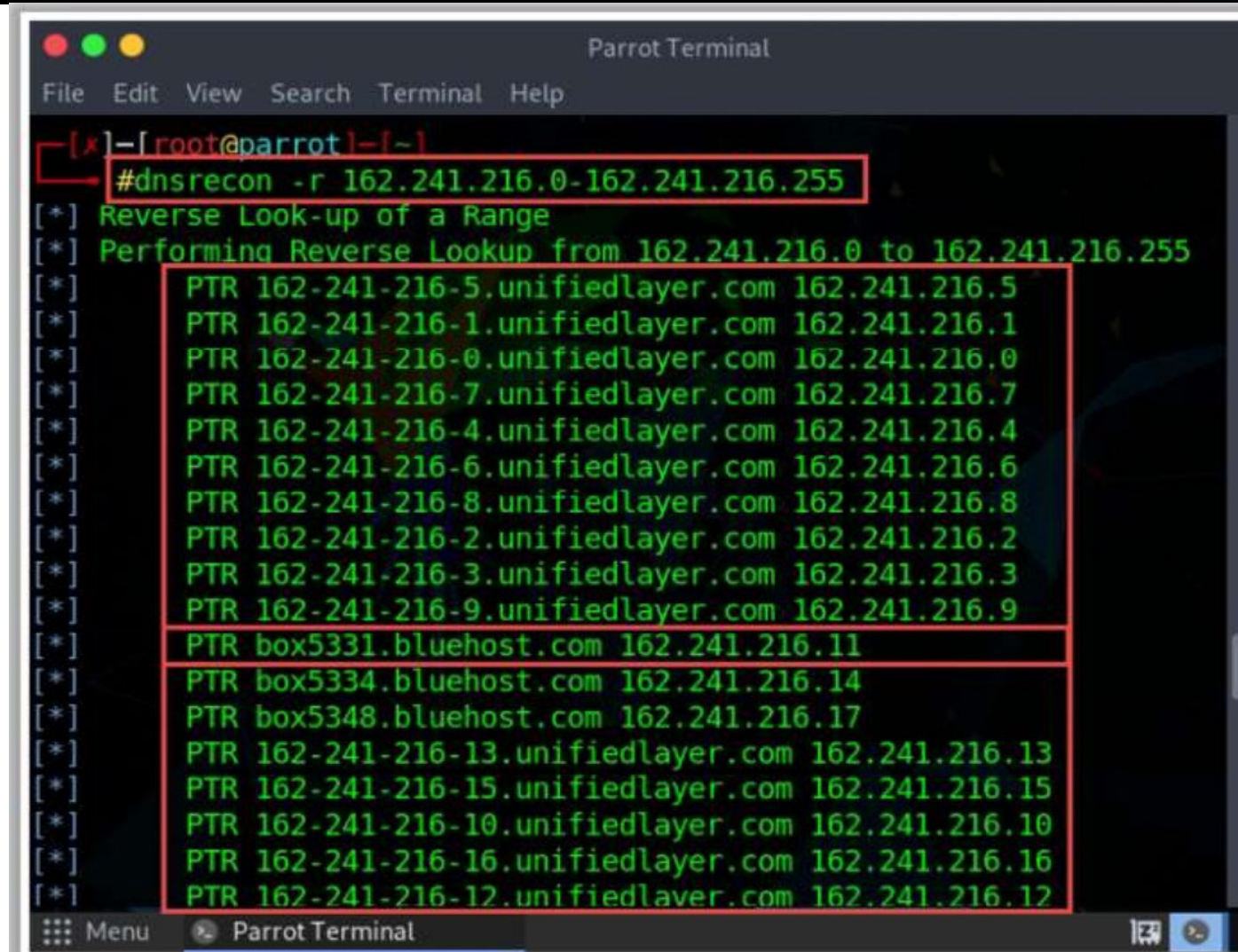
dig google.com any

dig google.com MX

Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for a domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

Reverse DNS Lookup

- Attackers use reverse DNS lookups on IP ranges to find DNS PTR records. Tools like "DNSRecon" help perform reverse lookups on target hosts. Additionally, attackers can identify other domains sharing the same server using tools such as "Reverse IP Domain Check".



```
Parrot Terminal
File Edit View Search Terminal Help
[*] - [root@parrot] - [~]
#dnsrecon -r 162.241.216.0-162.241.216.255
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[*] PTR 162-241-216-5.unifiedlayer.com 162.241.216.5
[*] PTR 162-241-216-1.unifiedlayer.com 162.241.216.1
[*] PTR 162-241-216-0.unifiedlayer.com 162.241.216.0
[*] PTR 162-241-216-7.unifiedlayer.com 162.241.216.7
[*] PTR 162-241-216-4.unifiedlayer.com 162.241.216.4
[*] PTR 162-241-216-6.unifiedlayer.com 162.241.216.6
[*] PTR 162-241-216-8.unifiedlayer.com 162.241.216.8
[*] PTR 162-241-216-2.unifiedlayer.com 162.241.216.2
[*] PTR 162-241-216-3.unifiedlayer.com 162.241.216.3
[*] PTR 162-241-216-9.unifiedlayer.com 162.241.216.9
[*] PTR box5331.bluehost.com 162.241.216.11
[*] PTR box5334.bluehost.com 162.241.216.14
[*] PTR box5348.bluehost.com 162.241.216.17
[*] PTR 162-241-216-13.unifiedlayer.com 162.241.216.13
[*] PTR 162-241-216-15.unifiedlayer.com 162.241.216.15
[*] PTR 162-241-216-10.unifiedlayer.com 162.241.216.10
[*] PTR 162-241-216-16.unifiedlayer.com 162.241.216.16
[*] PTR 162-241-216-12.unifiedlaver.com 162.241.216.12
Menu Parrot Terminal
```

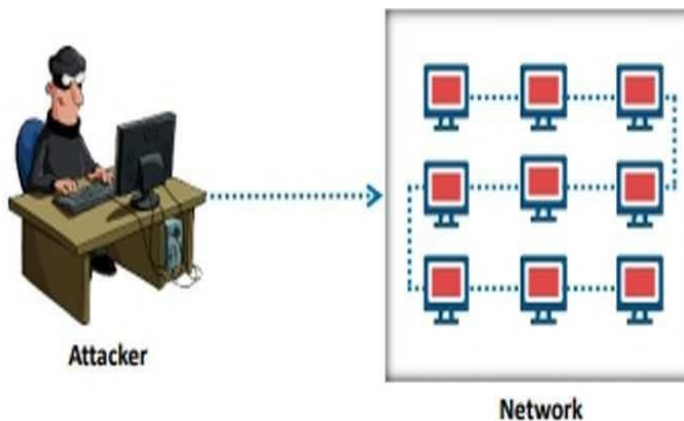
Reverse DNS Lookup

- DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address. When you are looking for a domain and type the domain name in the browser, the DNS converts that domain name into an IP address and forwards the request for further processing. This conversion of a domain name into an IP address is performed by a record. Attackers perform a reverse DNS lookup on the IP range to locate a DNS PTR record for such IP addresses. Attackers use various tools such as DNSRecon and Reverse IP Domain Check for performing the reverse DNS lookup on the target host. When we get an IP address or a range of IP addresses, we can use these tools to obtain the domain name.
- **DNSRecon**
- Source: <https://github.com>
- As shown in the screenshot, attackers use the following command to perform a reverse DNS lookup on the target host: `dnsrecon -r 162.241.216.0-162.241.216.255`
- In the above command, the `-r` option specifies the range of IP addresses (first-last) for a reverse lookup by brute force.
- Attackers also find the other domains that share the same web server using tools such as Reverse IP Domain Check. These tools list the possible domains that are hosted on the same web server.

8- Network Footprinting

Locate the Network Range

- Network range information assists attackers in creating a **map of the target network**
- One can find the **range of IP addresses** using **ARIN whois database search tool**
- One can also find the range of IP addresses and the subnet mask used by the target organization from **Regional Internet Registry (RIR)**



Network: NET-207-46-0-0-1

Source Registry ARIN
Net Range 207.46.0.0 - 207.46.255.255
CIDR 207.46.0.0/16
Name MICROSOFT-GLOBAL-NET
Handle NET-207-46-0-0-1
Parent NET-207-0-0-0-0
Net Type DIRECT ASSIGNMENT
Origin AS not provided
Registration Mon, 31 Mar 1997 05:00:00 GMT (Mon Mar 31 1997 local time)
Last Changed Wed, 21 Aug 2013 00:16:49 GMT (Wed Aug 21 2013 local time)
Self <https://rdap.arin.net/registry/ip/207.46.0.0>
Alternate <https://whois.arin.net/net/net/NET-207-46-0-0-1>
Port 43 Whois whois.arin.net

Related Entities ▾ 1 Entity

Source Registry ARIN
Kind Org
Full Name Microsoft Corporation
Handle MSFT
Address One Microsoft Way
Redmond
WA
98052
United States
Roles Registrant
Registration Fri, 10 Jul 1998 03:00:00 GMT (Fri Jul 10 1998 local time)
Last Changed Sat, 28 Jan 2017 13:32:29 GMT (Sat Jan 28 2017 local time)
Comments To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to:
* <https://cert.microsoft.com>.

Network Whois Record

Queried
whois.arin.net with
"207.46.232.182"

Information Gathering by Attackers

- How the network is structured
- Which machines in the networks are alive
- Network topology
- Access control device
- OS used in the target network.
- To find the network range of the target network, enter the server IP address (that was gathered in WHOIS footprinting) in the ARIN whois database search tool or you can go to the ARIN website (<https://www.arin.net/knowledge/rirs.html>) and enter the server IP in the SEARCH Whois text box
- If the DNS servers are not set up correctly, the attacker has a good chance of obtaining a list of internal machines on the server. Also, sometimes if an attacker traces a route to a machine, he or she can get the internal IP address of the gateway, which might be useful.



207.46.232.182

Search

all requests subject to [terms of use](#)

Pay Now

Feedback

Our Region

On this page

- » [ARIN's Region](#)
 - [Complete List of Countries in the ARIN Region](#)
- » [Regional Internet Registry Regions](#)

ARIN's Region

ARIN's geographical service area includes all of the countries in the list below. The links on the right provide a list of the countries within each Regional Internet Registry's region, and a map is available below showing all regions.

Complete List of Countries in the ARIN Region

by sector

Canada Sector

Country	A 2	A 3
CANADA	CA	CAN

Caribbean and North Atlantic Islands Sector

Country	A 2	A 3
ANGUILLA	AI	AIA
ANTIGUA AND BARBUDA	AG	ATG
BAHAMAS	BS	BHS

Attackers use target server's IP to locate network range

Welcome to ARIN

[Organization Structure & Staff](#)

[Our Region](#)

[ARIN Board of Trustees](#)

[Advisory Council](#)

[NRO Number Council](#)

[Careers](#)

Related

[All](#)

[AFRINIC](#)

[APNIC](#)

[LACNIC](#)

[RIPE NCC](#)

- Obtaining network information often requires the use of multiple tools because a single tool may not provide all the desired information.

Network: NET-207-46-0-0-1

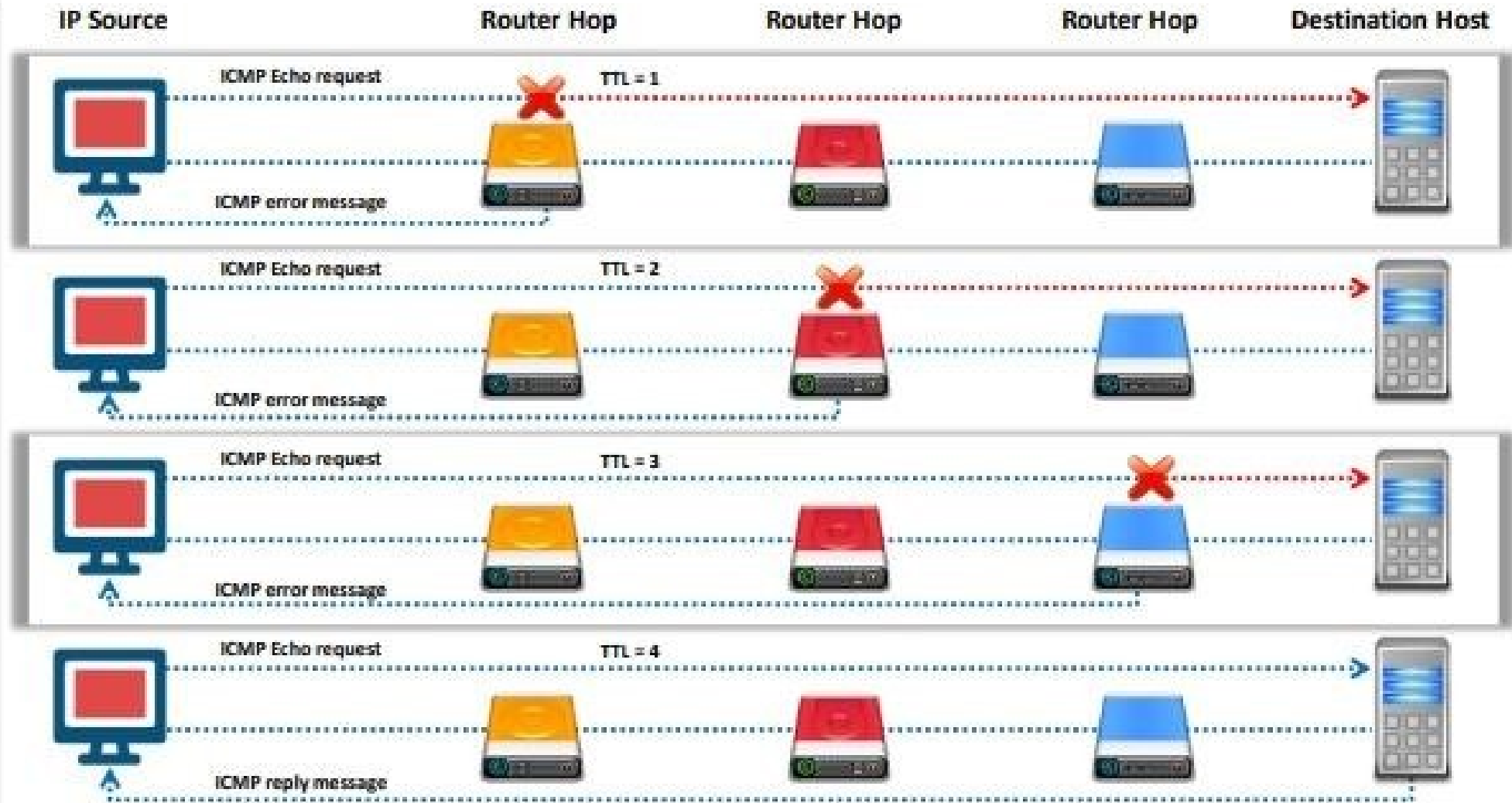
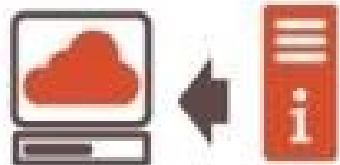
Source Registry	ARIN
Net Range	207.46.0.0 - 207.46.255.255
CIDR	207.46.0.0/16
Name	MICROSOFT-GLOBAL-NET
Handle	NET-207-46-0-0-1
Parent	NET-207-0-0-0-0
Net Type	DIRECT ASSIGNMENT
Origin AS	<i>not provided</i>
Registration	Mon, 31 Mar 1997 05:00:00 GMT (Mon Mar 31 1997 local time)
Last Changed	Wed, 21 Aug 2013 00:16:49 GMT (Wed Aug 21 2013 local time)
Self	https://rdap.arin.net/registry/ip/207.46.0.0
Alternate	https://whois.arin.net/rest/net/NET-207-46-0-0-1
Port 43 Whois	whois.arin.net

Related Entities ▼ 1 Entity

Source Registry	ARIN	Network Whois Record Queried whois.arin.net with "207.46.232.182"
Kind	Org	
Full Name	Microsoft Corporation	
Handle	MSFT	
Address	One Microsoft Way Redmond WA 98052 United States	
Roles	Registrant	
Registration	Fri, 10 Jul 1998 03:00:00 GMT (Fri Jul 10 1998 local time)	
Last Changed	Sat, 28 Jan 2017 13:32:29 GMT (Sat Jan 28 2017 local time)	
Comments	To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to: * https://cert.microsoft.com .	

Traceroute

Traceroute programs work on the concept of **ICMP protocol** and use the **TTL field in the header of ICMP packets** to discover the routers on the path to a target host



Traceroute

- Finding the route of the target host is necessary to test against man-in-the-middle attacks and other relative attacks. Therefore, you need to find the route of the target host in the network. This can be accomplished
- with the help of the Traceroute utility provided with most operating systems. It allows you to trace the path or route through which the target host packets travel in the network.
- Traceroute uses the ICMP protocol concept and TTL (Time to Live) field of IP header to find the path of the target host in the network.
- The Traceroute utility can detail the path IP packets travel between two systems. It can trace the number of routers the packets travel through, the round trip time duration in transiting between two routers, and, if the routers have DNS entries, the names of the routers and their network affiliation, as well as the geographic location. It works by exploiting a feature of the Internet Protocol called Time To Live (TTL). The TTL field is interpreted to indicate the maximum number of routers a packet may transit. Each router that handles a packet will decrement the TTL count field in the ICMP header by one. When the count reaches zero, the packet will be discarded and an error message will be transmitted to the originator of the packet.

Traceroute

- ICMP Traceroute
- `tracert 216.239.36.10`

- TCP Traceroute
- `tcptraceroute www.google.com`
- UDP Traceroute
- `traceroute www.google.com`

```
Command Prompt - tracert 2 x + v - □ ×
C:\Users\hp>tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10]
over a maximum of 30 hops:

  1    2 ms    2 ms    2 ms    192.168.0.1
  2    6 ms    8 ms    6 ms    10.10.10.1
  3    6 ms    6 ms    8 ms    10.224.100.89
  4    7 ms    6 ms    6 ms    10.224.100.253
  5    7 ms    6 ms    7 ms    10.224.101.45
  6   12 ms   11 ms    8 ms    10.5.9.62
  7   30 ms   32 ms   33 ms   37.236.240.137
  8   16 ms   15 ms   16 ms   37.236.249.126
  9   69 ms   *       70 ms   185.71.205.10
 10   63 ms   61 ms   80 ms   142.250.164.74
 11   65 ms   63 ms   63 ms   192.178.107.129
 12   65 ms   66 ms   65 ms   192.178.107.124
 13   96 ms   97 ms   96 ms   142.251.246.73
 14   97 ms   97 ms   97 ms   142.250.57.166
 15  104 ms  104 ms  105 ms  142.251.230.113
 16  102 ms  109 ms  116 ms  142.250.58.230
```

TCP Traceroute

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~#
[root@parrot]~# tcptraceroute www.google.com
Running:
tcptraceroute -T -D info www.google.com
tcptraceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
 1  10.10.10.2 (10.10.10.2)  0.312 ms  0.172 ms  0.207 ms
 2  maa05s05-in-f4.1e106.net (172.217.163.164) <syn,ack> 17.775 ms 17.367
ms 17.491 ms
```

UDP Traceroute

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~#
[root@parrot]~# traceroute www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
 1  10.10.10.2 (10.10.10.2)  0.260 ms  0.189 ms  0.196 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
```

9- Footprinting through Social Engineering

- Social engineering is an art of exploiting human behaviour to **extract confidential information**
- Social engineers depend on the fact that **people are unaware** of their valuable information and are careless about protecting it



Social engineers attempt to gather

- Credit card details and social security number
- User names and passwords
- Security products in use
- Operating systems and software versions
- Network layout information
- IP addresses and names of servers



Social engineering techniques include

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation



9- Footprinting through Social Engineering

Eavesdropping

- Unauthorized listening of conversations or reading of messages.
- It is the interception of any form of communication, such as audio, video, or text.

Shoulder Surfing

- Secretly observing the target to gather critical information, such as passwords, personal identification number, account numbers, and credit card information.

Dumpster Diving

- Looking for treasure in someone else's trash
- It involves the collection of phone bills, contact information, financial information, operations-related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

Impersonation

- Pretending to be a legitimate or authorized person and using the phone or other communication medium to mislead targets and trick them into revealing information

Maltego

- Source: <https://www.paterva.com>
- Maltego is a program that can be used to determine the relationships and real-world links between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.
- Attackers can use different entities available in the tool to obtain information such as email addresses, a list of phone numbers, and a target's Internet infrastructure (domains, DNS names, Netblocks, IP addresses information).

The screenshot displays the Maltego Community Edition 4.1.6 interface. The main window shows a graph titled 'New Graph (1)' with a 'Person' entity 'John Doe' at the top. Four arrows point from 'John Doe' to four email address entities: 'John.Doe@hotmail.com', 'jDoe@hotmail.com', 'JohnD@hotmail.com', and 'JohnDoe@hotmail.com'. A red box highlights these email addresses. A callout bubble points to 'John Doe' with the text 'Attackers add a Person entity to target an individual'. Another callout bubble points to the email addresses with the text 'Obtain target's email addresses'. The interface includes a menu bar (Investigate, View, Entities, Collections, Transforms, Machines, Collaboration, Import, Export, Windows), a toolbar with icons for Copy, Paste, Cut, Delete, Clear Graph, and Entity Selection, and a sidebar with an Entity Palette containing categories like Recently Used, Groups, Infrastructure, and AS. The bottom status bar shows '1 of 5 entities'.


```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# usufy.py -n Mark Zuckerberg -p twitter facebook youtube
```

Attackers search for a target user on social media platforms

OSRFramework

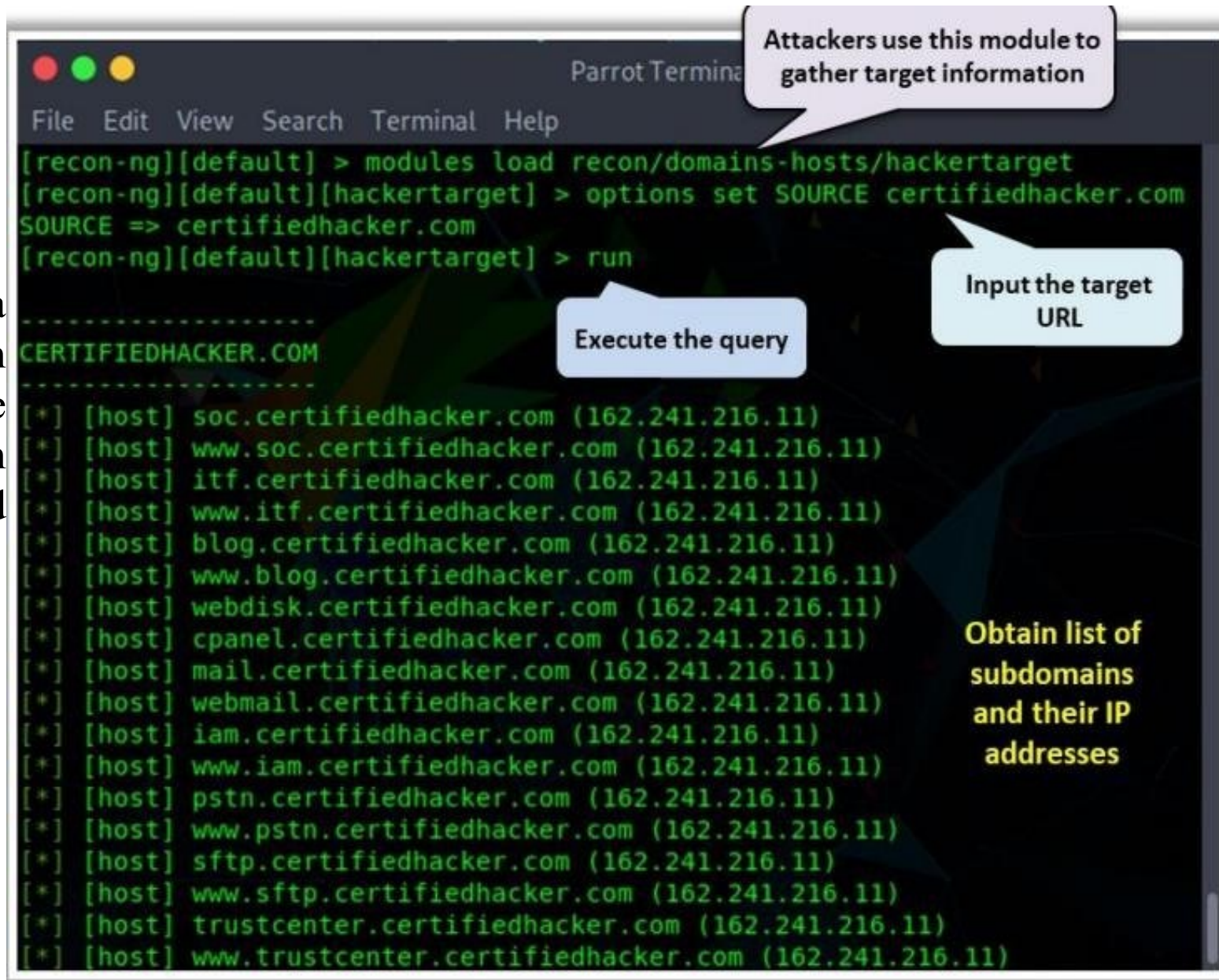
- includes applications related to username checking, DNS lookups, information leaks research, deep web search, and regular expression extraction.
- The tools included in the OSRFramework:
- **usufy.py** - Checks for a user profile on up to 290 different platforms
- **mailfy.py** - Check for the existence of a given email
- **searchfy.py** - Performs a query on the platforms in OSRFramework
- **domainfy.py** - Checks for the existence of domains
- **phonefy.py** - Checks for the existence of a given series of phones
- **entify.py** - Uses regular expressions to extract entities

```
Parrot Terminal
File Edit View Search Terminal Help
2019-10-09 02:01:05.453780 Results obtained: Search results
Sheet Name: Profiles recovered (2019-10-9_2h1m).
+-----+-----+-----+
| i3visio_uri | i3visio_alias | i3visio_platform |
+-----+-----+-----+
| https://www.facebook.com/Mark | Mark | Facebook |
+-----+-----+-----+
| https://www.youtube.com/user/Mark/about | Mark | Youtube |
+-----+-----+-----+
| http://twitter.com/Mark | Mark | Twitter |
+-----+-----+-----+
| http://twitter.com/Zuckerberg | Zuckerberg | Twitter |
+-----+-----+-----+
2019-10-09 02:01:05.467942 You can find all the information here:
./profiles.csv
2019-10-09 02:01:05.468303 Finishing execution...
Total time consumed: 0:00:30.249380
Average seconds/query: 10.0831266667 seconds
```

Recon-ng

Source: <https://github.com> Recon-ng is a web reconnaissance framework with independent modules for database interaction that provides an environment in which open-source web-based reconnaissance can be conducted.

As shown in the screenshot, attackers use the module recon/domains-hosts/hackertarget to extract a list of subdomains and IP addresses associated with the target URL.



Parrot Terminal

```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][default][hackertarget] > run
```

CERTIFIEDHACKER.COM

```
[*] [host] soc.certifiedhacker.com (162.241.216.11)
[*] [host] www.soc.certifiedhacker.com (162.241.216.11)
[*] [host] itf.certifiedhacker.com (162.241.216.11)
[*] [host] www.itf.certifiedhacker.com (162.241.216.11)
[*] [host] blog.certifiedhacker.com (162.241.216.11)
[*] [host] www.blog.certifiedhacker.com (162.241.216.11)
[*] [host] webdisk.certifiedhacker.com (162.241.216.11)
[*] [host] cpanel.certifiedhacker.com (162.241.216.11)
[*] [host] mail.certifiedhacker.com (162.241.216.11)
[*] [host] webmail.certifiedhacker.com (162.241.216.11)
[*] [host] iam.certifiedhacker.com (162.241.216.11)
[*] [host] www.iam.certifiedhacker.com (162.241.216.11)
[*] [host] pstn.certifiedhacker.com (162.241.216.11)
[*] [host] www.pstn.certifiedhacker.com (162.241.216.11)
[*] [host] sftp.certifiedhacker.com (162.241.216.11)
[*] [host] www.sftp.certifiedhacker.com (162.241.216.11)
[*] [host] trustcenter.certifiedhacker.com (162.241.216.11)
[*] [host] www.trustcenter.certifiedhacker.com (162.241.216.11)
```

Attackers use this module to gather target information

Execute the query

Input the target URL

Obtain list of subdomains and their IP addresses

Footprinting Countermeasures

- Restrict the employees' access to social networking sites from the organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums
- Do not reveal critical information in press releases, annual reports, product catalogs, and so on.
- Limit the amount of information that you are publishing on the website/Internet
- Use footprinting techniques to discover and remove any sensitive information publicly available
- Prevent search engines from caching a web page and use anonymous registration services
- Develop and enforce security policies such as information security policy, password policy, and so on, to regulate the information that employees can reveal to third parties
- Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers
- Conduct security awareness training periodically to educate employees about various social engineering tricks and risks
- Choose privacy services when conducting a Whois lookup on a database for enhanced data protection.

Footprinting Countermeasures

- Avoid domain-level cross-linking for critical assets
- Disable directory listings in the web servers
- Encrypt and password-protect sensitive information
- Do not enable protocols that are not required
- Always use TCP/IP and IPSec filters for defense in depth
- Configure IIS to avoid information disclosure through banner grabbing
- Hide the IP address and the related information by implementing VPN or keeping the server behind a secure proxy
- Request archive.org to delete the history of the website from the archive database
- Keep the domain name profile private

Footprinting Countermeasures

- Place critical documents such as business plans and proprietary documents offline to prevent exploitation
- Train employees to thwart social engineering techniques and attacks
- Sanitize the details provided to the Internet registrars to hide the direct contact details of the organization
- Disable the geo-tagging functionality on cameras to prevent geolocation tracking
- Avoid revealing one's location or travel plans on social networking sites
- Turn-off geolocation access on all mobile devices when not required
- Ensure that no critical information such as strategic plans, product information, and sales projections is displayed on notice boards or walls.

Network Scanning

- Network scanning refers to a set of procedures used for **identifying hosts, ports, and services** in a network.
- Network scanning is one of the **components of intelligence gathering** which can be used by an attacker to create a profile of the target organization

The main objective of Network Scanning

- To identify live hosts on a network
 - To identify open & closed ports
 - To identify operating system information
 - To identify services running on a network
 - To identify running processes on a network
 - To identify vulnerabilities
-
- Network scanning gathers detailed target information using aggressive techniques.
 - It identifies hosts, ports, services, active machines, and target OS in a network.
 - Vital for intelligence gathering, helping attackers profile target organizations.
 - Collects specific IP addresses, OS, system architecture, and services on each computer.

Network Scanning

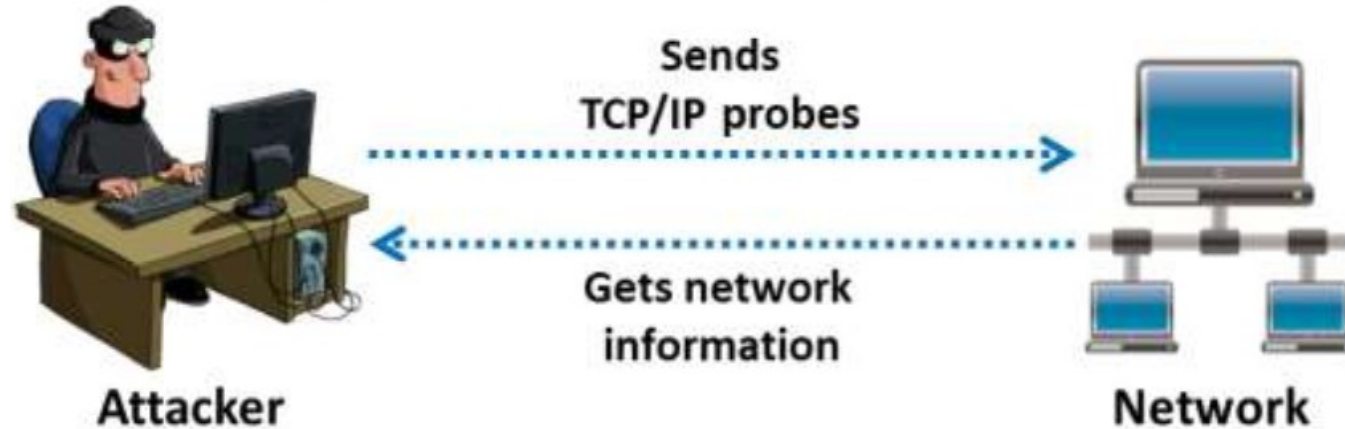


Figure 3.1: Network scanning process

The purpose of scanning is to **discover exploitable communications channels**, probe as many listeners as possible, and track the ones that are responsive or useful to an attacker's particular needs. In the scanning phase of an attack, the attacker tries to find various ways to intrude into a target system. The attacker also tries to discover more information about the target system to determine the presence of any configuration lapses. The attacker then uses the information obtained to develop an attack strategy.

Types of Scanning

- **Port Scanning** - Lists the open ports and services. Port scanning is **the process of checking the services running on the target computer by sending a sequence of messages** in an attempt to break in. Port scanning involves connecting to or probing TCP and UDP ports of the target system to determine whether the services are running or are in a listening state. The listening state provides information about the OS and the application currently in use. Sometimes, **active services that are listening may allow unauthorized users to misconfigure systems or to run software with vulnerabilities.**
- **Network Scanning** - Lists the active hosts and IP addresses. Network scanning is a procedure for identifying active hosts on a network, either to attack them or assess the security of the network.
- **Vulnerability Scanning** — Shows the presence of known weaknesses. Vulnerability scanning is a method for checking whether a system is exploitable by identifying its vulnerabilities. A vulnerability scanner consists of a scanning engine and a catalog. The catalog includes a list of common files with known vulnerabilities and common exploits for a range of servers. A vulnerability scanner may, for example, look for backup files or directory traversal exploits. The scanning engine maintains logic for reading the exploit list, transferring the request to the web server, and analyzing the requests to ensure the safety of the server. These tools generally target vulnerabilities that secure host configurations can fix easily through updated security patches and a clean web document.

Scanning Methodology

Check for live systems
- Ping or other type of way to determine live hosts

Check for open ports
- Once you know live host IPs, scan them for listening ports

Scan beyond IDS - If needed, use methods to scan beyond the detection systems; evade IDS using proxies, spoofing, fragmented packets and so on

Perform banner grabbing - Grab from servers as well as perform OS fingerprinting (versions of the running services)

Scan for vulnerabilities - Use tools to look at the vulnerabilities of open systems

Draw network diagrams - Shows logical and physical pathways into networks

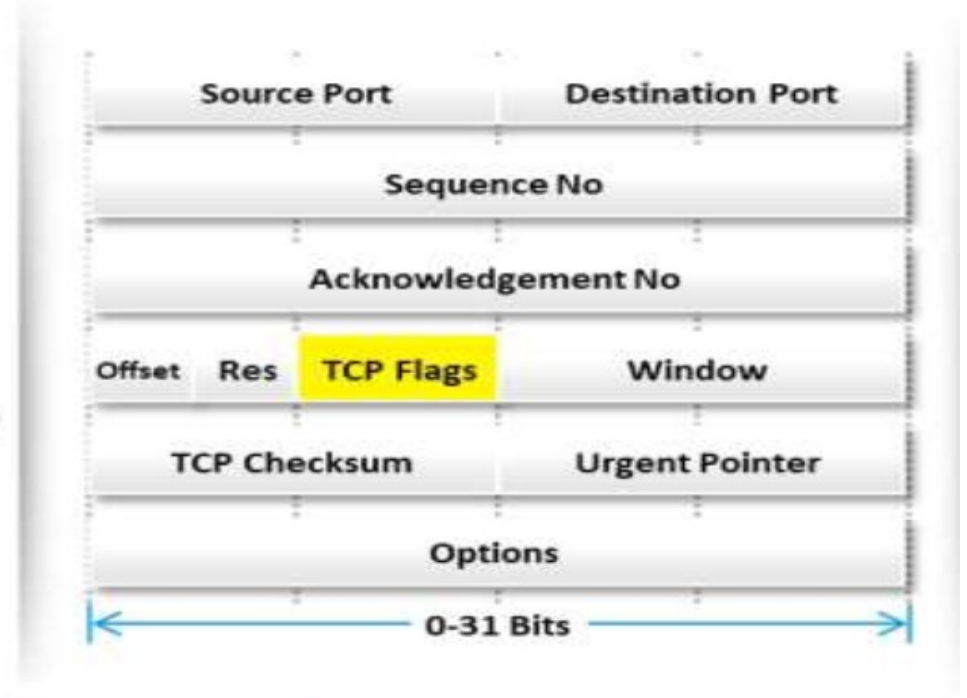
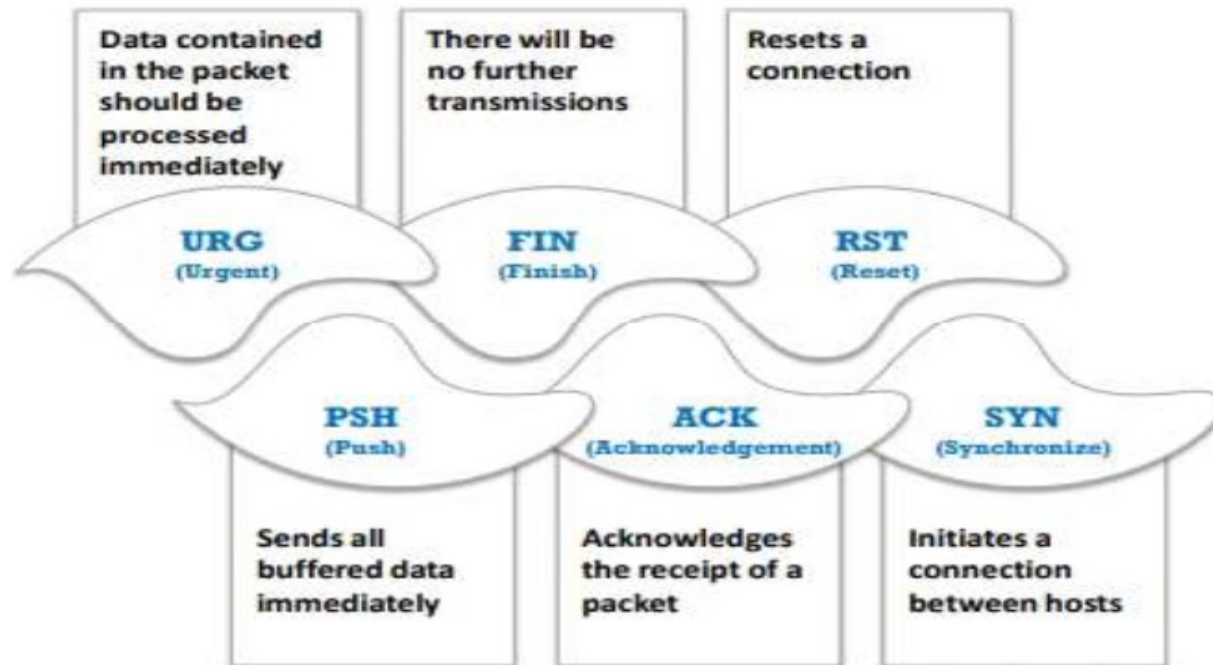
Use proxies - Obscures efforts to keep you hidden

Pentest Report - Document everything that you find



TCP Communication Flag

- **TCP (Transmission Control Protocol)** : is connection oriented - once a connection is established, data can be sent bidirectional.
- **UDP (User Datagram Protocol)** : is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.
- Flags are also called control bits. Each flag corresponds to 1-bit information. The most commonly used flags are **SYN, URG, ACK, PSH, FIN, and RST.**



Standard TCP communications are controlled by flags in the TCP packet header

TCP Communication Flag

- The TCP header contains various flags that control the transmission of data across a TCP connection. Six TCP control flags manage the connection between hosts and give instructions to the system. Four of these flags (SYN, ACK, FIN, and RST) govern the establishment, maintenance, and termination of a connection. The other two flags (PSH and URG) provide instructions to the system. The size of each flag is 1 bit. As there are six flags in the TCP Flags section, the size of this section is 6 bits. When a flag value is set to "1," that flag is automatically turned on.

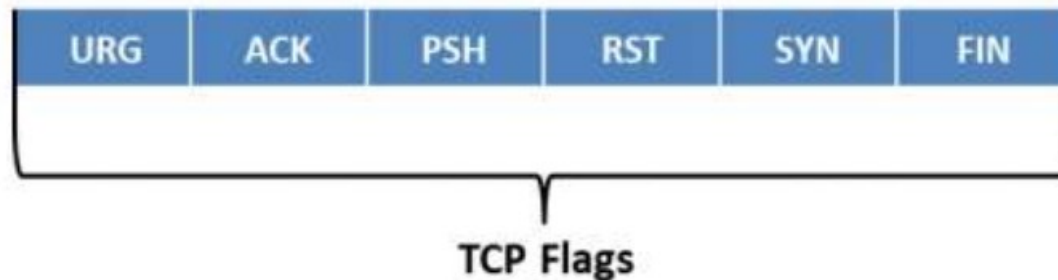
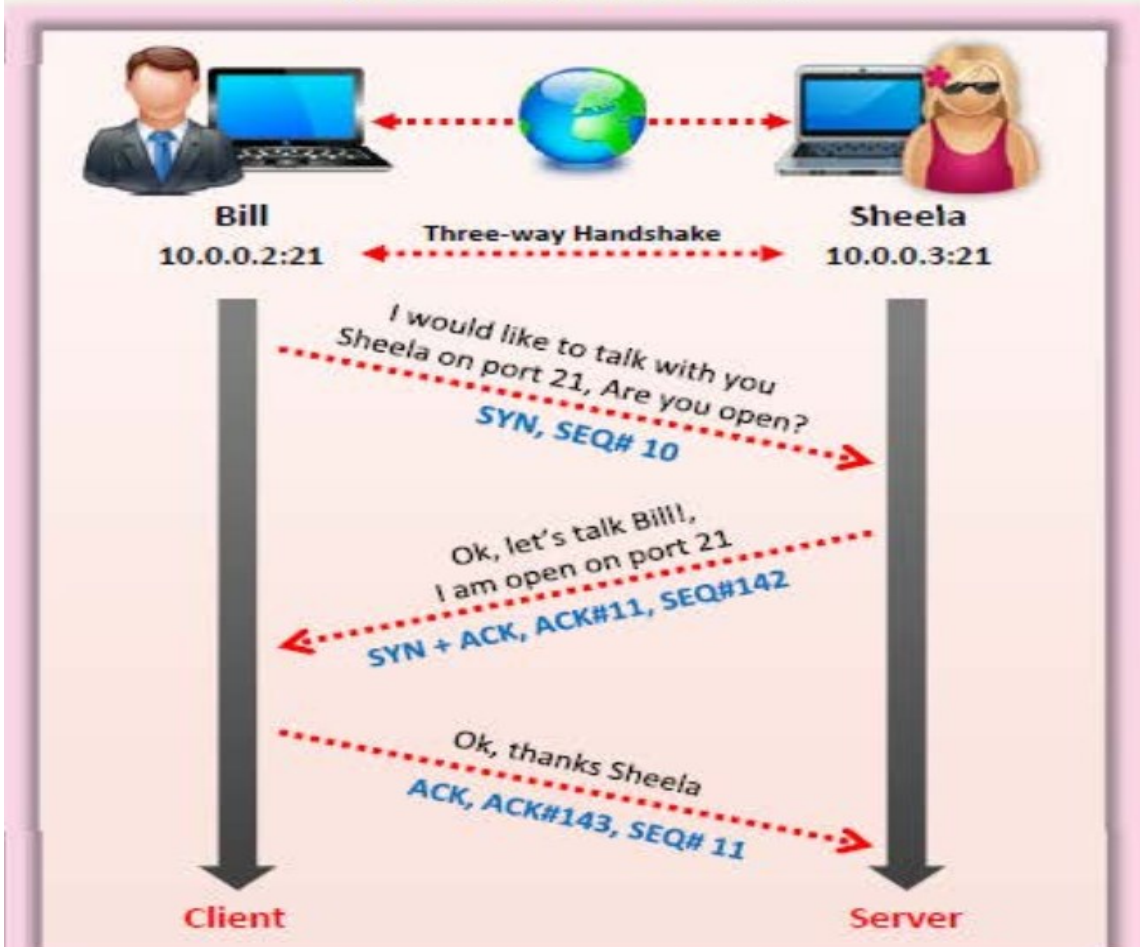


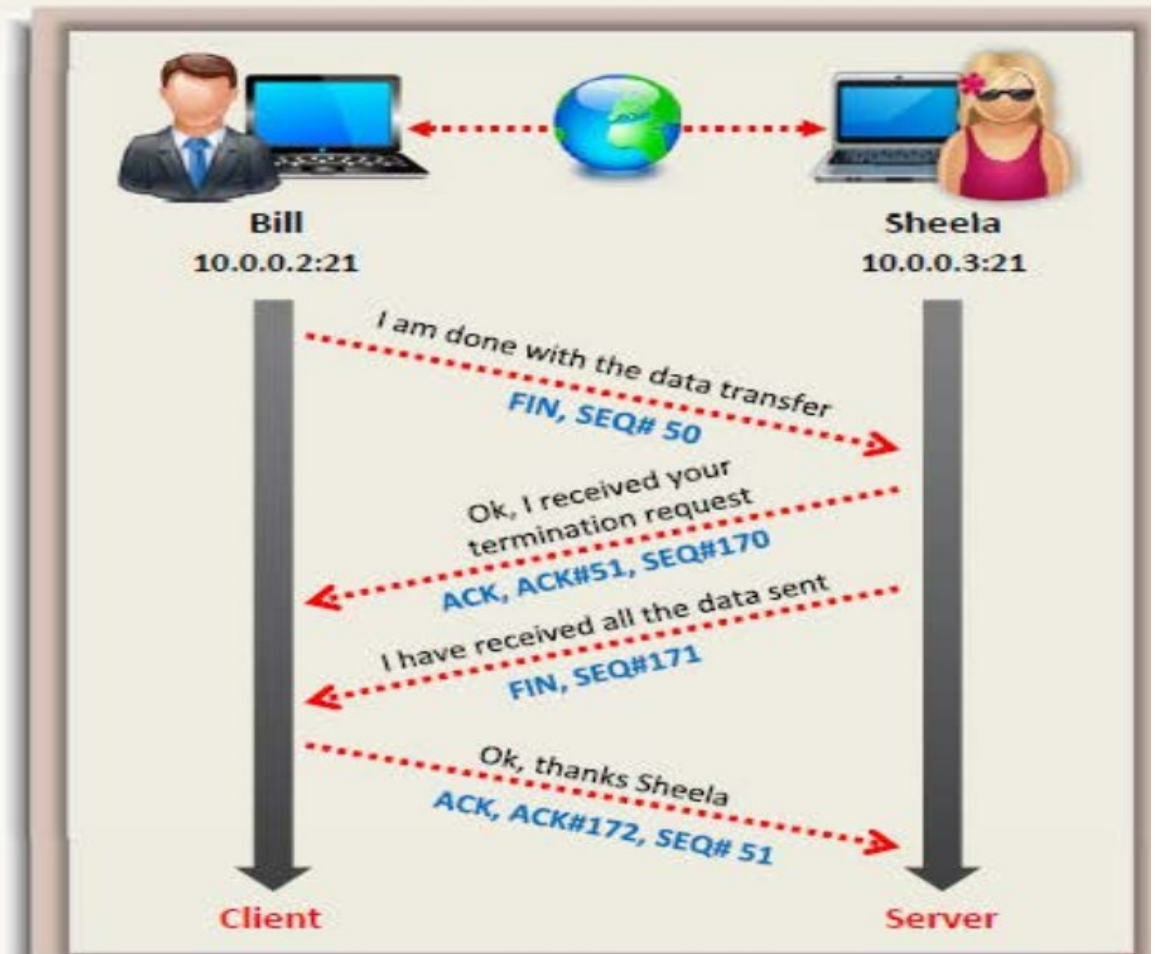
Figure 3.3: TCP communication flags

TCP/IP Communication

TCP Session Establishment (Three-way Handshake)



TCP Session Termination



Scanning Tools

- Scanning tools are used to scan and identify live hosts, open ports, running services on a target network, location info, NetBIOS info, and information about all TCP/IP and UDP open ports. The information obtained from these tools will help an ethical hacker in creating the profile of the target organization and scanning the network for open ports of the devices connected.
- **Nmap**
- Source: <https://nmap.org>
- Nmap ("Network Mapper") is a security scanner for network exploration and hacking. It allows you to discover hosts, ports, and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. It scans vast networks of literally hundreds of thousands of machines. Nmap includes many mechanisms for port scanning (TCP and UDP), OS detection, version detection, ping sweeps, and so on. Either a network administrator or an attacker can use this tool for their specific needs. Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime. Attackers use Nmap to extract information such as live hosts on the network, open ports, services (application name and version), type of packet filters/firewalls, MAC details, and OSs along with their versions.
- **Syntax: # nmap <options> <Target IP address>**

```

(kali@kali)-[~]
└─$ nmap 172.16.121.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-27 05:30 PDT
Nmap scan report for 172.16.121.128
Host is up (0.00020s latency)
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 2.34 seconds

```

Example of a single target scan

- 1- A total of 995 ports are in a *closed* state.
- 2- The five open ports run Windows-specific services [*msrpc*, *netbios-ssn*, *microsoft-ds*, *wsddapi*, *Elite*].

Port state	Description
OPEN	A port that responds actively to an incoming connection.
CLOSED	A port that responds actively to a probe but there is no service running on the respective port.
FILTERED	A port that is actively protected by a firewall and prevents Nmap from determining the port status [open or closed].
UNFILTERED	A port can be scanned, but Nmap cannot precisely determine if the port is open or closed.
OPEN FILTERED	A port that Nmap sees as open but cannot precisely determine the actual state of the port.
CLOSED FILTERED	A port that Nmap sees as closed but cannot precisely determine the actual state of the port.

Table : NMAP commands – port states

Multiple Targets Scan With NMAP

Syntax : `nmap <Target1 Target2 Target3 etc.>`

```
(kali@kali) - [~]
└─$ nmap 172.16.121.128 172.16.121.131 172.16.121.132
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-27 06:32 PDT
Nmap scan report for 172.16.121.128
Host is up (0.00082s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
31337/tcp open  Elite

Nmap scan report for 172.16.121.131
Host is up (0.00083s latency).
All 1000 scanned ports on 172.16.121.131 are closed

Nmap scan report for 172.16.121.132
Host is up (0.00041s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind

Nmap done: 3 IP addresses (3 hosts up) scanned in 6.38 seconds

(kali@kali) - [~]
└─$
```

IP Range Scan With NMAP

Syntax : `nmap <IP range>`

```
(kali@kali) - [~]
└─$ nmap 172.16.121.125-135
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-27 06:59 PDT
Nmap scan report for 172.16.121.128
Host is up (0.00091s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
31337/tcp open  Elite

Nmap scan report for 172.16.121.129
Host is up (0.00032s latency).
All 1000 scanned ports on 172.16.121.129 are closed

Nmap scan report for 172.16.121.131
Host is up (0.00068s latency).
All 1000 scanned ports on 172.16.121.131 are closed

Nmap scan report for 172.16.121.132
Host is up (0.00079s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind

Nmap done: 11 IP addresses (4 hosts up) scanned in 7.31 seconds

(kali@kali) - [~]
└─$
```

Scanning Tools

- **Hping2/Hping3**
- Source: <http://www.hping.org>
- Hping2/Hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions. It can send custom TCP/IP packets and display target replies similarly to a ping program with ICMP replies. It handles fragmentation as well as arbitrary packet body and size, and it can be used to transfer encapsulated files under the supported protocols. It also supports idle host scanning. IP spoofing and network/host scanning can be used to perform an anonymous probe for services. Hping2/Hping3 also has a Traceroute mode, which enables attackers to send files between covert channels. It also determines whether the host is up even when the host blocks ICMP packets. Its firewalk-like usage allows the discovery of open ports behind firewalls. It performs manual path MTU discovery and enables attackers to perform remote OS fingerprinting. Using Hping, an attacker can study the behavior of an idle host and gain information about the target, such as the services that the host offers, the ports supporting the services, and the OS of the target. This type of scan is a predecessor to either heavier probing or outright attacks.
- **Syntax: # hping <options> <Target IP address>**

Scanning Tools

- **Hping Commands**

- The various Hping commands are as follows:

- **ICMP ping**

- Ex. `hping3 -1 10.0.0.25`

- Hping performs an ICMP ping scan by specifying the argument `-1` in the command line. You may use `--ICMP` or `-1` as the argument in the command line. By issuing the above command, hping sends an ICMP echo request to 10.0.0.25 and receives an ICMP reply similarly to a ping utility.

- **ACK scan on port 80**

- Ex. `hping3 -A 10.0.0.25 -p 80`

- Hping can be configured to perform an ACK scan by specifying the argument `-A` in the command line. Here, you set the ACK flag in the probe packets and perform the scan. You perform this scan when a host does not respond to a ping request. By issuing this command, Hping checks if a host is alive on a network. If it finds a live host and an open port, it returns an RST response.

Scanning Tools

- **UDP scan on port 80**
- Ex. `hping3 -2 10.0.0.25 -p 80`
- Hping uses TCP as its default protocol. Using the argument `-2` in the command line specifies that Hping operates in the UDP mode. You may use either `--udp` or `-2` as the argument in the command line.
- By issuing the above command, Hping sends UDP packets to port 80 on the host (10.0.0.25). It returns an ICMP port unreachable message if it finds the port closed and does not return a message if the port is open.
- **Collecting Initial Sequence Number**
- Ex. `hping3 192.168.1.103 -Q -p 139 -s`
- Using the argument `-Q` in the command line, Hping collects all the TCP sequence numbers generated by the target host (192.168.1.103).
- **Firewalls and Timestamps**
- Ex. `hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
- Many firewalls drop those TCP packets that do not have the TCP Timestamp option set. By adding the `--tcp-timestamp` argument in the command line, you can enable the TCP timestamp option in Hping and try to guess the timestamp update frequency and uptime of the target host (72.14.207.99).

Scanning Tools

- **SYN scan on port 50-60**
- Ex. `hping3 -8 50-60 -s 10.0.0.25 -V`
- Using the argument `-8` or `--scan` in the command line, you are operating Hping in the scan mode to scan a range of ports on the target host. Adding the argument `-S` allows you to perform a SYN scan. Therefore, the above command performs a SYN scan on ports 50-60 on the target host.
- **FIN, PUSH and URG scan on port 80**
- Ex. `hping3 -F -P -U 10.0.0.25 -p 80`
- By adding the arguments `-F`, `-P`, and `-U` in the command line, you are setting FIN, PUSH, and URG packets in the probe packets. By issuing this command, you are performing FIN, PUSH, and URG scans on port 80 on the target host (10.0.0.25). If port 80 is open, you will not receive a response. If the port is closed, Hping will return an RST response.
- **Scan entire subnet for live host**
- Ex. `hping3 -1 10.0.1.x --rand-dest -I eth0`
- By issuing this command, Hping performs an ICMP ping scan on the entire subnet 10.0.1.x; in other words, it sends an ICMP echo request randomly (`--rand-dest`) to all the hosts from 10.0.1.0 to 10.0.1.255 that are connected to the interface eth0. The hosts whose ports are open will respond with an ICMP reply. In this case, you have not set a port; hence, Hping sends packets to port 0 on all IP addresses by default.

Scanning Tools

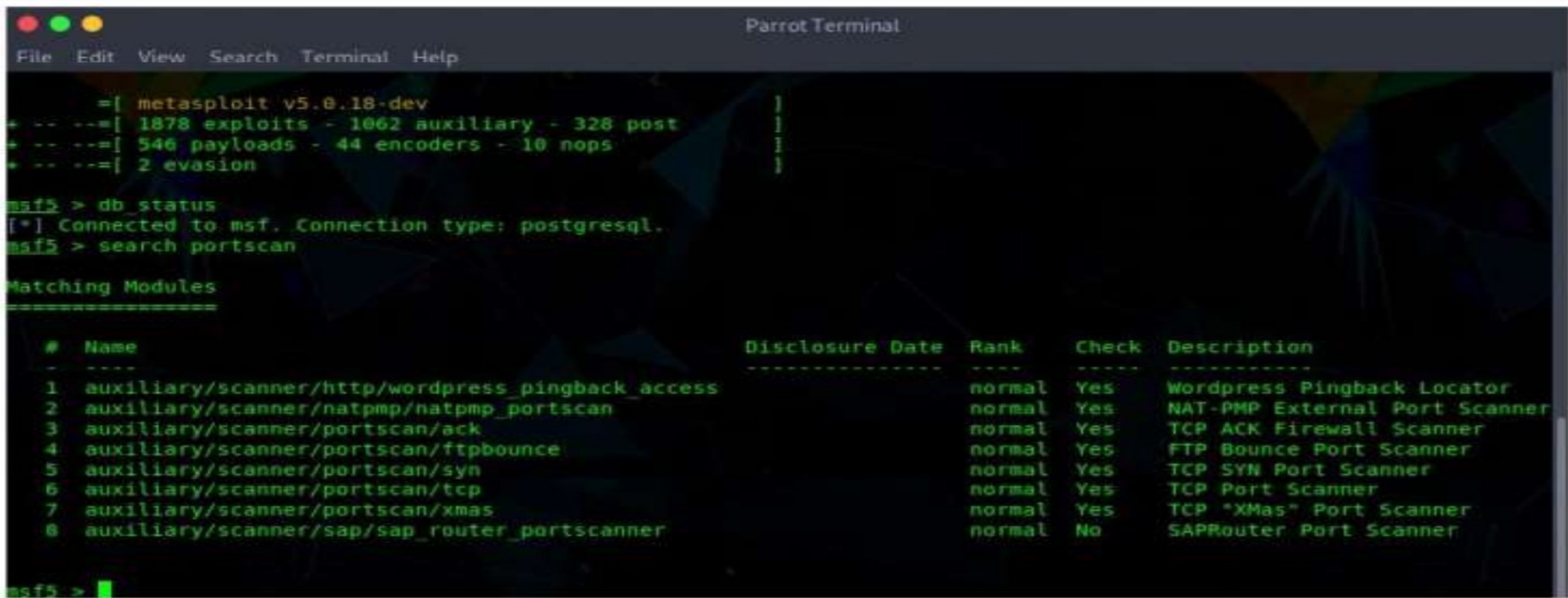
- **Metasploit**

Source: <https://www.metasploit.com>

Metasploit is an open-source project that provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing. It provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It facilitates the tasks of attackers, exploits writers, and payload writers. A major advantage of the framework is the modular approach, i.e., allowing the combination of any exploit with any payload.

It enables you to automate the process of discovery and exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

Scanning Tools



The screenshot shows a Parrot Terminal window with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar (Parrot Terminal). The terminal displays the following text:

```
msf5 > db_status  
[*] Connected to msf. Connection type: postgresql.  
msf5 > search portscan
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
1	auxiliary/scanner/http/wordpress_pingback_access		normal	Yes	Wordpress Pingback Locator
2	auxiliary/scanner/natpmp/natpmp_portscan		normal	Yes	NAT-PMP External Port Scanner
3	auxiliary/scanner/portscan/ack		normal	Yes	TCP ACK Firewall Scanner
4	auxiliary/scanner/portscan/ftpbounce		normal	Yes	FTP Bounce Port Scanner
5	auxiliary/scanner/portscan/syn		normal	Yes	TCP SYN Port Scanner
6	auxiliary/scanner/portscan/tcp		normal	Yes	TCP Port Scanner
7	auxiliary/scanner/portscan/xmas		normal	Yes	TCP "XMas" Port Scanner
8	auxiliary/scanner/sap/sap_router_portscanner		normal	No	SAPRouter Port Scanner

msf5 >

Figure 3.10: Screenshot displaying various Metasploit port scan modules

Thank
You

