

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Reconnaissance & Footprinting



*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Previous sessions...

- **Testing Terminologies**
- **Information Security**
- **Hacking**
- **Understanding Risk**
- **Assessing, Managing and Monitoring Risk**
- **Cyber risk resilience**
- **Penetration Testing**
- **Laws and Standards**

Lab/ Tutorials

- **Activity 1: Download and Setup your Lab.**
- **Coursework Description.**

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

So far, we discussed about Information security, the threats and attack vectors. In continuation to that, I hope you all have understood the hacking concepts and the reasons to stay ethical. Add more insight, we also discussed various security laws and standards. To conclude, we covered various “Risk” concepts like risk factors, cyber risk resilience in the process of enhancing security.



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Footprinting and Reconnaissance

- **Introduction**
- **Concepts**
- **Methodology**
- **Tools**
- **Countermeasures**
- **Penetration Testing**

Lab/ Tutorials

- **Activity 2 – Information Gathering**

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk

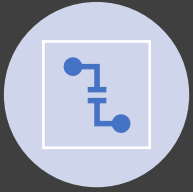
During this week, we shall continue to understand Footprinting concepts focusing on different methodologies like Search Engines, Google Hacking Techniques etc.

We shall also walkthrough Website Footprinting, Email Footprinting, Competitive Intelligence, Network Footprinting etc.

During the tutorials, under isolated lab environment you will be using different Footprinting tools to understand the countermeasures and pen testing attacks.



Footprinting and Reconnaissance



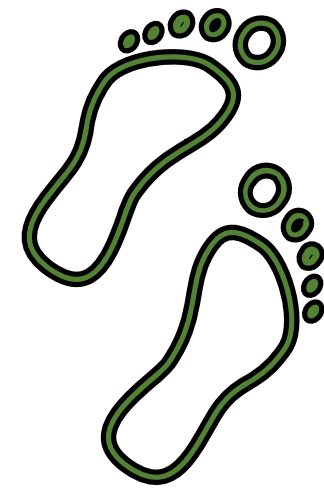
FOOTPRINTING IS THE INITIAL STAGE OF AN ATTACK ON INFORMATION SYSTEMS.



PRECISELY, AS AN ATTACKER, YOU COLLECT RELEVANT INFORMATION ABOUT THE TARGET NETWORK.



USING THE GATHERED INFORMATION, VARIOUS WAYS TO INTRUDE THE SYSTEM WILL BE IDENTIFIED.



- ✓ **Reconnaissance** is the method of collecting information about a target system without alerting it.
- ✓ Also known as **Footprinting**, it is the first step in any form of hacking.
- ✓ It will help in understanding the target system and identify potential attack vectors & vulnerabilities



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

Footprinting

- A 7-step process is followed to gather as much information about the network as possible

Information Gathering

- The information gathering steps are vital. Good information helps in successful analysis

Determining network range

- It is important to find the available IP addresses for scanning and further enumeration.

Identify Active Machines

- It is important to know if a machine is alive before an attack is performed

Finding open ports and access points

- Identifying open ports will be the next step to initiate potential attack vectors.

OS Fingerprinting

- After getting the IP addresses, active systems, & open ports, the type of systems is the next checkbox to tick

Fingerprinting services

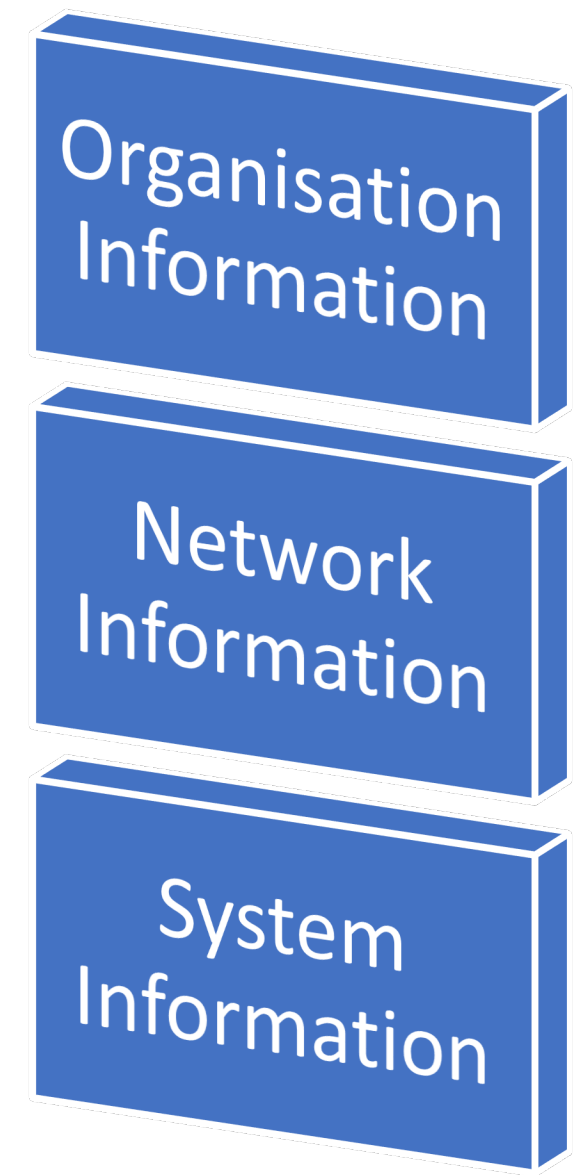
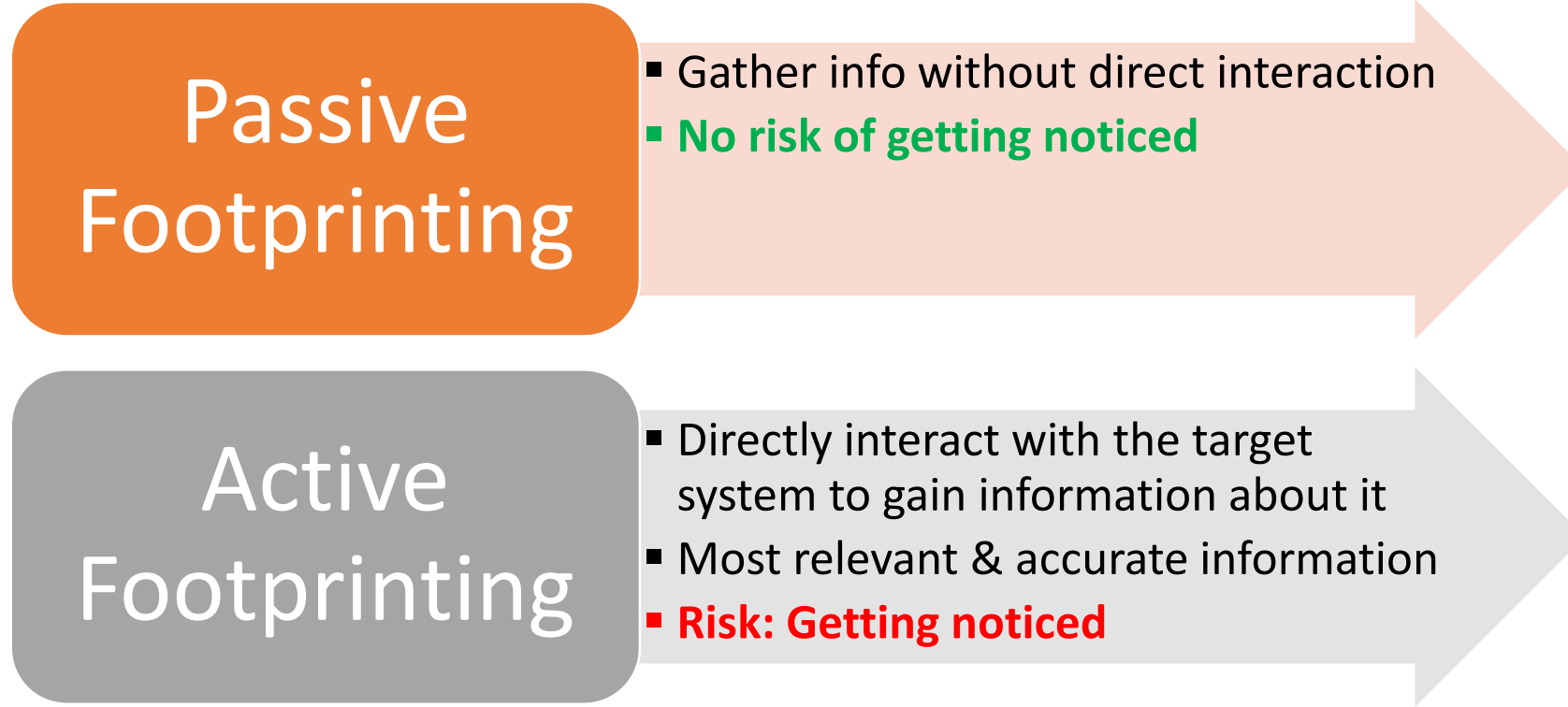
- The services running on specific ports allows to formulate & launch app specific attacks.

Mapping the network

- Mapping the network provides with a blueprint of the organization.

Footprinting

Types



Footprinting

- Footing helps to

Know Security Posture

- Understand the security posture of the target

Reduce Focus Area

- Instead of focusing on a large range of IP address, based on the gathered information, more specific ranges, networks, domain names, etc

Identify Vulnerabilities

- Privilege to select appropriate exploits based on the identified vulnerabilities.

Map the network

- To know the actual environment by mapping based on the gathered information.

Footprinting – Using Search Engines

- *Attackers use search engines to extract information about a target*
- *Use those gathered information to do social engineering attacks*
- *Create advanced search operators supported by search engines to create complex queries. Search operators help in finding, filtering very specific target information.*
- *Google Hacking Techniques: Using Google search engine to create complex search queries.*
- *[cache:] Display the web pages stored in Google Cache*
- *[link:] Lists web pages that have links to the specified web page*
- *[related:] Lists web page that are similar to a specified web page*
- *[site:] Restricts the results to those websites in the given domain*
- *[allintitle:] Restricts the results to those websites with all of the search keywords in the title.*
- *[intitle:] Restricts the results to documents containing the search keywords in the URL*
- *[allinurl:] Restricts the results to those with all of the search keywords in the URL*
- *[inurl:] Restricts the results to documents containing the search keyword in the URL*
- *[location:] Finds information for a specific location.*
- *[info:] Presents some information that Google has about a particular web page*
- *Alternate Options: Google Advanced Search*

Footprinting – Sources

- **Google Hacking**
 - Using basic search techniques combined with advanced operations, Google can be used as a powerful vulnerability search tool
- **USENET**
 - A collection of tons of discussion groups on the internet
- **Insecure Applications**
 - When defense in depth is not used and an application is insecure, a lot of information can be leaked
- **Registrar Query**
 - Obtain registrar information from bodies like The Internet Corporation for Assigned Names and Numbers (ICANN), Regional Internet Registries (RIR), etc.
- **DNS Enumeration**
 - Locating the DNS servers and their corresponding records of an organization

Footprinting – Using Databases

The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end penetration testing services. The Exploit Database is a non-profit project that is provided as a public service by Offensive Security.

[<https://www.exploit-db.com/>]

The screenshot displays the Exploit Database website. A modal window titled "About The Exploit Database" by Offensive Security is open, providing information about the database's purpose and history. The background shows a list of exploits with columns for Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author. The list includes various exploits such as "WordPress Plugin Learnpress 4.1.4.1 - Arbitrary Image Renaming" and "WordPress Plugin Post Grid 2.1.1 - Cross Site Scripting (XSS)".

About The Exploit Database
Offensive Security.

The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Our aim is to serve the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database. The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who need actionable data right away.

The Google Hacking Database (GHDB) is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, information made publicly available on the Internet. In most cases, this information was never meant to be made public but due to any number of factors this information was linked in a web document that was crawled by a search engine that subsequently followed that link and indexed the sensitive information.

The process known as "Google Hacking" was popularized in 2000 by Johnny Long, a professional hacker, who began cataloging these queries in a database known as the Google Hacking Database. His initial efforts were amplified by countless hours of community member effort, documented in the book Google Hacking For Penetration Testers and popularised by a barrage of media attention and Johnny's talks on the subject such as this early talk recorded at DEFCON 13. Johnny coined the term "Googledork" to refer to "a foolish or inept person as revealed by Google". This was meant to draw attention to the fact that this was not a "Google problem" but rather the result of an often unintentional misconfiguration on the part of a user or a program installed by the user. Over time, the term "dork" became shorthand for a search query that located sensitive information and "dorks" were included with many web application vulnerability releases to show examples of vulnerable web sites.

After nearly a decade of hard work by the community, Johnny turned the GHDB over to Offensive Security in November 2010, and it is now maintained as an extension of the Exploit Database. Today, the GHDB includes searches for other online search engines such as Bing, and other online repositories like GitHub, producing different, yet equally valuable results.

EXPLOIT DATABASE

☐ Verified ☐ Has App

Show 15

Date	D	A	V	Title	Type	Platform	Author
2022-02-02	↓		×	WordPress Plugin Learnpress 4.1.4.1 - Arbitrary Image Renaming	WebApps	PHP	Ceylan BOZOĞULLARINDAN
2022-02-02	↓		×	WordPress Plugin Post Grid 2.1.1 - Cross Site Scripting (XSS)	WebApps	PHP	0xb9
2022-02-02	↓		×	WordPress Plugin Product Slider for WooCommerce 1.13.21 - Cross Site Scripting (XSS)	WebApps	PHP	0xb9
2022-02-02	↓		×	WordPress Plugin Contact Form Check Tester 1.0.2 - Broken Access Control	WebApps	PHP	0xb9
2022-02-02	↓		×	PHP Unit 4.8.28 - Remote Code Execution (RCE) (Unauthenticated)	WebApps	PHP	souzo
2022-02-02	↓		×	Huawei DG8045 Router 1.0 - Credential Disclosure	WebApps	Hardware	Abdalrahman Gamal
2022-02-02	↓		×	Moodle 3.11.4 - SQL Injection	WebApps	PHP	lavclash75
2022-02-02	↓		×	PHP Restaurants 1.0 - SQLi (Unauthenticated)	WebApps	PHP	Nefrit ID
2022-02-02	↓		×	Wordpress Plugin 404 to 301 2.0.2 - SQL-Injection (Authenticated)	WebApps	PHP	Ron Jost
2022-02-02	↓		×	WordPress Plugin Domain Check 1.0.16 - Reflected Cross-Site Scripting (XSS) (Authenticated)	WebApps	PHP	Ceylan BOZOĞULLARINDAN
2022-02-02	↓		×	Fetch Softworks Fetch FTP Client 5.8 - Remote CPU Consumption (Denial of Service)	Local	macOS	LiquidWorm

Footprinting – Sources

- **Documentation**
 - Profile a target and record the results based on domain name, IP address, DNS servers, employee information, open ports, etc.
- **Organization's website**
 - Look for open-source information
- **Alternative websites**
 - Finding information related to an organization on other websites, for example, blogs of dissatisfied employees that could leak information
- **Job Boards**
 - Information can be obtained from job postings on company website or any other job websites
- **Databases**
 - Vast information available about publicly traded organizations in database
 - Eg: Companies House for UK, EDGAR for US, SEDAR for Canada etc...

The screenshot shows the homepage of the University of Wales Trinity Saint David. At the top, there is a dark blue navigation bar with links for NEWS, QUICK LINKS, and CYMRAEG, along with social media icons for Facebook, Twitter, and YouTube. Below this, a banner features the university's crest, name in Welsh and English, and a 200th anniversary logo (1822-2022). A main navigation menu includes links for STUDY, ABOUT, STUDENT LIFE, INTERNATIONAL, RESEARCH, and ALUMNI. A large hero image shows three students smiling. A white cookie consent pop-up is centered over the hero image, asking for permission to use cookies and providing links to the Privacy and Cookie Policy, with 'Accept all' and 'Adjust Cookie Settings' buttons. On the right side, a white Netcraft site report overlay is visible for the URL www.uwtsd.ac.uk. It shows a risk rating of 0, a site rank of 841,832, and various security details. A 'Report malicious URL' form is also present at the bottom of the report.

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Coronavirus - UWTSd Response and Recovery >>

STUDY ABOUT STUDENT LIFE INTERNATIONAL RESEARCH ALUMNI

VISIT US

BOOK AN OPEN

Using our website

We use cookies to understand how visitors use our website and to improve the user experience. For more information, please read our [Privacy and Cookie Policy](#).

Accept all

Adjust Cookie Settings

www.uwtsd.ac.uk

Site Report

Risk Rating: 0

Country:	UK	Site rank:	841,832
First seen:	May 2018	Host:	University o...
PFS:	✓	SSLv3:	Not supported

Disable protection for this site ☐

Report malicious URL:

The URL of the site: ☒
<https://www.uwtsd.ac.uk/>

Add a reason ☐

Your email address (to receive updates): ☒
you@example.com

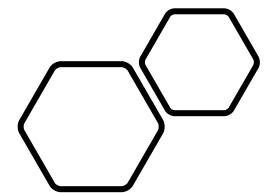
NETCRAFT

Submit Report

Footprinting – Tools

- Finding **Target's external URL**
- Sub-domains using tools like Netcraft, Sublist3r etc
- Google Earth, Google Maps, Wikimapia, National Geographic Maps, Bing Maps

➤ Sublist3r is a python script that enumerates subdomains across multiple sources at once.



Footprinting – Tools

- Finding **Individuals**
- Using Social networking services to get individual's information to perform social engineering attacks
- Facebook, Twitter, LinkedIn, YouTube etc.
- Sites like Intelius, BeenVerified, Spokeo etc
- Use Utilities like InSpy to enumerate LinkedIn and find people based on Job Title, company, or email address



HOME

CONTACT

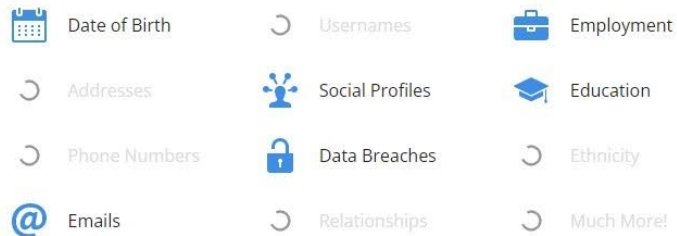
CUSTOMER SUPPORT
800-433-0567

LOGIN

56%

Searching for [REDACTED] in Wales

Checking...



Scanning Sources...

Blackwood Public Records Databases
Blaenau Ffestiniog Public Records Databases
Blaenavon Public Records Databases
Blaina Public Records Databases
Brecon Public Records Databases
Bridgend Public Records Databases
Briton Ferry Public Records Databases
Brynawr Public Records Databases
Buckley Public Records Databases
Builth Wells Public Records Databases

FEDERAL

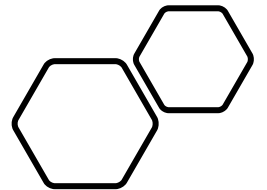
STATE

COUNTY

MUNICIPAL

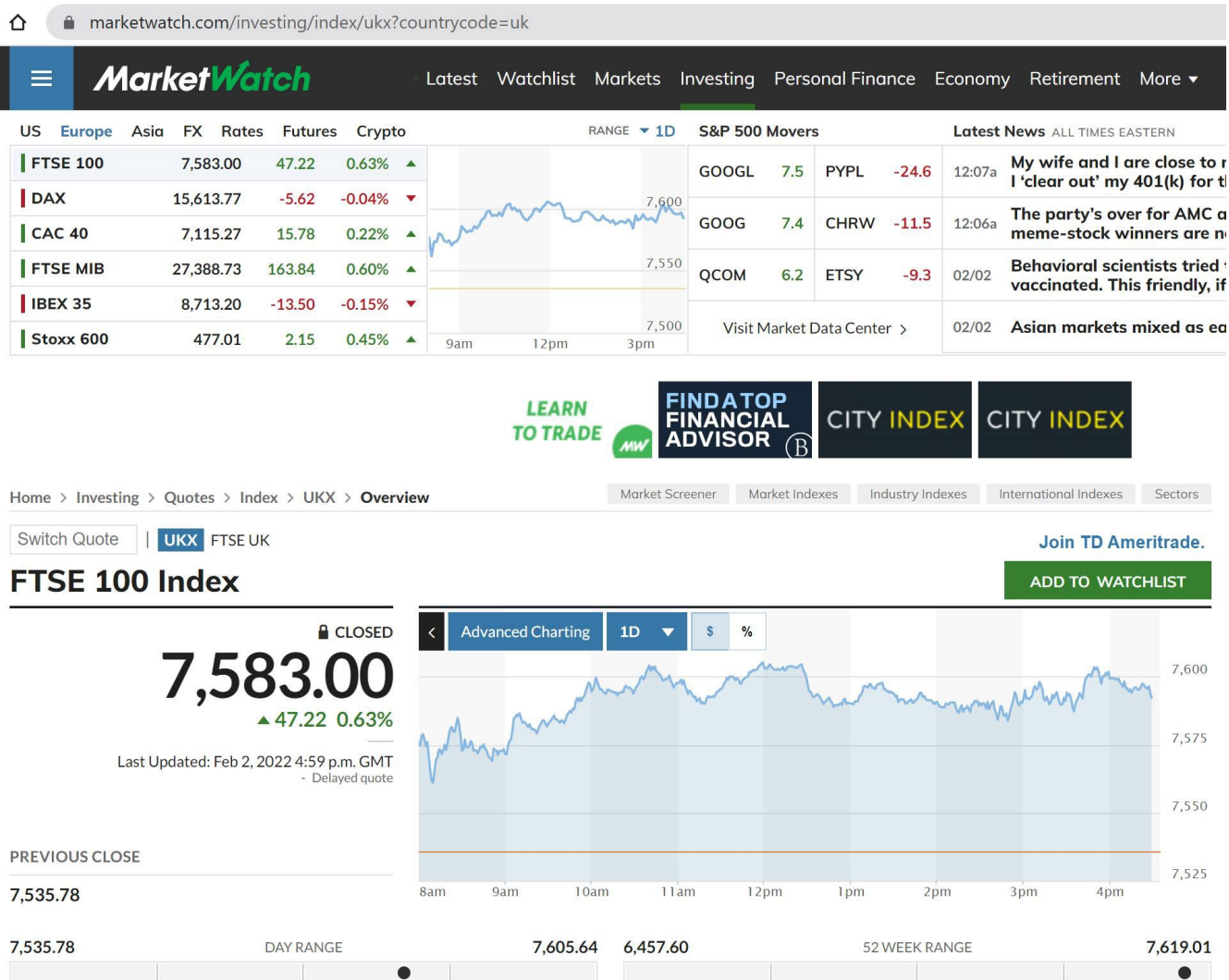


© COPYRIGHT 2022 INFOPAY, INC. ALL RIGHTS RESERVED.

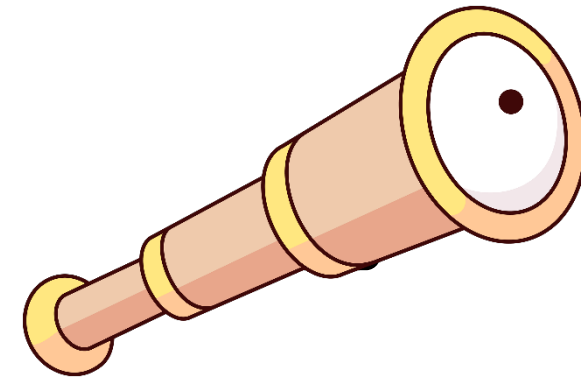


Footprinting – Tools

- Finding **Organisations**
- Using various available sources like financial services, Job Sites etc to collect information about organizations.

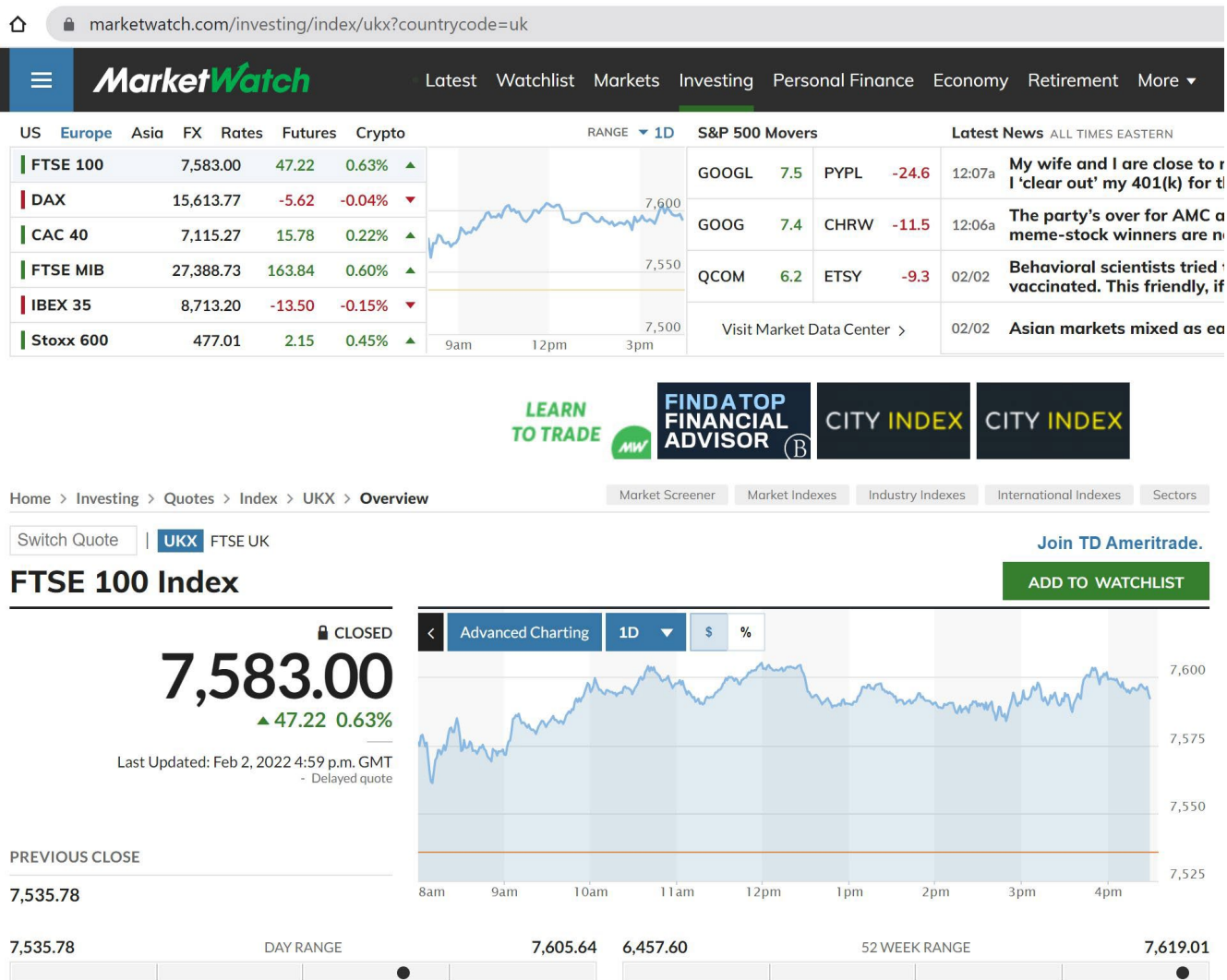


- Sites like MarketWatch helps you to gather information like market value, company shares, company profile, competitor details etc about the organization
- Sites like Indeed, linkedin helps you to gather information like companies' infrastructure, history etc

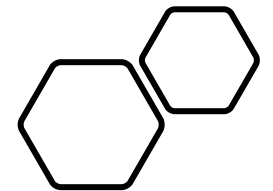


Footprinting – Tools

- Finding **Organisations**
- Using various available sources like financial services, Job Sites etc to collect information about organizations.



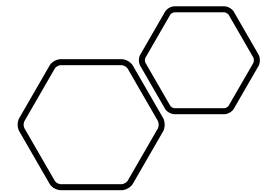
- Sites like MarketWatch helps you to gather information like market value, company shares, company profile, competitor details etc about the organization
- Sites like Indeed, linkedin helps you to gather information like companies' infrastructure, history etc



Footprinting – Tools

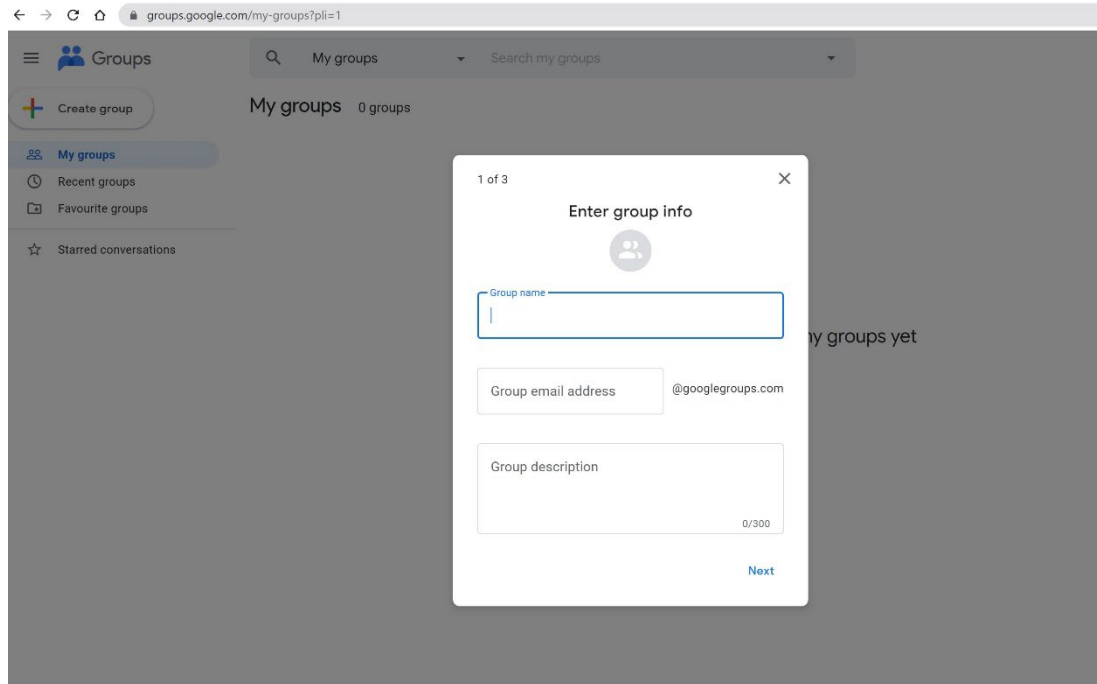
- Finding **Individuals**
- Using Social networking services to get individual's information to perform social engineering attacks
- Facebook, Twitter, LinkedIn, YouTube etc.
- Sites like Intelius, BeenVerified, Spokeo etc
- Use Utilities like InSpy to enumerate LinkedIn and find people based on Job Title, company, or email address

User Activity	Attackers View	Organizations Activity	Attackers View
Profile Maintenance	Contact Information, Location details etc	User Surveys	Business Strategies
Connect with People	Friend List, Information about friends etc	Promote Products	Product Profile
Share	Identify persons, interest etc	User Support	Social Engineering
Play	Interests	Recruitment	Platform/ Technology
Events (Birthday Parties etc)	Activities	Background Checks	Type of Business

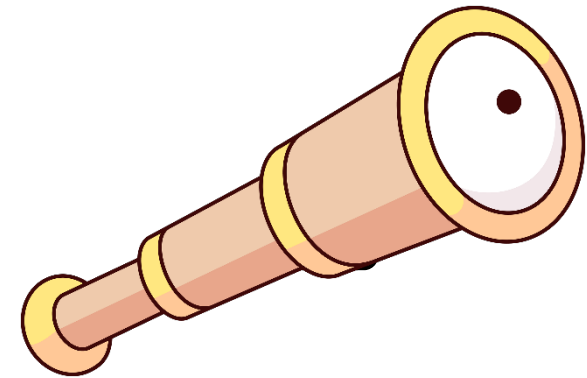


Footprinting – Tools

- Use Groups, Forums, blogs to gather information. Sometimes, you may be very lucky to gather sensitive information like network, system, personal information about target.



- Hackers use Fake Profiles to target organizations/ individuals



Information Gathering

Whois Record for ItsEcGAmes.com

Domain Profile

Registrant Org	MME BV
Registrant Country	be
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: https://www.godaddy.com , http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	3,544 days old Created on 2012-05-21 Expires on 2023-05-21 Updated on 2021-05-21
Name Servers	NS53.DOMAINCONTROL.COM (has 59,906,655 domains) NS54.DOMAINCONTROL.COM (has 59,906,655 domains)
Tech Contact	—
IP Address	31.3.96.40 - 6 other sites hosted on this server
IP Location	 Noord-holland - Amsterdam - XI Internet Services Amsterdam Network
ASN	 AS35470 XL-AS, NL (registered Nov 29, 2006)
Domain Status	Registered And Active Website
IP History	2 changes on 2 unique IP addresses over 10 years
Registrar History	3 registrars

Website

Website Title	 bWAPP, a buggy web application!
Server Type	Apache
Response Code	200
Terms	184 (Unique: 115, Linked: 13)
Images	10 (Alt tags missing: 10)
Links	17 (Internal: 5, Outbound: 12)

Whois Record (last updated on 2022-02-02)

Domain Name: itsecgames.com
Registry Domain ID: 1721761149_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: <https://www.godaddy.com>
Updated Date: 2021-05-22T06:49:34Z
Creation Date: 2012-05-21T08:35:16Z
Registrar Registration Expiration Date: 2023-05-21T08:35:16Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Domain Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>
Domain Status: clientRenewProhibited <https://icann.org/epp#clientRenewProhibited>
Domain Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>
Registrant Organization: MME BV
Registrant State/Province: West-Vlaanderen
Registrant Country: BE
Registrant Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=itsecgames.com>
Tech Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=itsecgames.com>
Admin Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=itsecgames.com>
Name Server: NS53.DOMAINCONTROL.COM
Name Server: NS54.DOMAINCONTROL.COM

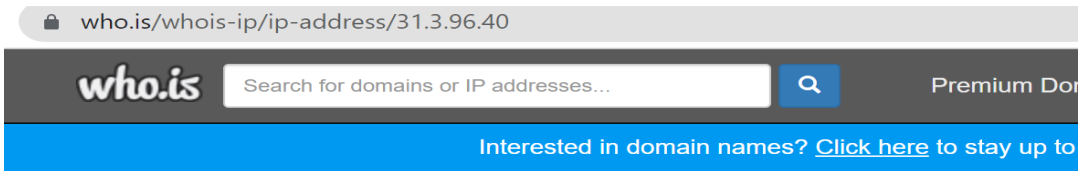
Footprinting – Tools

- With the basic information you have, let us now step up the next process.
- Find out available IP addresses for scanning and further enumeration.
- Locating the network range helps us in targeting more specific IP address to gather more information to scan and analysis.
- Tools/ Utilities like Whois, Traceroute etc could be used to determine the network range and its path.
- Tools like SHODAN, Censys, Netcraft could be used to gather information like IP addresses, hosting platform, the technology in use, about websites which are based on the target information



The screenshot shows the Shodan search engine interface. At the top, the search bar contains 'CISCO.COM'. Below the search bar, there are tabs for 'Shodan', 'Maps', 'Images', 'Monitor', 'Developer', and 'More'. The main content area displays search results for 'CISCO.COM'. On the left, there is a section for 'TOTAL RESULTS' showing '339' results. Below this, there is a 'TOP COUNTRIES' section with a world map and a list of countries: United States (229), Netherlands (14), Germany (13), United Kingdom (12), and Australia (7). Further down, there is a 'TOP PORTS' section with a list of ports: 443 (217), 80 (67), 25 (14), 3389 (5), and 8443 (5). On the right side of the results, there are two detailed entries. The first entry is titled '302 Found' and shows a redirect from '135.84.173.146' to 'https://135.84.173.146/'. The second entry is titled 'Not Found' and shows a '404 Not Found' response from '192.133.218.229'. Both entries include details about the server, date, content type, and organization.

Footprinting – Tools



31.3.96.40 address profile

Whois

Diagnostics

IP Whois

NetRange: 31.0.0.0 - 31.255.255.255
CIDR: 31.0.0.0/8
NetName: RIPE-31
NetHandle: NET-31-0-0-0-1
Parent: ()
NetType: Allocated to RIPE NCC
OriginAS:
Organization: RIPE Network Coordination Centre (RIPE)
RegDate:
Updated: 2010-05-18
Comment: These addresses have been further assigned to users in the RIPE NCC region. Contact information can be found in the RIPE database at <http://www.ripe.net/whois>
Ref: <https://rdap.arin.net/registry/ip/31.0.0.0>

ResourceLink: <https://apps.db.ripe.net/search/query.html>
ResourceLink: [whois.ripe.net](https://apps.db.ripe.net/search/query.html)

OrgName: RIPE Network Coordination Centre
OrgId: RIPE
Address: P.O. Box 10096
City: Amsterdam
StateProv:
PostalCode: 1001EB
Country: NL
RegDate:
Updated: 2013-07-29



Ref: <https://rdap.arin.net/registry/entity/RIPE>

ReferralServer: [whois://whois.ripe.net](https://apps.db.ripe.net/search/query.html)
ResourceLink: <https://apps.db.ripe.net/search/query.html>

OrgAbuseHandle: ABUSE3850-ARIN
OrgAbuseName: Abuse Contact
OrgAbusePhone: +31205354444
OrgAbuseEmail: abuse@ripe.net
OrgAbuseRef: <https://rdap.arin.net/registry/entity/ABUSE3850-ARIN>

OrgTechHandle: RNO29-ARIN
OrgTechName: RIPE NCC Operations
OrgTechPhone: +31 20 535 4444
OrgTechEmail: hostmaster@ripe.net
OrgTechRef: <https://rdap.arin.net/registry/entity/RNO29-ARIN>

Footprinting – Tools



```
PING 31.3.96.40 (31.3.96.40) 56(84) bytes of data.  
64 bytes from 31.3.96.40: icmp_seq=1 ttl=43 time=90.0 ms  
64 bytes from 31.3.96.40: icmp_seq=2 ttl=43 time=89.9 ms  
64 bytes from 31.3.96.40: icmp_seq=3 ttl=43 time=89.9 ms  
64 bytes from 31.3.96.40: icmp_seq=4 ttl=43 time=89.9 ms  
64 bytes from 31.3.96.40: icmp_seq=5 ttl=43 time=90.0 ms
```

```
--- 31.3.96.40 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4001ms  
rtt min/avg/max/mdev = 89.930/90.006/90.078/0.333 ms
```

Traceroute

```
traceroute to 31.3.96.40 (31.3.96.40), 30 hops max, 60 byte packets  
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.681 ms  0.686 ms  0.626 ms  
 2  216.182.226.38 (216.182.226.38)  357.190 ms  216.182.229.176 (216.182.229.176)  9.236 ms  216.182.229.172 (216.182.229.172)  8.366 ms  
 3  100.66.36.70 (100.66.36.70)  4.914 ms  100.66.9.54 (100.66.9.54)  16.851 ms  100.66.12.36 (100.66.12.36)  21.856 ms  
 4  100.66.38.98 (100.66.38.98)  20.068 ms  100.66.11.80 (100.66.11.80)  21.365 ms  100.66.11.222 (100.66.11.222)  20.004 ms  
 5  100.66.62.252 (100.66.62.252)  13.468 ms  241.0.4.192 (241.0.4.192)  1.245 ms  241.0.4.210 (241.0.4.210)  1.372 ms  
 6  240.0.40.18 (240.0.40.18)  1.303 ms  241.0.4.211 (241.0.4.211)  0.815 ms  240.0.40.22 (240.0.40.22)  0.788 ms  
 7  242.0.170.1 (242.0.170.1)  0.777 ms  240.0.40.29 (240.0.40.29)  0.672 ms  242.0.171.17 (242.0.171.17)  1.087 ms  
 8  52.93.28.173 (52.93.28.173)  1.473 ms  52.93.28.167 (52.93.28.167)  1.446 ms  52.93.28.197 (52.93.28.197)  1.380 ms  
 9  100.100.2.72 (100.100.2.72)  1.479 ms  100.100.4.74 (100.100.4.74)  1.344 ms  100.100.2.78 (100.100.2.78)  1.331 ms  
10  * 100.100.4.78 (100.100.4.78)  1.212 ms  100.100.2.76 (100.100.2.76)  1.205 ms
```

Footprinting – Tools

Background

Network

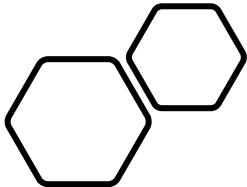
Site	http://www.itsecgames.com	Domain	itsecgames.com
Netblock Owner	XL Internet Services Amsterdam Network	Nameserver	ns53.domaincontrol.com
Hosting company	CloudVPS	Domain registrar	godaddy.com
Hosting country	NL	Nameserver organisation	whois.wildwestdomains.com
IPv4 address	31.3.96.40 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS35470	DNS admin	dns@jomax.net
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	web.mmebvba.com		

IP delegation

IPv4 address (31.3.96.40)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
31.0.0.0-31.255.255.255	Netherlands	RIPE-31	RIPE Network Coordination Centre
31.3.96.0-31.3.103.255	Netherlands	NL-SIGNET-20110408	Signet B.V.
31.3.96.0-31.3.96.255	Netherlands	XLIS-VPS30	XL Internet Services Amsterdam Network
31.3.96.40	Netherlands	XLIS-VPS30	XL Internet Services Amsterdam Network

```
C:\Windows\system32>nmap -n -vv -sn 31.3.96.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 13:49 India Standard Time
Initiating Ping Scan at 13:49
Scanning 31.3.96.40 [4 ports]
Completed Ping Scan at 13:49, 0.30s elapsed (1 total hosts)
Nmap scan report for 31.3.96.40
Host is up, received syn-ack ttl 49 (0.27s latency).
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
Raw packets sent: 4 (152B) | Rcvd: 1 (44B)
```

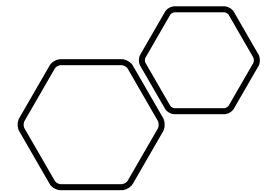


Footprinting – Tools

Port Scanning: The process of connecting to TCP and UDP ports to identify the services and applications that are running in the target device

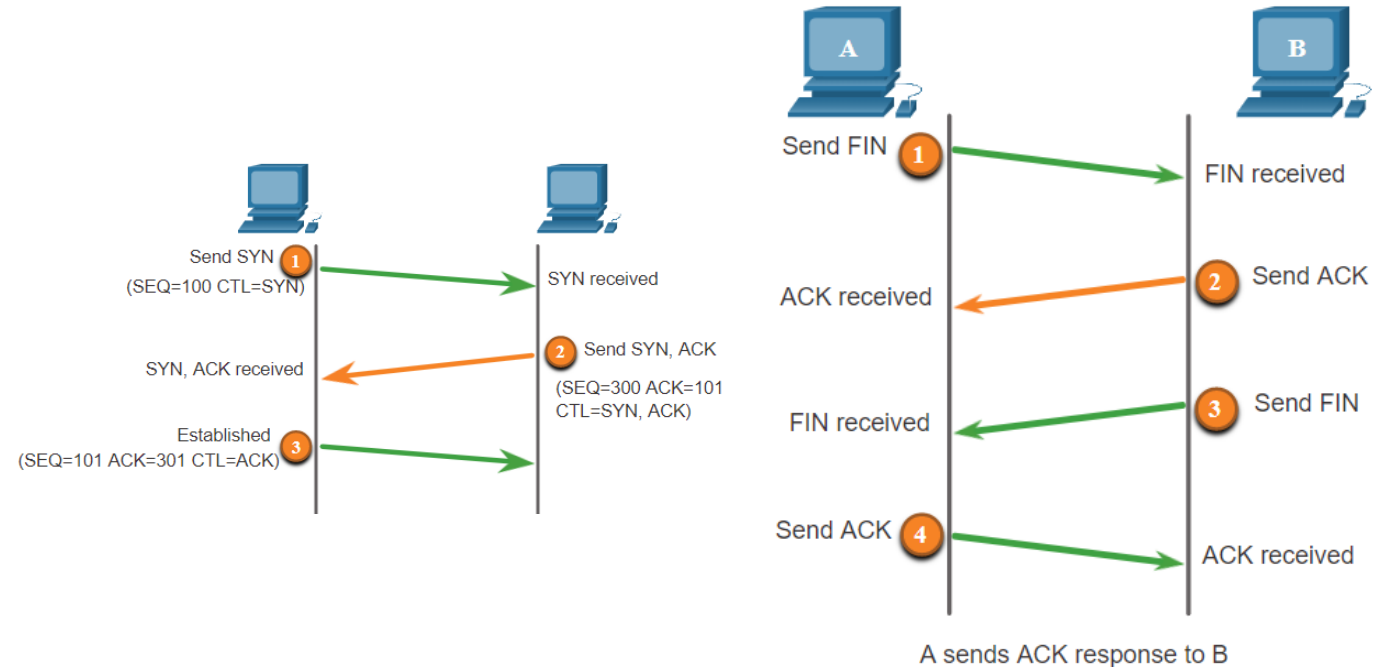
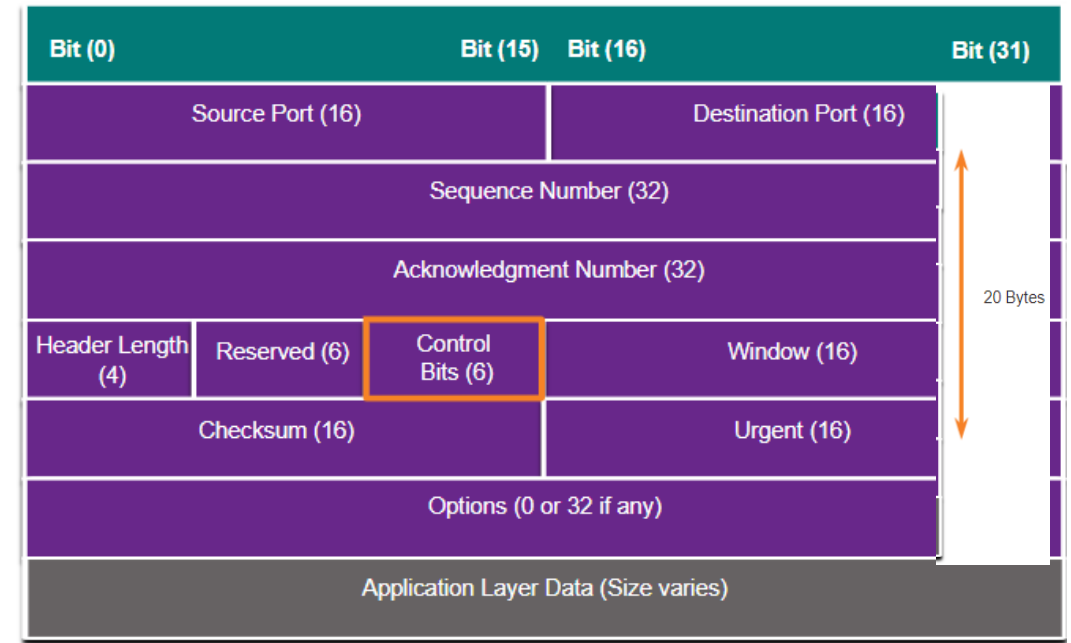
Common ports and protocols:

Port	Service	Protocol
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
161/162	SNMP	UDP
1433/1434	MSSQL	TCP



Footprinting – Tools

- **Port Scanning:** The process of connecting to TCP and UDP ports to identify the services and applications that are running in the target device
- TCP segment information appears immediately after the IP header. The fields of the TCP segment and the flags for the Control Bits field are displayed in the figure.
- The following are the six control bits of the TCP segment:
 - ✓ **URG** - Urgent pointer field significant
 - ✓ **ACK** - Acknowledgment field significant
 - ✓ **PSH** - Push function
 - ✓ **RST** - Reset the connection
 - ✓ **SYN** - Synchronize sequence numbers
 - ✓ **FIN** - No more data from sender



Footprinting – Tools

Port Scanning: The process of connecting to TCP and UDP ports to identify the services and applications that are running in the target device



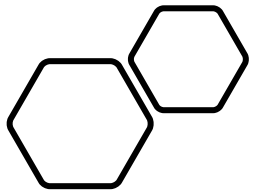
```
C:\Windows\system32>nmap www.itsecgames.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 14:34 India Standard Time
Nmap scan report for www.itsecgames.com (31.3.96.40)
Host is up (0.27s latency).
rDNS record for 31.3.96.40: web.mmebvba.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 22.64 seconds
```

Footprinting – Tools

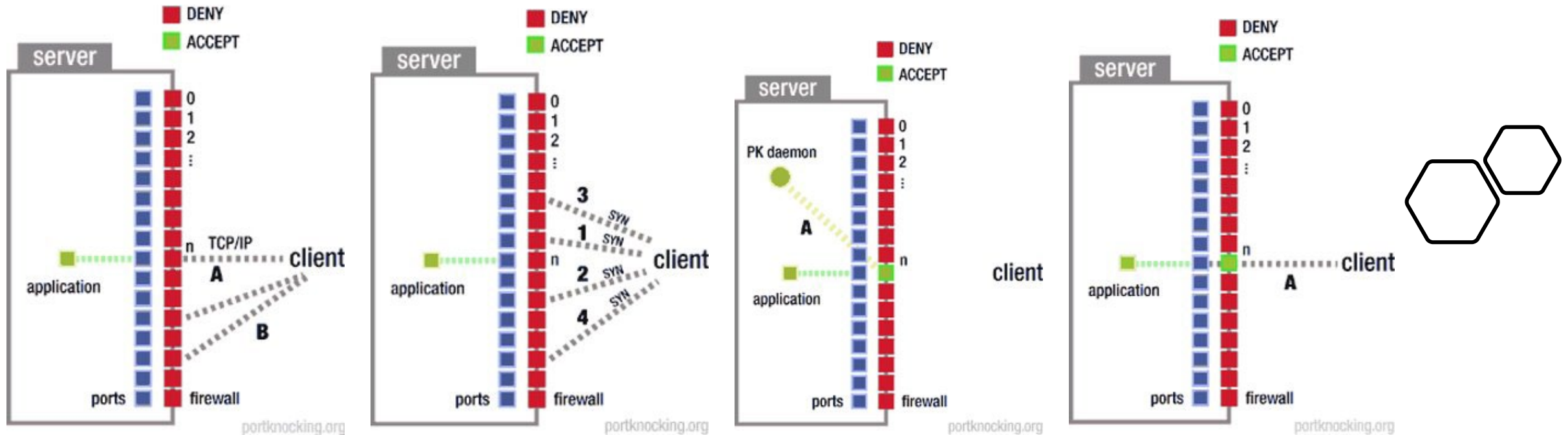
Port Knocking

- Open ports are most likely closed by Firewall.
- Port Knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports (*Wikipedia*).
- Pros: Attackers cannot easily identify open ports.
- Cons: This technique does not harden when someone with the ability to sniff the network traffic. Because, most likely they may be aware of appropriate knock sequence.



Footprinting – Tools

- (A) client cannot connect to application listening on port n;
- (B) client cannot establish connection to any port.
- (1,2,3,4) client connects to a well-defined set of ports in a sequence that contains an encrypted message by sending SYN packets;
- Client has a prior knowledge of the port knocking daemon and its configuration but receives no acknowledgement during this phase because firewall rules preclude any response.
- (A) server process (a port knocking daemon) intercepts connection attempts and interprets (decrypts and decodes) them as comprising an authentic "port knock";
- server carries out specific task based on content of port knock, such as opening port n to client.
- (A) client connects to port n and authenticates using applications regular mechanism.

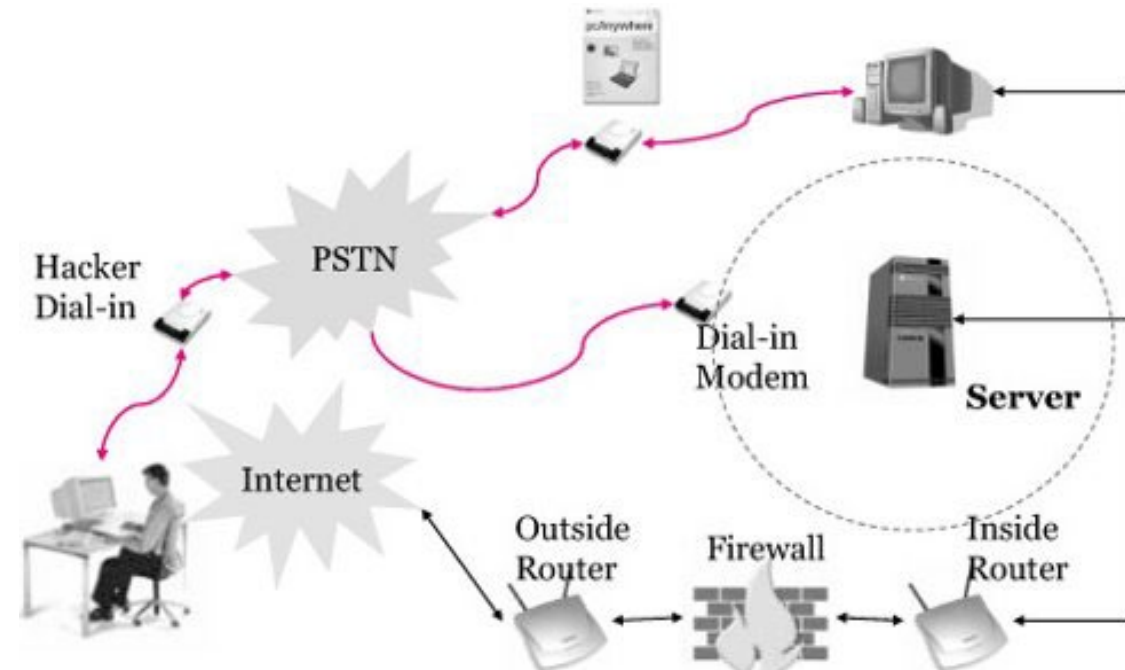


Footprinting – Tools

There is also the possibility of using war dialing programs to find ways around an organization's firewall. If the organization is located close by, the attacker might war drive the area to look for open access points.

WAR Dialing

- War dialing is the act of **using a modem and software to scan for other systems with modems attached.**
- Modems are a tempting target for hackers because they offer them the opportunity to bypass the corporate firewall.
- A modem can be seen as a backdoor into the network.
- The goal of war driving is to identify open or rogue access points
- Unsecured wireless access points can be a huge threat to any organization
- Employees could have installed their own access points without the company's permission.
- Unsecured wireless access points can be a danger offering a way into the network bypassing the firewall.



Footprinting – Tools

Website Footprinting: Monitoring and analyzing the target organizations website.

Look for

- Software used and its version
- Operating System and Scripting Platform
- Sub-directories and parameters
- Filename, Path, Database fields, query
- Contact Details of Web Developer/ Admin
- Source Code Comments

Tools/ Utilities like Burp Suite, Zaproxy, Firebug, Website Informer etc could help in additional information like

Connection Status, Content-type, Last Modified Information, Web Server and its version etc.

The screenshot displays the Burp Suite Professional website. The main heading is "Burp Suite Professional" in orange, followed by "Faster, more reliable security testing" in white. Below this is the tagline "The leading toolkit for web security testing." and two buttons: "TRY FOR FREE" and "BUY - £319".

On the right side, there are several overlapping panels representing different tools in the suite:

- Burp Scanner:** Shows a "Scan Type" dropdown with "Crawl and audit" selected, and a list of "URLs to Scan".
- Issue type:** A list of detected issues, including "Suspicious input transformation (reflected)", "SMTP header injection", "Serialized object in HTTP message", "Cross-site scripting (DOM-based)", "XML external entity injection" (highlighted), "External service interaction (HTTP)", "Web cache poisoning", "Server-side template injection", and "SQL injection".
- Poll Collaborator interactions:** A table showing a list of interactions with columns for ID, Time, and details. The table has 4 rows, all dated 2020-May-28 at 10:54:39 UTC.
- Payload Positions:** A diagram showing the positions of various payloads (blue and red bars) and a "Start attack" button.
- Burp Intruder:** A panel showing an "Attack type" dropdown set to "Cluster bomb" and buttons for "Add", "Clear", "Auto", and "Refresh".
- Burp Collaborator:** A panel with a "Poll every" input set to 60 seconds and a "Poll now" button.

WEB DATA EXTRACTOR

Automatically extract specific information from web pages

Home

Products

Purchase

Help

Modules

FAQ

WEB DATA EXTRACTOR PRO (NEW RELEASE 2022)

Main Features:

- ✓ Completely new powerful spidering
- ✓ Completely reworked UI - slick & se
- ✓ Pro version of WDE doesn't have an
- ✓ sites, gigabytes of data
- ✓ Extremely fast search and accurac
- ✓ Extract any data you want by Cust
- ✓ Support of working with proxy serv
- ✓ New session management allows y
- ✓ Brand new simplified user interface
- ✓ Unicode support

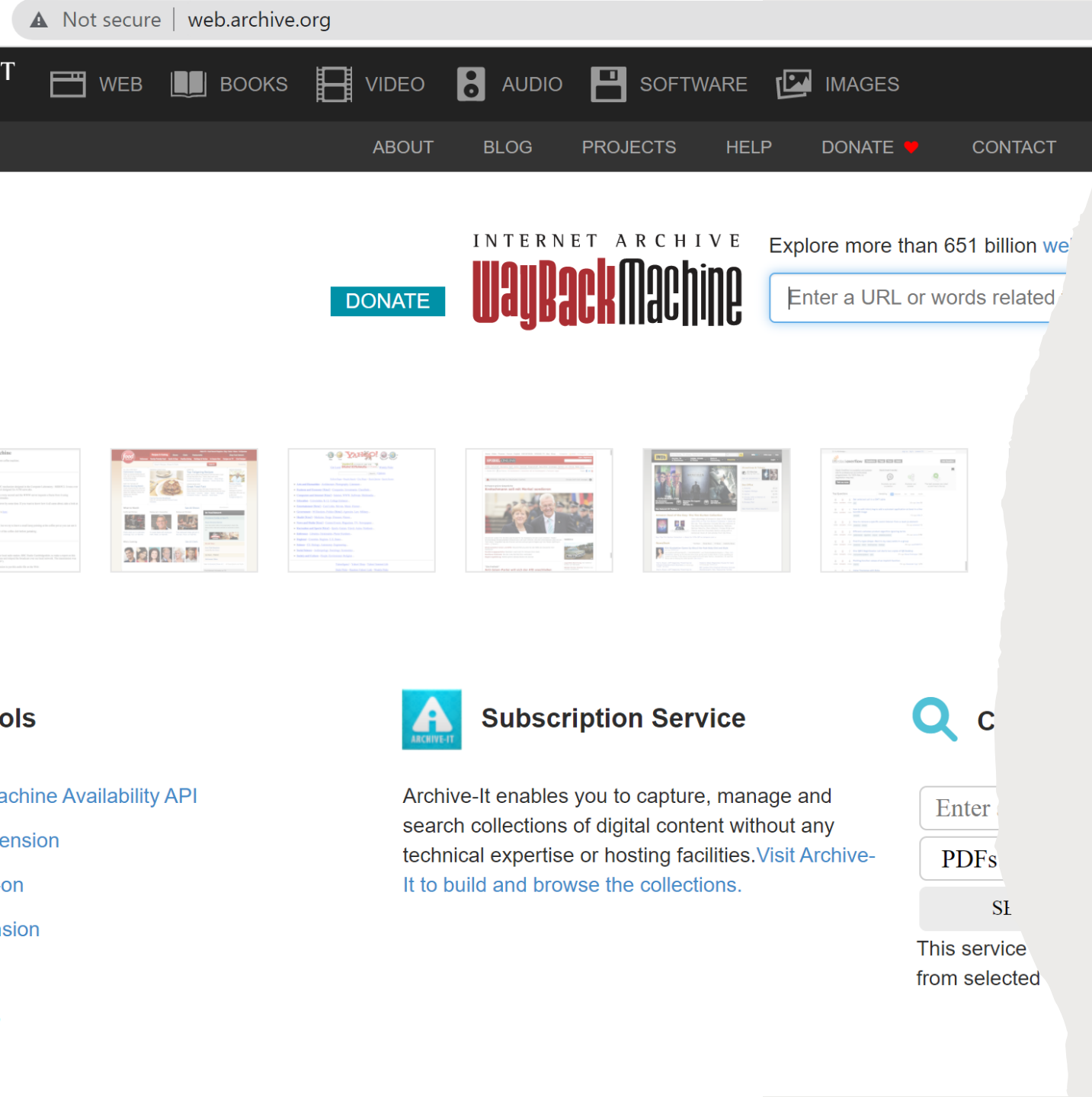
DOWNLOAD

P



Footprinting – Tools

- **Web Spiders** perform automated searches on the target website and collect specific information like employee name, email etc.
 - Tools like SpiderFoot, Visual SEO Studio, Wildshark SEO Spider Tool etc
- Web Data Extractor is another tool which could automatically extract specific information from web pages.
- HTTrack Website Copier



Footprinting – Tools

- Internet Archive's WAYBACK Machine allows to visit archived versions of websites
- Useful information may reside on the target organization's website in the form of PDF Documents, Word Files etc.
- Attackers use metadata and hidden information to do SE attacks
- Metagoogil extracts metadata of public documents

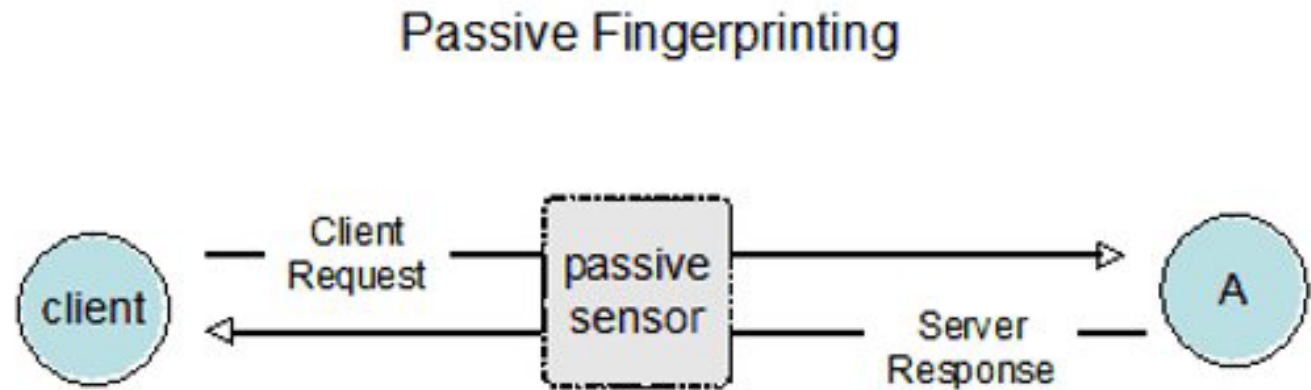
Footprinting – Tools

So far, IP Addresses, Live systems, Open Ports are identified. Next step is to identify the Operating System.

- To identify, an attacker uses passive fingerprinting or active fingerprinting. Although active fingerprinting is more accurate, it is not as stealthy as passive fingerprinting.

Passive OS Fingerprinting

- Passive fingerprinting is sniffing packets as they come by. These packets are examined for certain characteristics that can be pointed out to determine the OS.
 - Eg: IP TTL value, TCP Window Size, IP DF Option, IP Type of Service (TOS) Option, etc.



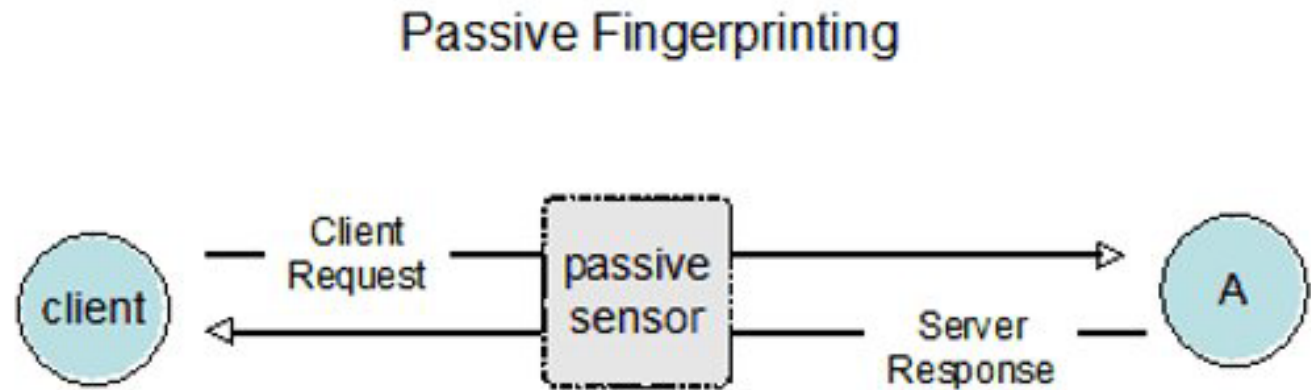
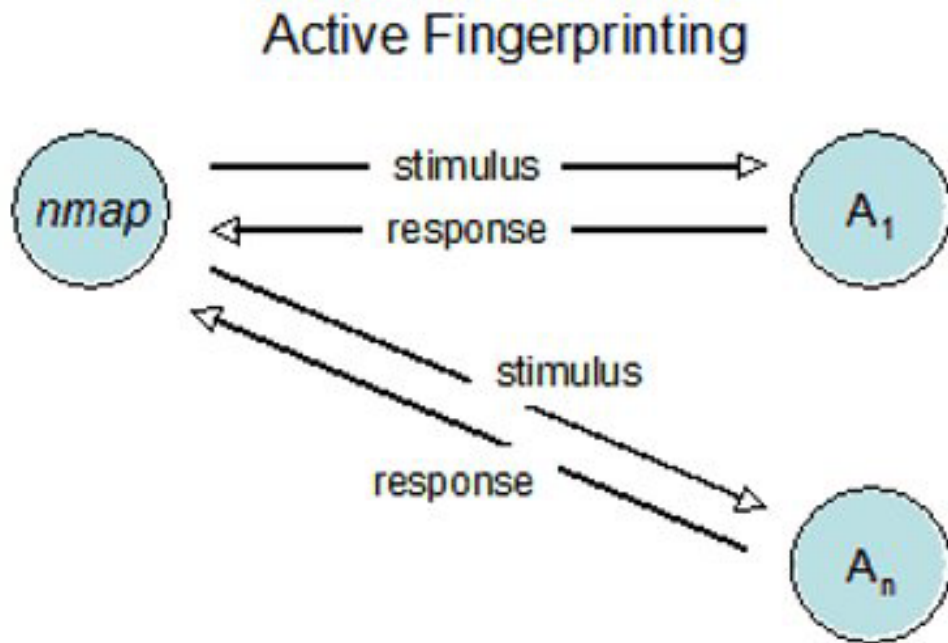
Footprinting – Tools

So far, IP Addresses, Live systems, Open Ports are identified. Next step is to identify the Operating System.

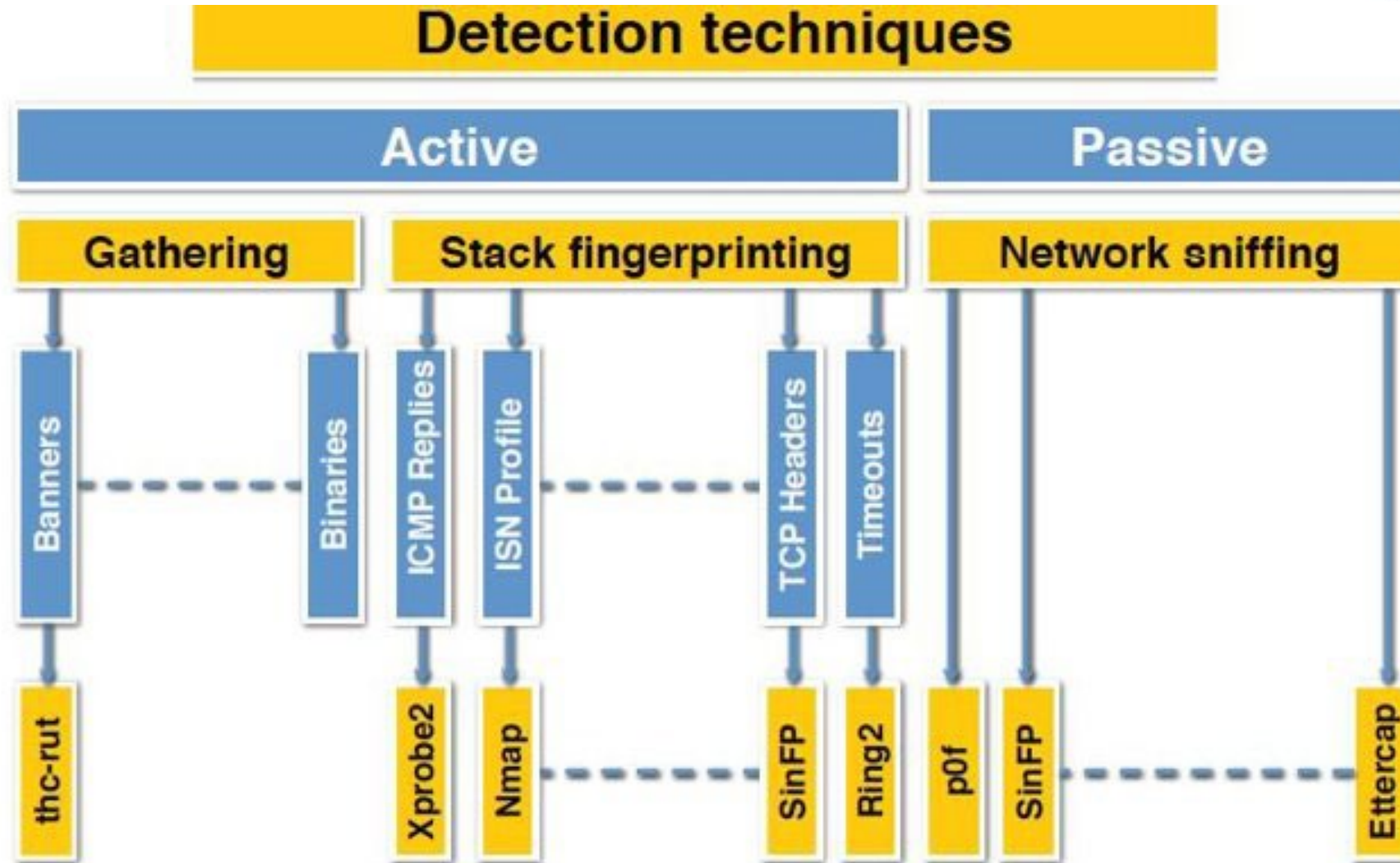
- To identify, an attacker uses passive fingerprinting or active fingerprinting. Although active fingerprinting is more accurate, it is not as stealthy as passive fingerprinting.

Active OS Fingerprinting

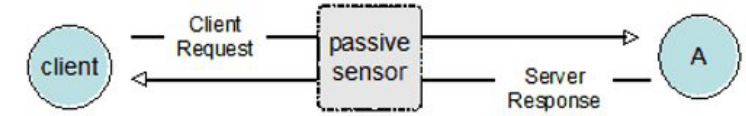
- The attacker injects packets into the network. This makes active fingerprinting good chance for being discovered or noticed. More powerful than passive fingerprint scanning because the hacker doesn't have to wait for random packets.



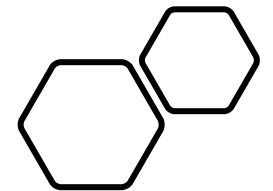
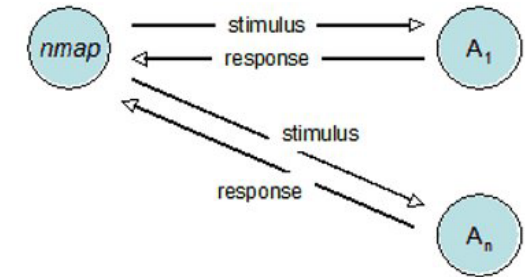
Footprinting – Tools



Passive Fingerprinting



Active Fingerprinting

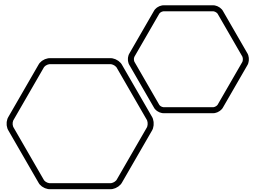


Footprinting – Tools

So far, IP Addresses, Live systems, Open Ports, Operating System are identified. Next step is to clarify any doubts about the target system.

Key Points to Note:

- Know the services running on specific ports. This will allow you to formulate and launch application specific attacks.
- Know the common default ports and services. This will help you ensure success at this pre-attack stage.
- A certain amount of default information and behavior can be obtained from any system. Just because a port is active or a known banner is returned, it is not certain that the information is correct. **Ports and banners can be changed and assumptions by themselves can be dangerous.**
- Banner Grabbing could be used to determine the services associated with the open ports. This will give information about the type & version of software running.



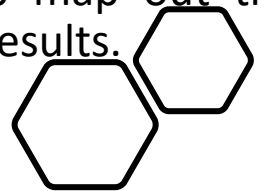
Footprinting – Mapping

Mapping the network provides the attacker a blueprint of the target's infrastructure.

- Manual Mapping - The information matrix formed using the previous steps must help you to collect the following details, using which a logical mapping of the network can be created manually with the gathered information to plan further activities.

Domain name info	IP addresses	DNS Servers	Employee info	Company location	Phone numbers	Yearly earnings
Recently acquired organizations	Email addresses	Publicly available IP address range	Open ports	Wireless access points	Modem lines	Banner details

- Automated Mapping - Visual traceroute programs, such as Path Analyzer Pro and VisualRoute are used for automated network mapping. Running traceroute to different servers such as web, email, and FTP can help map out the placement of these servers. Automatic mapping can be faster but might sometimes provide erroneous results.



Footprinting – Tools

STEP	TITLE	ACTIVE/PASSIVE	COMMON TOOLS
One	Information Gathering	Passive	ARIN, IANA, Whois, Nslookup
Two	Determining Network Range	Passive	RIPE, APNIC, Shodan.io, Traceroute, Netcraft
Three	Identify Active Machines	Active	Traceroute, SuperScan, Angry IP Scanner, Hping3
Four	Finding Open Ports and Applications	Active	Nmap, SuperScan, Solarwinds Port Scanner
Five	OS Fingerprinting	Active/Passive	Nmap, P0f, Xprobe2, ettercap, NetworkMiner
Six	Fingerprinting Services	Active/Passive	Telnet, FTP, Netcat, Satori
Seven	Mapping the Network	Active	Traceroute, VisualRoute, Path Analyzer Pro

Self Learning Exercise

Consider one of the following vulnerable, open-source test-base websites and perform footprinting

- <https://sudocyber.net/>
- <http://www.itsecgames.com/>
- <https://ctflearn.com>
- <https://damnvulnerableiosapp.com>
- <https://dvwa.co.uk>
- <https://defendtheweb.net/dashboard>
- <https://hack.me>
- <https://www.hackthebox.com>
- <https://hackthissite.org>

Gather Information: *Whois DomainTools* can be used to gain required information.

Determining Network range: The IP address obtained previously can be used in Whois IP lookup and Traceroute to determine the path

Identifying Active machines: Tools like Nmap, Pinger, Hping3, Super Scan, Angry IP scanner, WS_Ping_ProPack can be used for identifying active machines

Finding open ports and access points: Nmap can also be used for scanning for open ports

The above information gathered will give a good idea of the target system. Complete and Record your reflection!!!



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Any Questions?

*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

References

- EC-Council CEH
- Cisco Networking Academy
- Tevel Cyber Corps
- Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd edition
- Wikipedia
- Other website sources given in this presentation
- * The intension of usage is for Educational Purpose Only

***Advanced Cybersecurity
(ACCB6000)***

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Scanning Networks & Enumeration



*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Previous sessions...

- **Understanding Information Security, Risks involved, assessing, managing and monitoring Risks, Cyber risk resilience**
- **Purpose and role of Hackers, Penetration Testing, Various Laws and Standards**
- **Understanding Footprinting and Reconnaissance Concepts, Methodology.**
- **Using various Tools, Taking Countermeasures**

Lab/ Tutorials

- **Activity 1: Download and Setup your Lab.**
- **Coursework Description.**

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

So far, we discussed about Information security, the threats and attack vectors. In continuation to that, I hope you all have understood the hacking concepts and the reasons to stay ethical. Add more insight, we also discussed various security laws and standards. To conclude, we covered various “Risk” concepts like risk factors, cyber risk resilience in the process of enhancing security.

In continuation, we discussed Footprinting concepts focusing on different methodologies like Search Engines, Google Hacking Techniques etc. giving a walkthrough on Website Footprinting, Email Footprinting, Competitive Intelligence, Network Footprinting etc.

During the tutorials, under isolated lab environment we used different Footprinting tools to understand the countermeasures and pen testing attacks.



Scanning and Enumeration

- Network Scanning
- Tools and Techniques
- Banner Grabbing
- Scanning – PenTesting
- Enumeration
 - Concepts
 - Techniques
 - Countermeasures

Lab/Tutorials

- Activity 2 – Information Gathering

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

During this week, with applied knowledge and understanding on Footprinting, let us focus on Network Scanning, different tools and methodologies used etc. We shall also understand the concept of Banner Grabbing and scanning Penetration testing. we shall move ahead focusing on enumeration concepts, its different tools and techniques etc

During the tutorials, under isolated lab environment you will be using different tools to scan a network and understand the outcomes.

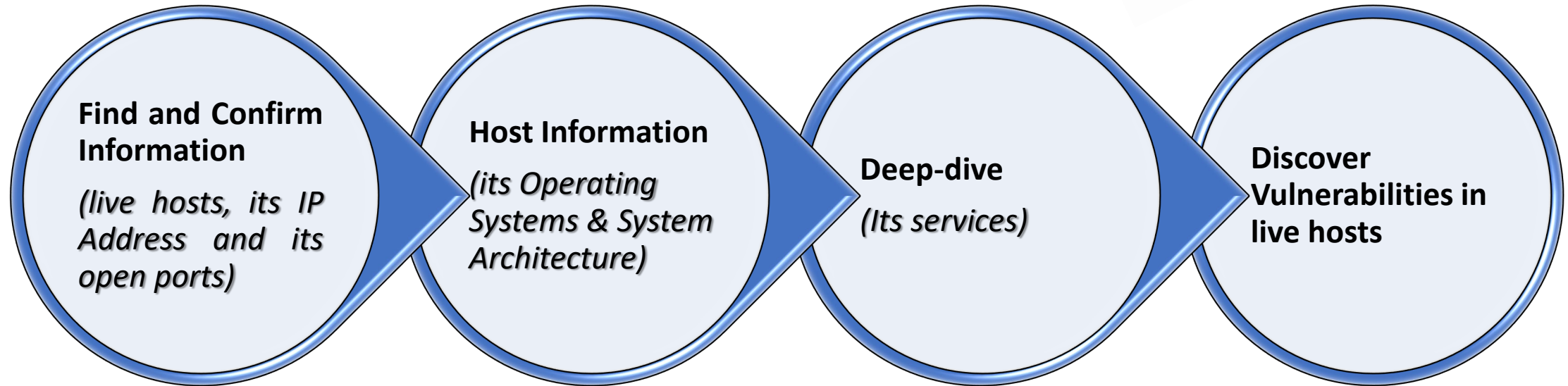
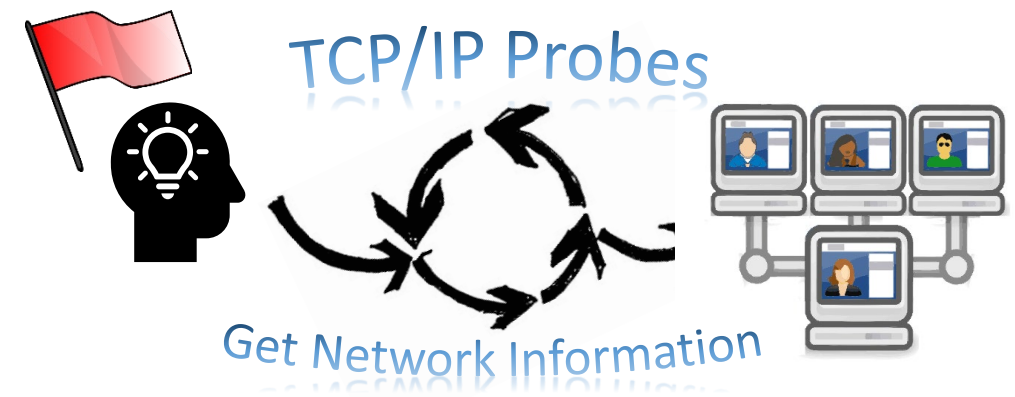
Scanning Networks

- Like, **Reconnaissance** is the method of collecting information about a target system without alerting it, also known as **Footprinting**, it is the first step in any form of hacking.
- It will help in understanding the target system and identify potential attack vectors & vulnerabilities
- **Network scanning** is the next process which helps in identifying hosts, ports and services in the network.
- Network scanning could be done using a set of procedures.
- It is **one of the components of intelligence gathering** that can be used by attackers to gather information and create a profile of their targets.



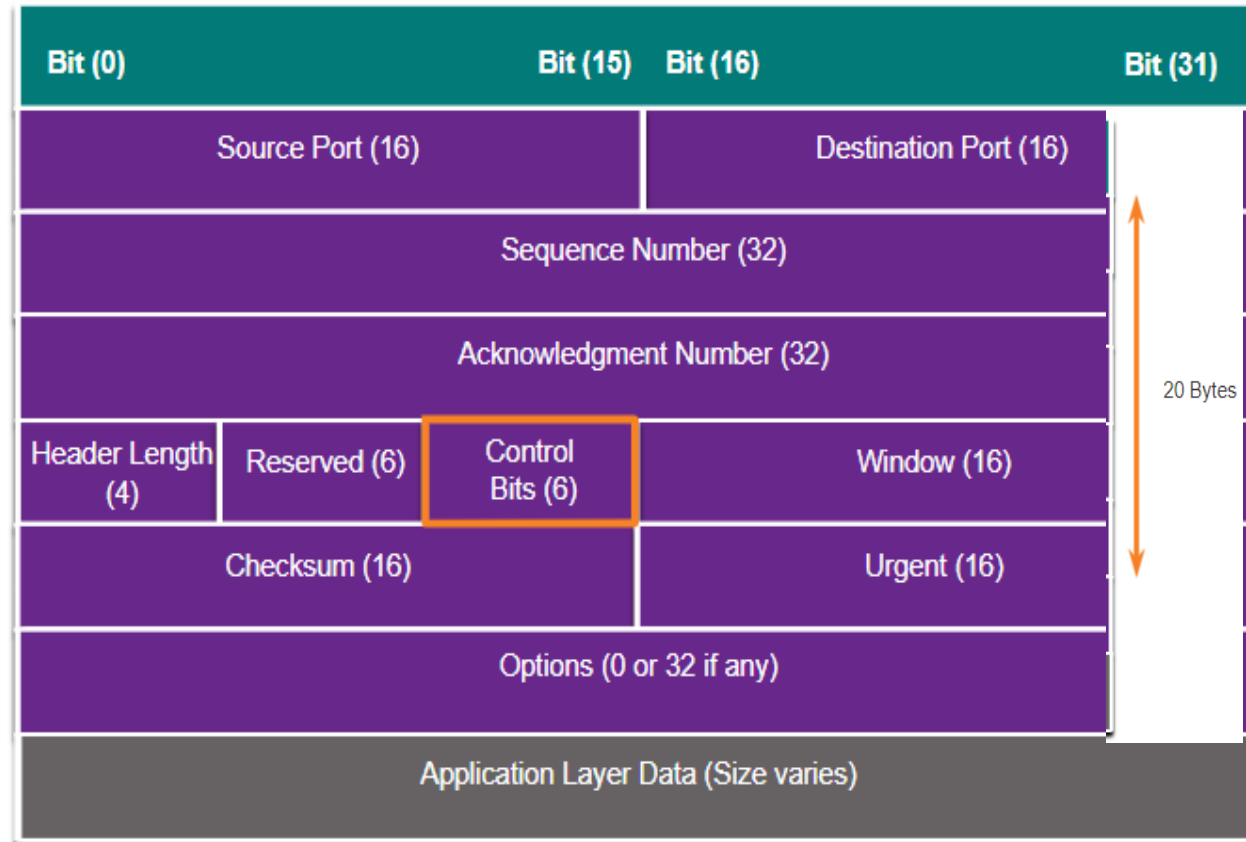
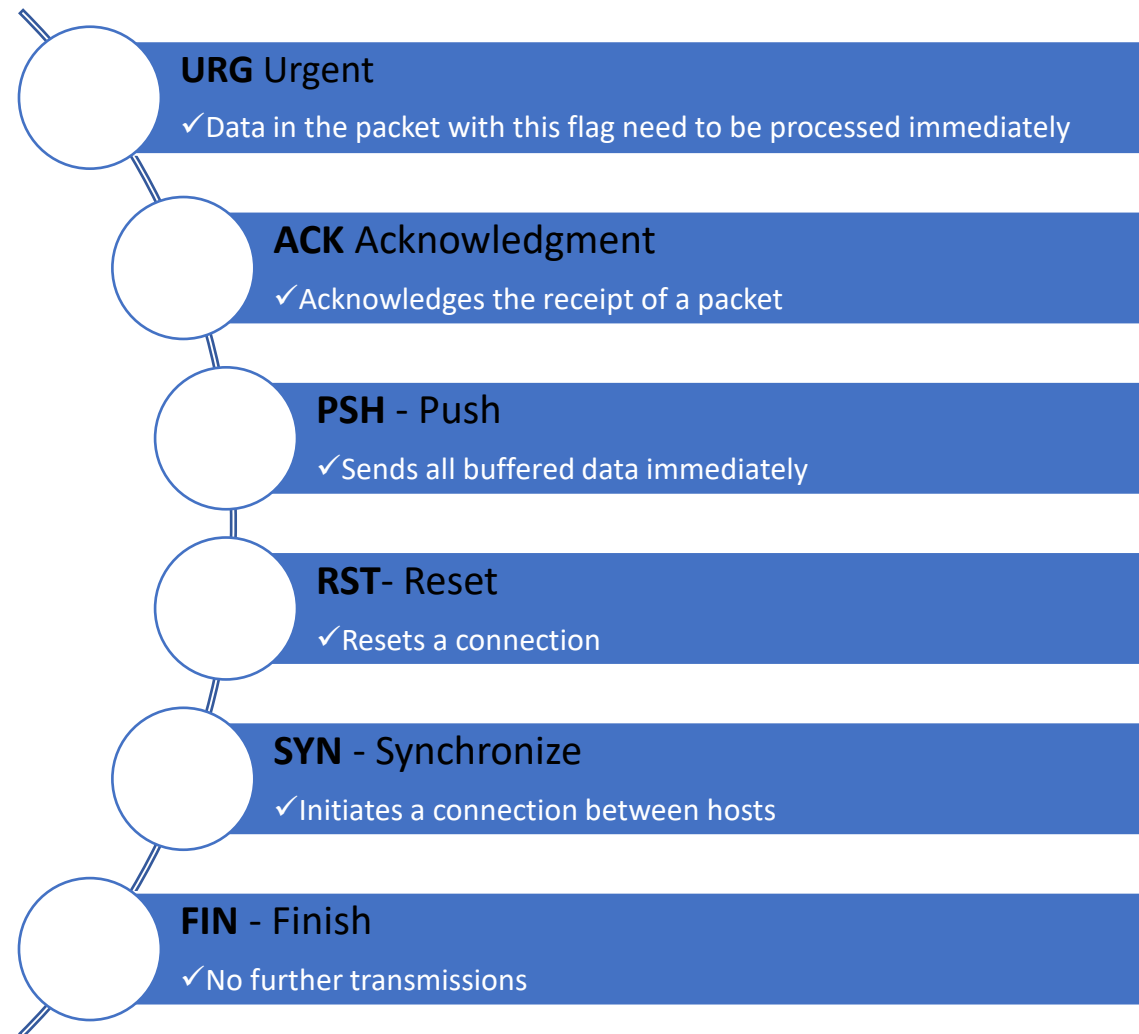
Scanning Networks

- The main objectives of network scanning



Scanning Networks – TCP Communication Flags

Earlier, we discussed about TCP Control Bits, As we know, TCP segment information appears immediately after the IP header.



Scanning Networks – TCP Communication Flags

URG Urgent

✓ Data in the packet with this flag need to be processed immediately

ACK Acknowledgment

✓ Acknowledges the receipt of a packet

PSH - Push

✓ Sends all buffered data immediately

RST- Reset

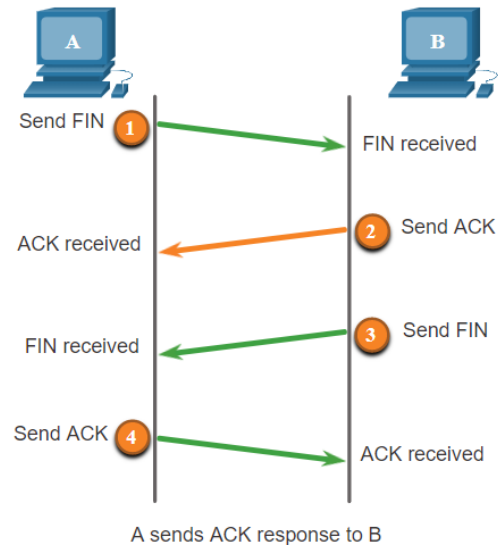
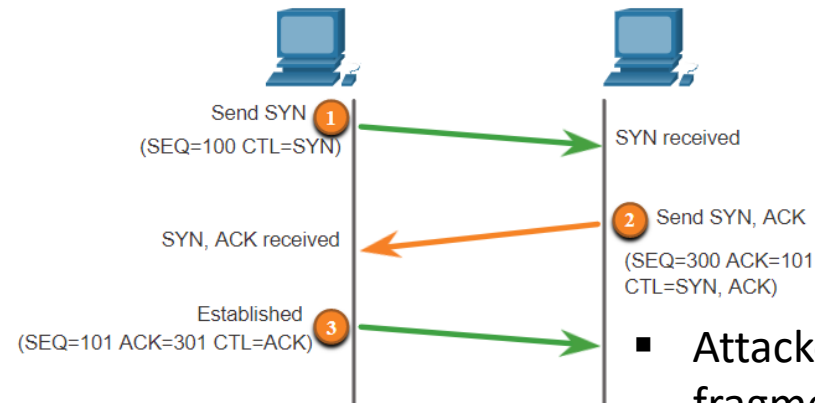
✓ Resets a connection

SYN - Synchronize

✓ Initiates a connection between hosts

FIN - Finish

✓ No further transmissions



- Attackers can also create fragmented packets to bypass security systems like firewalls, IDS/IPS.

- Packet Crafting Tools like NetScan Tools Pro, OSTINATO, LANforge FIRE etc can be used.

- Colasoft Packet Builder enables the creation of custom network packets to audit networks for various attacks

Scanning Networks – IPv6

- Structure of IPv6 is comparatively sophisticated and secured with more levels of addressing hierarchy.
- Focusing on Traditional network scanning Techniques for IPv6 networks brings in complex situation due to its larger subnets.
- So, scanning IPv6 networks involve more techniques rather than using the traditional network scanning tool, as most of the scanning tools do not support ping sweeps on IPv6 networks.
- Need to look into the network traffic, recorded logs, header lines etc to get information about IPv6 addresses.
- However, if successfully scanned, the IPv6 networks gives more privileges. Eg: Compromising One host in the subnet can help in probing all other hosts using “all hosts” and “link-local multicast addresses”

Scanning Networks: Tools

Many tools are available

NMAP

- Purpose of Nmap is to gather Network inventory, managing service upgrade schedules, monitoring hosts, its service uptime etc.
- Nmap can be also used to get live host, its services like application name, version, packet filters, firewalls, operating systems, its versions etc

```
(kali@kali)~$ nmap -p 1-65535 -T4 -A -v 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 08:08 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating Ping Scan at 08:08
Scanning 10.10.10.16 [2 ports]
Completed Ping Scan at 08:08, 2.00s elapsed (1 total hosts)
Nmap scan report for 10.10.10.16 [host down]
NSE: Script Post-scanning.
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.38 seconds
```

```
(kali@kali)~$ nmap -p 1-65535 -T4 -A -v 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 08:09 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating Ping Scan at 08:09
Scanning 10.10.10.16 [2 ports]
Completed Ping Scan at 08:09, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:09
Completed Parallel DNS resolution of 1 host. at 08:09, 0.03s elapsed
Initiating Connect Scan at 08:09
Scanning 10.10.10.16 [65535 ports]
Discovered open port 80/tcp on 10.10.10.16
Discovered open port 139/tcp on 10.10.10.16
Discovered open port 135/tcp on 10.10.10.16
Discovered open port 445/tcp on 10.10.10.16
Discovered open port 2107/tcp on 10.10.10.16
Discovered open port 5985/tcp on 10.10.10.16
Connect Scan Timing: About 23.02% done; ETC: 08:11 (0:01:44 remaining)
Connect Scan Timing: About 58.59% done; ETC: 08:11 (0:00:43 remaining)
Discovered open port 2103/tcp on 10.10.10.16
Discovered open port 49667/tcp on 10.10.10.16
Discovered open port 49668/tcp on 10.10.10.16
Discovered open port 2105/tcp on 10.10.10.16
Discovered open port 1801/tcp on 10.10.10.16
Completed Connect Scan at 08:10, 89.30s elapsed (65535 total ports)
Initiating Service scan at 08:10
Scanning 11 services on 10.10.10.16
Service scan Timing: About 54.55% done; ETC: 08:12 (0:00:41 remaining)
Completed Service scan at 08:11, 53.65s elapsed (11 services on 1 host)
NSE: Script scanning 10.10.10.16.
Initiating NSE at 08:11
Completed NSE at 08:12, 40.18s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 0.03s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 0.00s elapsed
Nmap scan report for 10.10.10.16
Host is up (0.0016s latency).
Not shown: 65524 filtered tcp ports (no-response)
```

```
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 10.0
|_ http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1801/tcp  open  msmq?
2103/tcp  open  msrpc            Microsoft Windows RPC
2105/tcp  open  msrpc            Microsoft Windows RPC
2107/tcp  open  msrpc            Microsoft Windows RPC
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
49667/tcp open  msrpc            Microsoft Windows RPC
49668/tcp open  msrpc            Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: o:microsoft:windows

Host script results:
|_ smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: SERVER2016, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:1d:c0:ef (VMware)
|_ Names:
|   WORKGROUP<00>          Flags: <group><active>
|   SERVER2016<00>        Flags: <unique><active>
|   SERVER2016<20>        Flags: <unique><active>
|_ smb2-security-mode:
|   3.1.1:
|_ Message signing enabled but not required
|_ smb2-time:
|   date: 2022-02-12T13:11:43
|_ start_date: 2022-02-12T13:08:51

NSE: Script Post-scanning.
Initiating NSE at 08:12
Completed NSE at 08:12, 0.00s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 0.00s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.78 seconds
```



Scanning Networks: Tools

Hping3

- *It is a command line network scanning and packet crafting tool focusing on TCP/IP protocol*
- *It can be used for*
 - *Auditing network security*
 - *Testing Firewall*
 - *manual path MTU discovery*
 - *Advanced traceroute,*
 - *Remote OS Fingerprinting*
 - *Remote uptime guessing*
 - *TCP/IP stacks auditing etc*

```
# hping3 --help
usage: hping3 host [options]
  -h --help      show this help
  -v --version   show version
  -c --count     packet count
  -i --interval  wait (uX for X microseconds, for example -i u1000)
                  --fast      alias for -i u10000 (10 packets for second)
                  --faster    alias for -i u1000 (100 packets for second)
                  --flood     sent packets as fast as possible. Don't show replies.
  -n --numeric   numeric output
  -q --quiet     quiet
  -I --interface interface name (otherwise default routing interface)
  -V --verbose   verbose mode
  -D --debug     debugging info
  -z --bind      bind ctrl+z to ttl (default to dst port)
  -Z --unbind    unbind ctrl+z
                  --beep      beep for every matching packet received

Mode
  default mode   TCP
  -0 --rawip     RAW IP mode
  -1 --icmp      ICMP mode
  -2 --udp       UDP mode
```

```
(root@ SC-205-03) - [/home/ethical]
# hping3 --traceroute -V -1 www.itsecgames.com
using eth0, addr: 172.17.226.155, MTU: 1500
HPING www.itsecgames.com (eth0 31.3.96.40): icmp mode set, 28 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=172.17.224.1 name=SC-205-03.mshome.net
hop=1 hoprtt=19.8 ms
hop=2 TTL 0 during transit from ip=192.168.1.1 name=ttrouter
hop=2 hoprtt=19.6 ms
hop=3 TTL 0 during transit from ip=78.144.1.17 name=ae54-ner001.csm.as13285.net
hop=3 hoprtt=19.6 ms
hop=4 TTL 0 during transit from ip=78.144.1.48 name=ae56-scr001.slh.as13285.net
hop=4 hoprtt=19.3 ms
hop=5 TTL 0 during transit from ip=78.144.1.134 name=ae64-scr101.thw.as13285.net
hop=5 hoprtt=19.1 ms
hop=6 TTL 0 during transit from ip=195.66.227.118 name=UNKNOWN
hop=6 hoprtt=18.9 ms
hop=7 TTL 0 during transit from ip=95.142.106.211 name=te0-14.cr1.nkf.as49685.net
hop=7 hoprtt=38.6 ms
hop=8 TTL 0 during transit from ip=176.74.228.8 name=eth42.eq3-iec-rtr-002.cloudvps.nl
hop=8 hoprtt=38.3 ms
len=28 ip=31.3.96.40 ttl=53 id=59312 tos=0 iplen=28
```

```
(root@ SC-205-03) - [/home/ethical]
# hping3 --traceroute -V 192.168.1.27
using eth0, addr: 172.17.226.155, MTU: 1500
HPING 192.168.1.27 (eth0 192.168.1.27): NO FLAGS are set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=172.17.224.1 name=SC-205-03.mshome.net
hop=1 hoprtt=19.9 ms
len=40 ip=192.168.1.27 ttl=63 DF id=9519 tos=0 iplen=40
sport=0 flags=RA seq=1 win=0 rtt=559.9 ms
seq=0 ack=12331971 sum=c427 urp=0

len=40 ip=192.168.1.27 ttl=63 DF id=9694 tos=0 iplen=40
sport=0 flags=RA seq=2 win=0 rtt=179.8 ms
seq=0 ack=1929757851 sum=a11c urp=0

len=40 ip=192.168.1.27 ttl=63 DF id=9849 tos=0 iplen=40
sport=0 flags=RA seq=3 win=0 rtt=419.6 ms
seq=0 ack=1310585994 sum=9911 urp=0

len=40 ip=192.168.1.27 ttl=63 DF id=10101 tos=0 iplen=40
sport=0 flags=RA seq=4 win=0 rtt=339.4 ms
seq=0 ack=421650747 sum=e359 urp=0
```



Scanning Networks: Tools

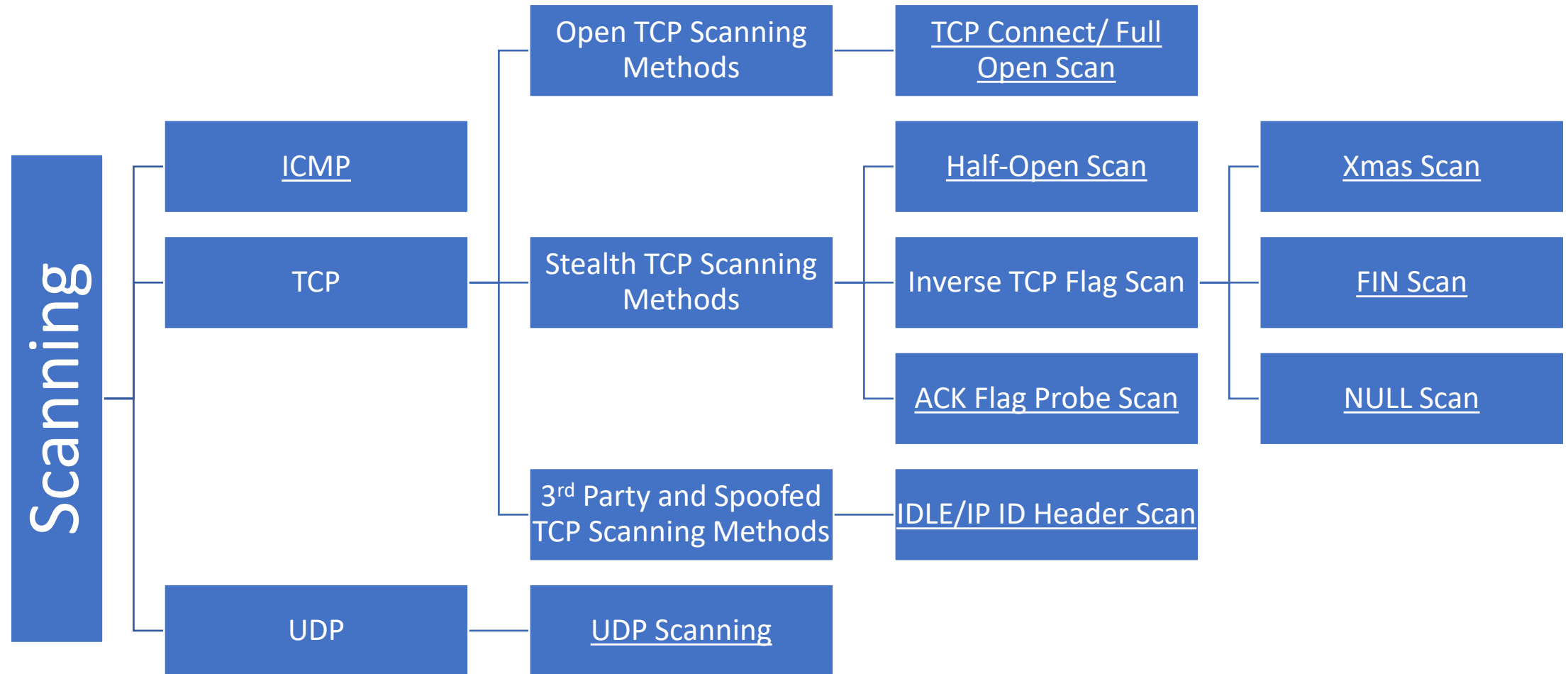
NetScanTools Pro

- It helps in troubleshooting, diagnosing, monitoring, discovering devices
- It lists IPv4, IPv6 Addresses, hostnames, domain names, email addresses, urls.
- It does automatically or manually.

The screenshot displays the NetScanTools Pro application window. The left sidebar contains a 'Welcome' section and a list of tools categorized into 'Automated Tools' and 'Manual Tools (all)'. The 'Manual Tools (all)' section is expanded, showing various tools like 'DNS Tools - Advanced', 'DNS Tools - Batch Queries', 'DNS Traffic Monitor', 'Duplicate IP Scanner', 'Email Validate', 'Finger', 'Firewall Rules', 'IP to Country', 'IP/MAC Address Database', 'Launcher', 'MAC Address to Manufacturer', and 'Network Connection Endpoints'. The 'IP/MAC Address Database' tool is selected, showing a table of IP addresses, MAC addresses, hostnames, and last update dates. A dialog box titled 'Edit IP/MAC Address Entry' is open, prompting the user to enter or edit an IP address and MAC address combination. The dialog includes fields for IP Address (e.g., 192.168.1.47), MAC Address (e.g., xx-xx-xx-xx-xx-xx), and Hostname (e.g., UOW-09147782557). Buttons for 'OK', 'Cancel', 'Get Hostname for IP Address', and 'Stop' are visible.

IP Address	MAC Address	Hostname	Last Update	Date/Time
172.17.226.155	00-15-5D-7D-7F-9B		2022-02-12	17:46:37.369
192.168.1.1	44-AD-B1-A5-04-86		2022-02-12	17:46:36.883
192.168.1.25	B8-5F-98-21-F3-AC		2022-02-12	17:46:37.037
192.168.1.53	44-85-00-EF-30-BC		2022-02-12	17:46:37.238
192.168.220.254	00-50-56-EF-23-54		2022-02-12	17:46:36.705
224.0.0.22	01-00-5E-00-00-16		2022-02-12	17:46:36.051
224.0.0.251	01-00-5E-00-00-FB		2022-02-12	17:46:36.203
224.0.0.252	01-00-5E-00-00-FC		2022-02-12	17:46:36.404
239.255.255.250	01-00-5E-7F-FF-FA		2022-02-12	17:46:36.551

Scanning Networks - Techniques



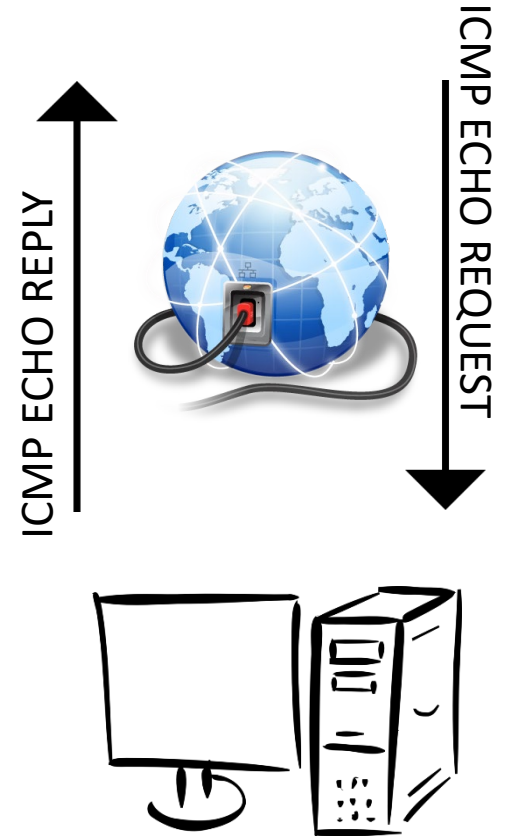
Scanning Networks – ICMP

- **ICMP Scanning – To check for live systems**
 - ICMP Scan will send ICMP ECHO requests to a particular host.
 - If the system is LIVE, it will send back an ICMP ECHO reply
 - Using an ICMP Scan, you may
 - ✓ determine an active device.
 - ✓ determine if Firewall is blocking ICMP

```
(root@SC-205-03)-[/home/ethical]
# nmap -sn 192.168.1.27
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 05:17 GMT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.17 seconds

(root@SC-205-03)-[/home/ethical]
# nmap -sn 192.168.1.47
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 05:18 GMT
Nmap scan report for [REDACTED] (192.168.1.47)
Host is up (0.0056s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
```

<<



Scanning Networks – Ping Sweep

- **PING Sweep – To find live systems from a range of IP Addresses**
 - Ping Sweep will send ICMP ECHO requests to multiple host.
 - If the system is LIVE, it will send back an ICMP ECHO reply
 - You need to determine the subnet mask to find out the number of hosts that are found in the subnet.
 - Mostly, Ping Sweeps are done to create an inventory of live systems in the subnet.

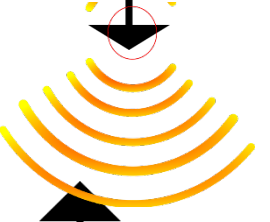
```
Nmap scan report for ttrouter (192.168.1.1)
Host is up (0.0039s latency).
Not shown: 845 closed tcp ports (reset), 151 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
49152/tcp open  unknown

Nmap scan report for 192.168.1.26
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.1.26 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for UOW-09147782557 (192.168.1.47)
Host is up (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.32 seconds
```

ICMP ECHO REQUEST



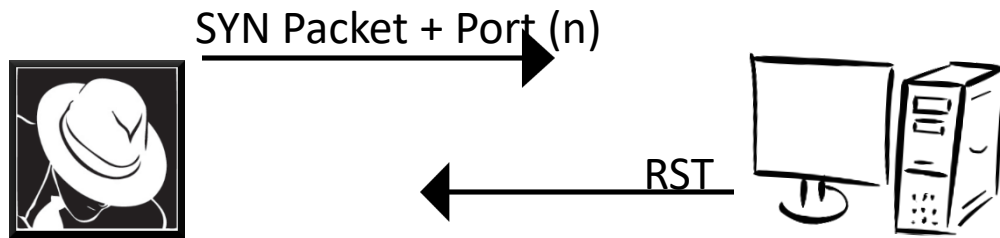
ICMP ECHO REPLY



Scanning Networks – TCP Connect/ Full Open Scan

- Full Open Scan can detect when a port is open after the three-way handshake
- It **establishes full connection** and **sends back RST Packets** to bring down
 - Does not require super user privileges.

When a Port is closed?



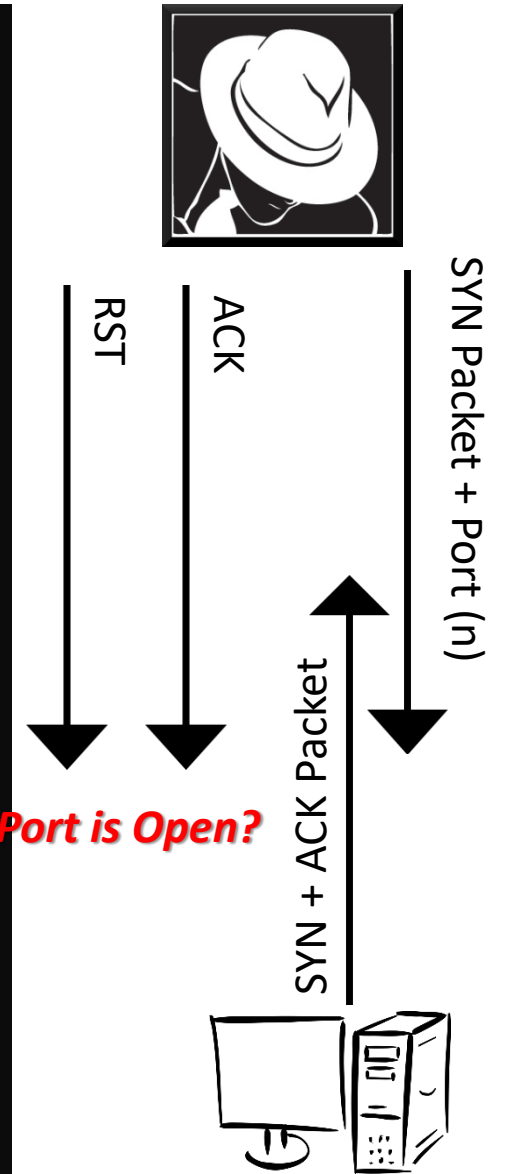
<<

```
(root@ SC-205-03) - [/home/ethical]
# nmap -sT -v 192.168.1.26
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 06:01 GMT
Initiating Ping Scan at 06:01
Scanning 192.168.1.26 [4 ports]
Completed Ping Scan at 06:01, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:01
Completed Parallel DNS resolution of 1 host. at 06:01, 1.01s elapsed
Initiating Connect Scan at 06:01
Scanning 192.168.1.26 [1000 ports]
Completed Connect Scan at 06:01, 4.28s elapsed (1000 total ports)
Nmap scan report for 192.168.1.26
Host is up (0.0068s latency).
Not shown: 975 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
458/tcp    filtered  appletcp
801/tcp    filtered  device
880/tcp    filtered  unknown
1174/tcp   filtered  fnet-remote-ui
1434/tcp   filtered  ms-sql-m
1443/tcp   filtered  ies-lm
1984/tcp   filtered  bigbrother
3003/tcp   filtered  cgms
3301/tcp   filtered  unknown
3784/tcp   filtered  bfd-control
3851/tcp   filtered  spectraport
4998/tcp   filtered  maybe-veritas
5033/tcp   filtered  jtnetd-server
5800/tcp   filtered  vnc-http
7496/tcp   filtered  unknown
9102/tcp   filtered  jetdirect
9415/tcp   filtered  unknown
9485/tcp   filtered  unknown
9878/tcp   filtered  kca-service
9900/tcp   filtered  iua
24444/tcp  filtered  unknown
49175/tcp  filtered  unknown
50001/tcp  filtered  unknown
55056/tcp  filtered  unknown
57797/tcp  filtered  unknown

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.65 seconds
Raw packets sent: 4 (152B) | Rcvd: 1 (40B)

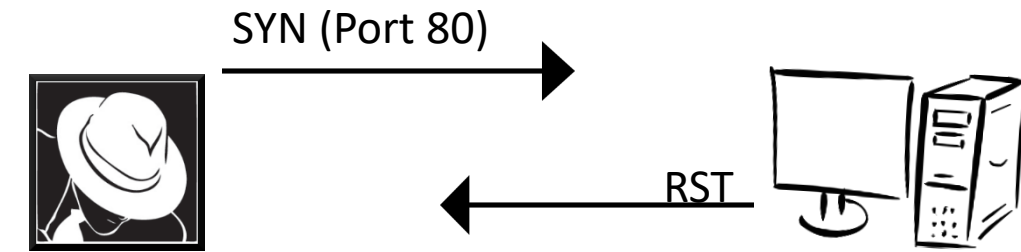
(root@ SC-205-03) - [/home/ethical]
# nmap -sT -v 192.168.1.25
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 06:01 GMT
Initiating Ping Scan at 06:01
Scanning 192.168.1.25 [4 ports]
Completed Ping Scan at 06:01, 3.08s elapsed (1 total hosts)
Nmap scan report for 192.168.1.25 [host down]
Read data files from: /usr/bin/./share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```

When a Port is Open?



Scanning Networks – Half Open Scan

- Otherwise, Stealth Scan can reset the TCP Connection between the client and the server quickly before the three-way handshake, resulting in a half open connection.
- This technique is used to bypass firewall rules, logging mechanism and hide under network traffic.



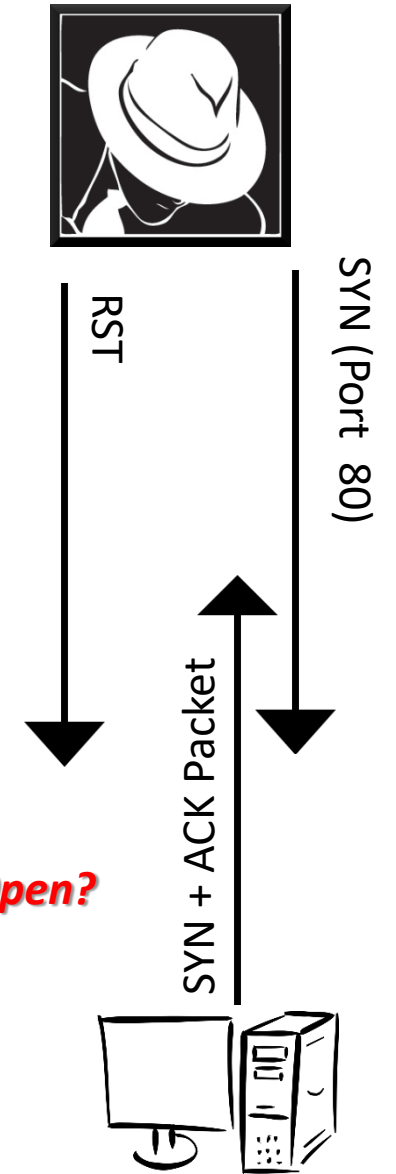
When a Port is closed?

The Attacker sends a single SYN packet to the target to app. port

An open port: sends the SYN/ACK packet

The Attacker sends back RST packet, stating the remote port is in CLOSED state

The Targets sends the RST packet to close the initiation before a connection is established

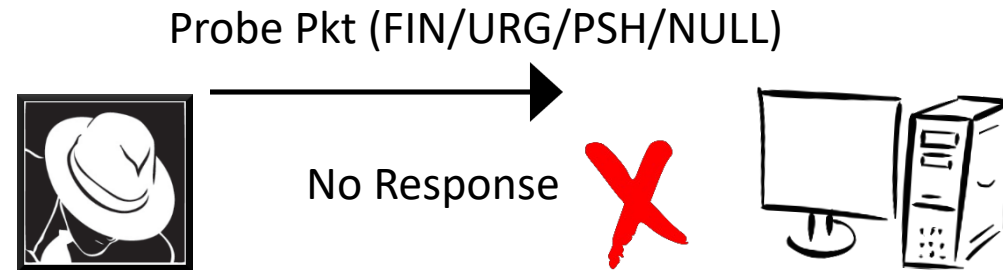


When a Port is Open?

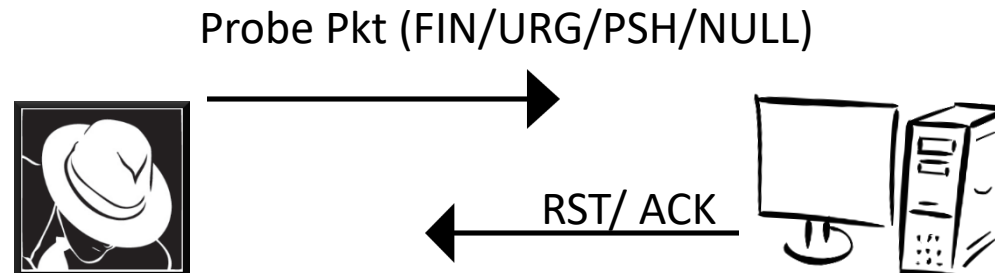
Scanning Networks – Inverse TCP Flag Scan

- Attackers send TCP probe packets with a TCP Flag (FIN, URG, PSH) set or with no flags.
- No Response? → Port is Open
- RST → Port is Closed

When a Port is Open?



When a Port is closed?

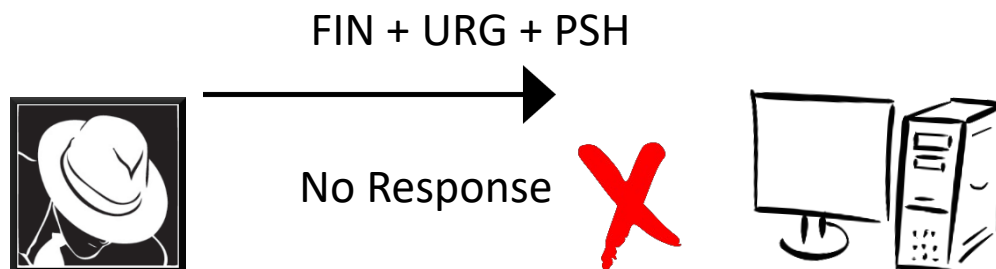


<<

Scanning Networks – Xmas Scan

- Attackers send TCP frame to a remote device with (FIN, URG, PSH) set.
- Note: FIN scan works only with RFC 793-based TCP/IP implementation OS. It will not work with any of the current Windows version

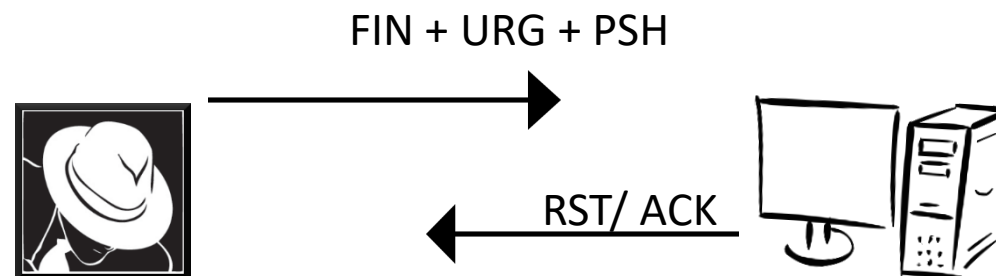
When a Port is Open?



```
# nmap -sX -v 192.168.1.47
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 06:35 GMT
Initiating Ping Scan at 06:35
Scanning 192.168.1.47 [4 ports]
Completed Ping Scan at 06:35, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:35
Completed Parallel DNS resolution of 1 host. at 06:35, 0.29s elapsed
Initiating XMAS Scan at 06:35
Scanning UOW-09147782557 (192.168.1.47) [1000 ports]
Completed XMAS Scan at 06:35, 21.13s elapsed (1000 total ports)
Nmap scan report for UOW-09147782557 (192.168.1.47)
Host is up (0.0064s latency).
All 1000 scanned ports on UOW-09147782557 (192.168.1.47) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

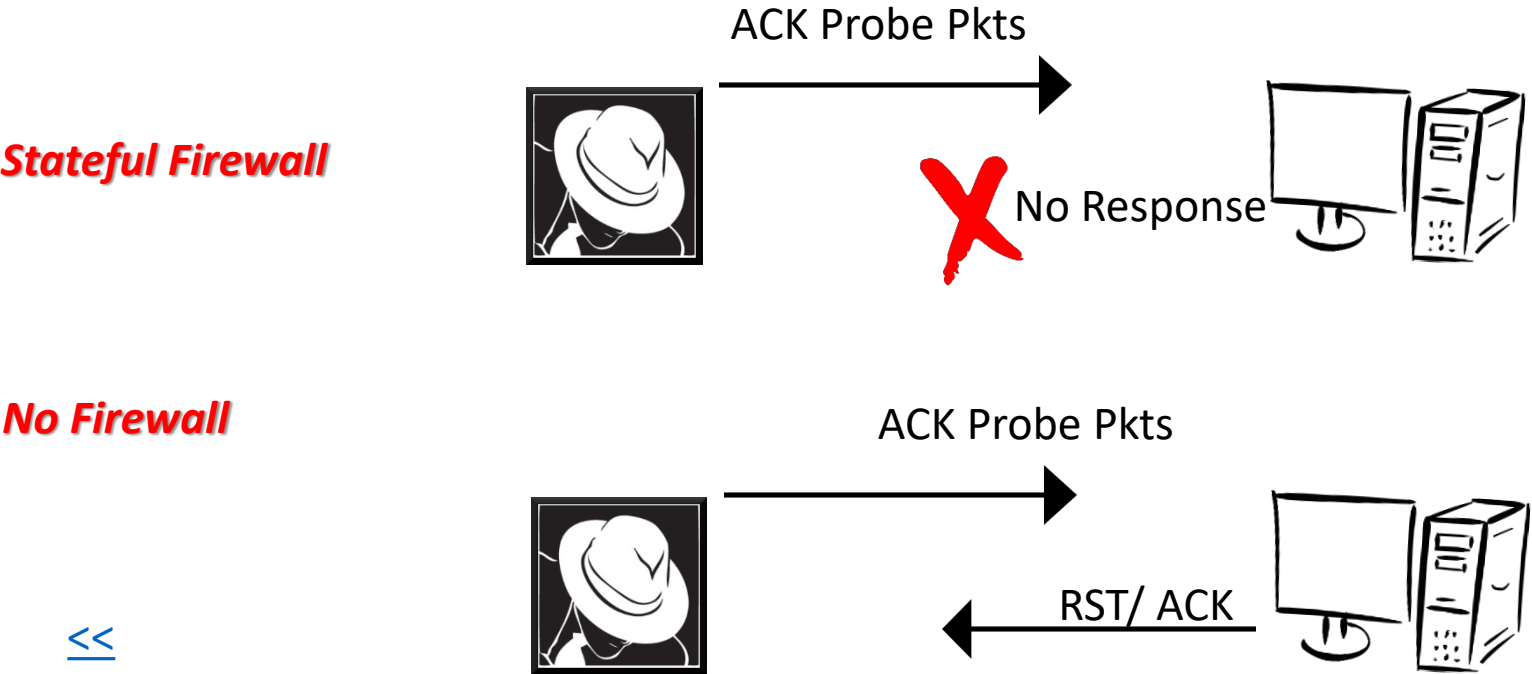
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.72 seconds
Raw packets sent: 2004 (80.152KB) | Rcvd: 1 (28B)
```

When a Port is closed?



Scanning Networks – ACK Flag Probe Scan

- Attackers send TCP probe pkts to remote devices with ACK Flag set.
- Analyse the header information like TTL, Window Field of received RST packets to find out the open/closed ports



```

(root@kali)-[/home/kali]
# nmap -sA -v 10.10.10.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 02:17 EST
Initiating Parallel DNS resolution of 1 host. at 02:17
Completed Parallel DNS resolution of 1 host. at 02:17, 1.07s elapsed
Initiating ACK Scan at 02:17
Scanning 10.10.10.11 [1000 ports]
Completed ACK Scan at 02:17, 0.04s elapsed (1000 total ports)
Nmap scan report for 10.10.10.11
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.10.10.11 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds
Raw packets sent: 1000 (40.000KB) | Rcvd: 2000 (80.000KB)

```

Wireshark packet capture details for a TCP RST packet (Seq: 65536, Win: 0, Len: 0) from 10.10.10.11 to 10.10.10.1. The packet is identified as a "Transmission Control Protocol, Seq: 65536, Seq: 1, Len: 0".

```

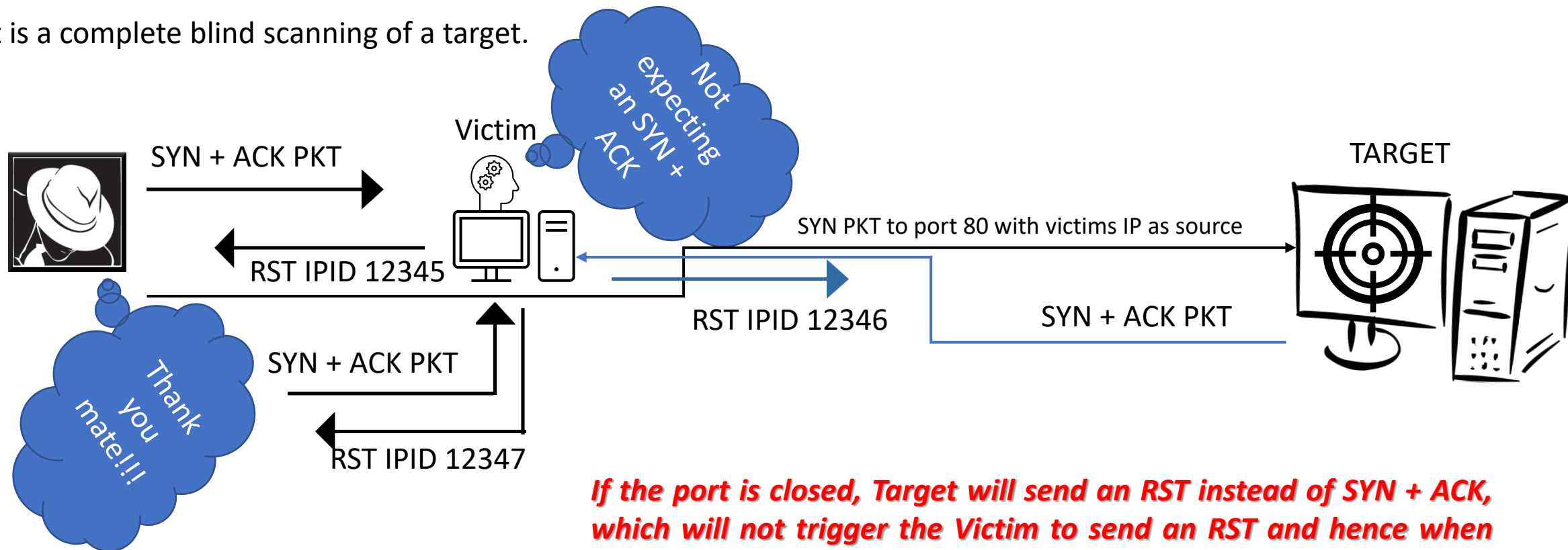
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0

1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512

```

Scanning Networks – IDLE/ IPID Header Scan

- It is a TCP port scan. However, it uses a spoofed source address to the target to find out the available services.
- It is a complete blind scanning of a target.

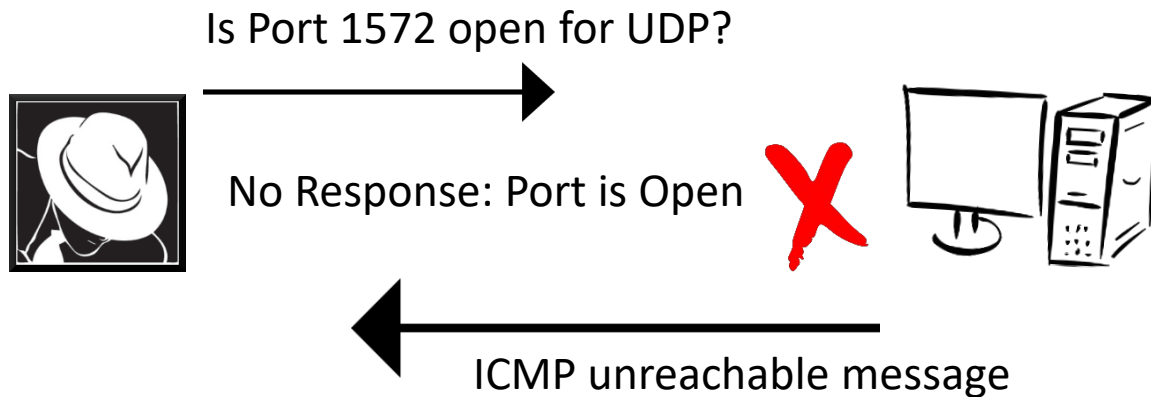


If the port is closed, Target will send an RST instead of SYN + ACK, which will not trigger the Victim to send an RST and hence when the attacker is again sending an SYN+ACK, the IPID would be 12346

<<

Scanning Networks – UDP Scan

- For UDP, there is no 3-way Handshake. That means, the system won't respond with a message to tell the port status.
- If a UDP packet is sent to a port that is closed, the system will respond with ICMP port unreachable message
- Generally, malicious applications, Trojan horses, Spywares use UDP Ports.



```
(root@kali)-[/home/kali]
# nmap -sU -v 10.10.10.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 03:35 EST
Initiating ARP Ping Scan at 03:35
Scanning 10.10.10.10 [1 port]
Completed ARP Ping Scan at 03:35, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:35
Completed Parallel DNS resolution of 1 host. at 03:35, 0.00s elapsed
Initiating UDP Scan at 03:35
Scanning 10.10.10.10 [1000 ports]
Discovered open port 137/udp on 10.10.10.10
Completed UDP Scan at 03:35, 7.30s elapsed (1000 total ports)
Nmap scan report for 10.10.10.10
Host is up (0.00039s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE
137/udp    open  netbios-ns
MAC Address: 00:0C:29:75:0F:C6 (VMware)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
Raw packets sent: 2034 (94.116KB) | Rcvd: 10 (1.693KB)
```

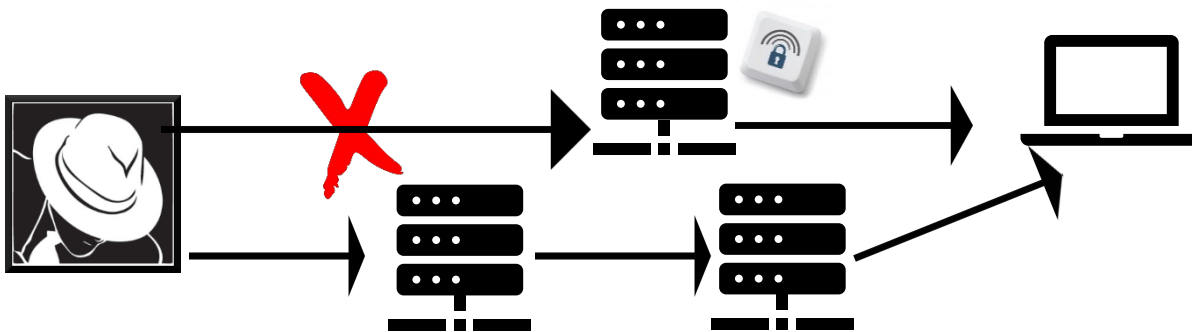
Scanning Networks – SSDP/ List Scan

- **SSDP: Simple Service Discovery Protocol** working with Universal Plug and Play to detect devices.
- This helps the attackers to launch Buffer Overflow or DoS attacks
- **Metasploits**, or UPnP SSDP M-Search info discovery tool could be used to check the UPnP vulnerability.
- List scan generates and prints the IP address and names without pinging them. A reverse DNS resolution could be carried out to identify the host names.

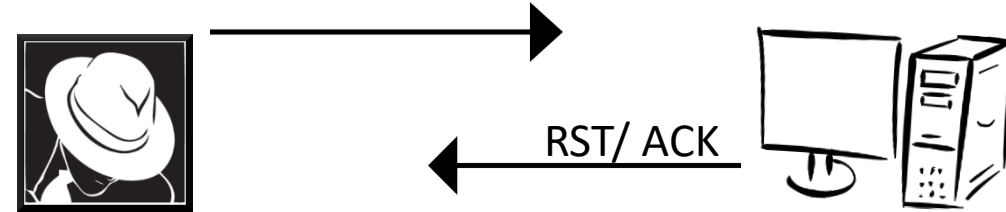
```
(root@kali)-[/home/kali]
# nmap -sL -v 10.10.10.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 03:49 EST
Initiating Parallel DNS resolution of 1 host. at 03:49
Completed Parallel DNS resolution of 1 host. at 03:49, 0.00s elapsed
Nmap scan report for 10.10.10.10
Nmap done: 1 IP address (0 hosts up) scanned in 0.00 seconds
```

Scanning Networks – Firewalls!!!

- *In many cases, placing a Firewall/ IDS, IPS Systems may protect the network from scanning networks. However, there are various methods to overcome Firewalls and other protection mechanisms.*
- One way, is to *fragment (divide into small packets) the probe packets.*
- TCP Header may be split into many small packets in order to avoid packet filtering mechanisms placed in the network.
- **Source Routing** is another way, where the attacker decides on the route (specified route) to ignore the IDS/IPS/Firewalls.



SYN/FIN Small IP Fragments + Port (n)



```
# nmap -sS -T4 -A -f -v 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-14 04:21 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating ARP Ping Scan at 04:21
Scanning 10.10.10.16 [1 port]
Completed ARP Ping Scan at 04:21, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:21
Completed Parallel DNS resolution of 1 host. at 04:21, 0.03s elapsed
Initiating SYN Stealth Scan at 04:21
Scanning 10.10.10.16 [1000 ports]
Discovered open port 139/tcp on 10.10.10.16
Discovered open port 445/tcp on 10.10.10.16
Discovered open port 80/tcp on 10.10.10.16
Discovered open port 135/tcp on 10.10.10.16
Discovered open port 1801/tcp on 10.10.10.16
Discovered open port 2105/tcp on 10.10.10.16
Discovered open port 2107/tcp on 10.10.10.16
Discovered open port 2103/tcp on 10.10.10.16
Completed SYN Stealth Scan at 04:21, 4.42s elapsed (1000 total ports)
Initiating Service scan at 04:21
Scanning 8 services on 10.10.10.16
```

Scanning Networks – Firewalls!!!

- *In many cases, placing a Firewall/ IDS, IPS Systems may protect the network from scanning networks. However, there are various methods to overcome Firewalls and other protection mechanisms.*
- Generate/ Manually assign an IP address to bypass the firewall. This is known as **IP Address decoy**.
- Change the source IP Address to make it look like an attack from a different source. This could bypass firewalls as 3-way handshake is not complete. This is **IP Address Spoofing**

```
(root@kali)-[/home/kali]
# nmap -D RND:10 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-14 04:33 EST
Nmap scan report for 10.10.10.16
Host is up (0.0022s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
MAC Address: 00:0C:29:1D:C0:EF (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds
```

```
(root@kali)~# nmap -n -D 10.10.10.1,10.10.10.3 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-14 04:37 EST
Nmap scan report for 10.10.10.16
Host is up (0.00078s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmsg-mgmt
MAC Address: 00:0C:29:1D:C0:EF (VMware)
```

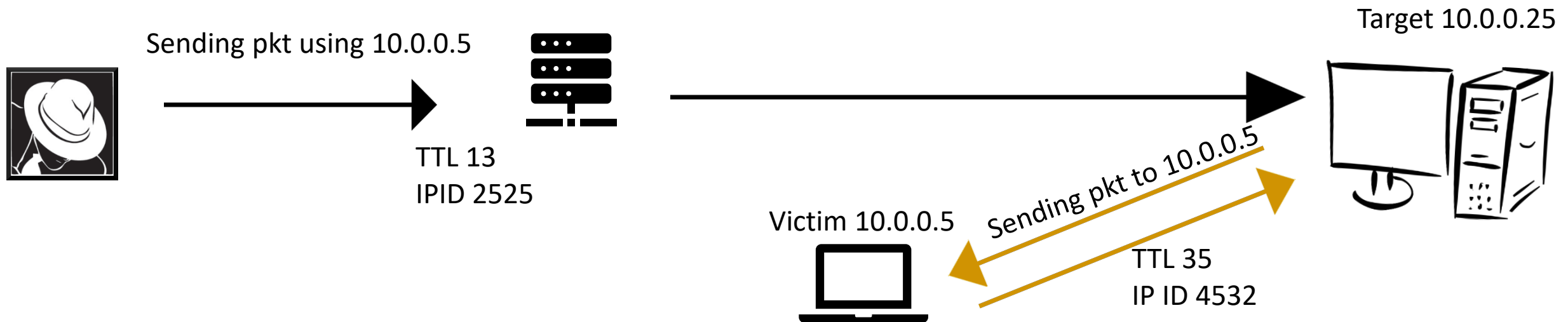
```
Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
```

[illegible]

Scanning Networks – Security Perspective

As a security professional, there is always ways to analyse the packets to identify these scans

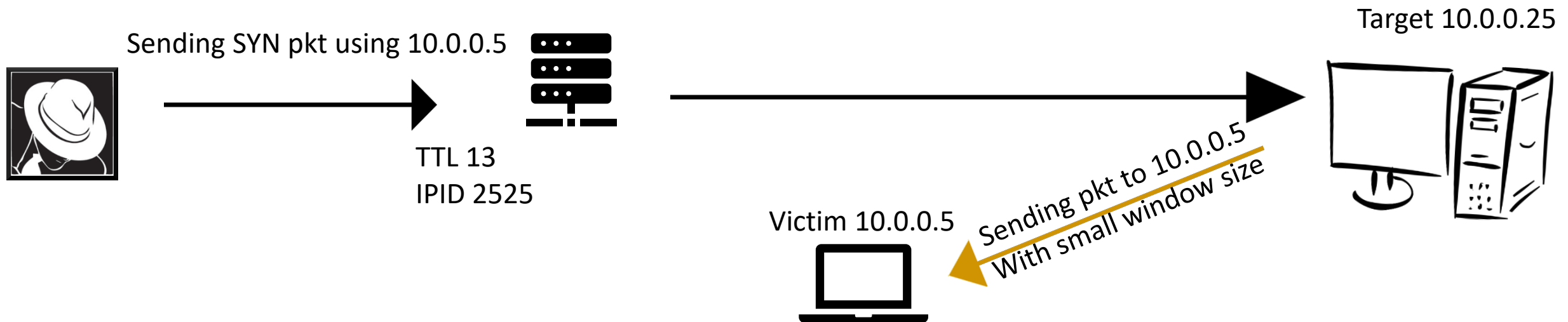
- Send a packet to the host. You will get a reply. **Look at the TTL** with the initial packet received. If the TTL is not same, it is a **spoofed packet**.
- Send probe to the suspected host. **Compare the IPID** in its reply. If IPID value is not any nearest value to the packet examining, it is a **spoofed traffic**.



Scanning Networks – Security Perspective

As a security professional, there is always ways to analyse the packets to identify these scans

- If an attacker is sending a spoofed TCP packet, he/she will **not receive the SYN-ACK**. (as it is spoofed with a different ip address and the SYN-ACK will reach the original spoofed address). This will limit the attackers from receiving any updates. If the received traffic continues even **after a window size exhaustion, the packets are spoofed**.



Scanning Networks - Countermeasures

- **Information is Wealth:** Restrict sensitive information from public access
- **Firewalls:** Always make sure firewalls/ IDS/ IPS are configured to *identify and block probes. Use multiple firewalls.*
- **Self-Test:** Try to do TCP and UDP scan along with ICMP probes against your networks IP address to check the status of your network
- **Configurations & Updates:** Have a look at routers and firewall configurations, firmware updates
- **Anti-Spoofing:** Make sure, anti-scanning & anti-spoofing rules are effective
- **Block:** Block unused ports
- **Filter:** Filter all inbound and outbound ICMP messages. Use routers and firewalls to filter incoming packets and outgoing packets.
- **Encrypt** all the traffic: Use Ipsec, TLS, SSH, HTTPS etc
- **IP-based authentication:** It is not reliable. Use random initial sequence number to prevent IP Spoofing attacks based on seq. number spoofing.

Scanning Networks Proxys

An intermediary device helping in connecting with devices is a proxy server. Proxys help in hiding the actual source of scan and bypass security restrictions.

- A Request is made for a resource via a Proxy Client
 - The Proxy Client connects to a Proxy server and passes the request
 - The Proxy server removes the user id's and passes it to the next proxy server.
 - The process continues until the request reaches the resource.
 - From the source to the destination, the traffic is encrypted. It is decrypted when it reaches the destination.
-
- Tools like Proxy Switcher is used to browse internet without disclosing the IP address.
 - CyberGhost VPN: Online Privacy, Anonymous Browsing, Access/Block censored contents etc
 - Tor, Burpsite, Proxifier etc...

- On discussing about scanning the target for concrete information which would be very helpful in identifying their vulnerabilities, details on Open Ports, Applications etc is good to know. Adding to those information, ***finding out the running operating system*** adds more value to the gathered information.
- Determining/ Identifying the target's Operating System is Banner Grabbing.

Active

- Packets are crafted and sent to the target
- The Responses were gathered, compared and analysed
- Determine OS
- Note: OS'es could have different responses because of their TCP/IP stack implementation

Passive

- Looking into the error messages.
- Information like Server Type, OS, Tools etc.
- Observing Packets. (Capture, analyse)
- Other available details (.php uses apache server, Linux, .aspx uses IIS Server, Windows)

Scanning Networks – Banner Grabbing

Scanning Networks – Banner Grabbing

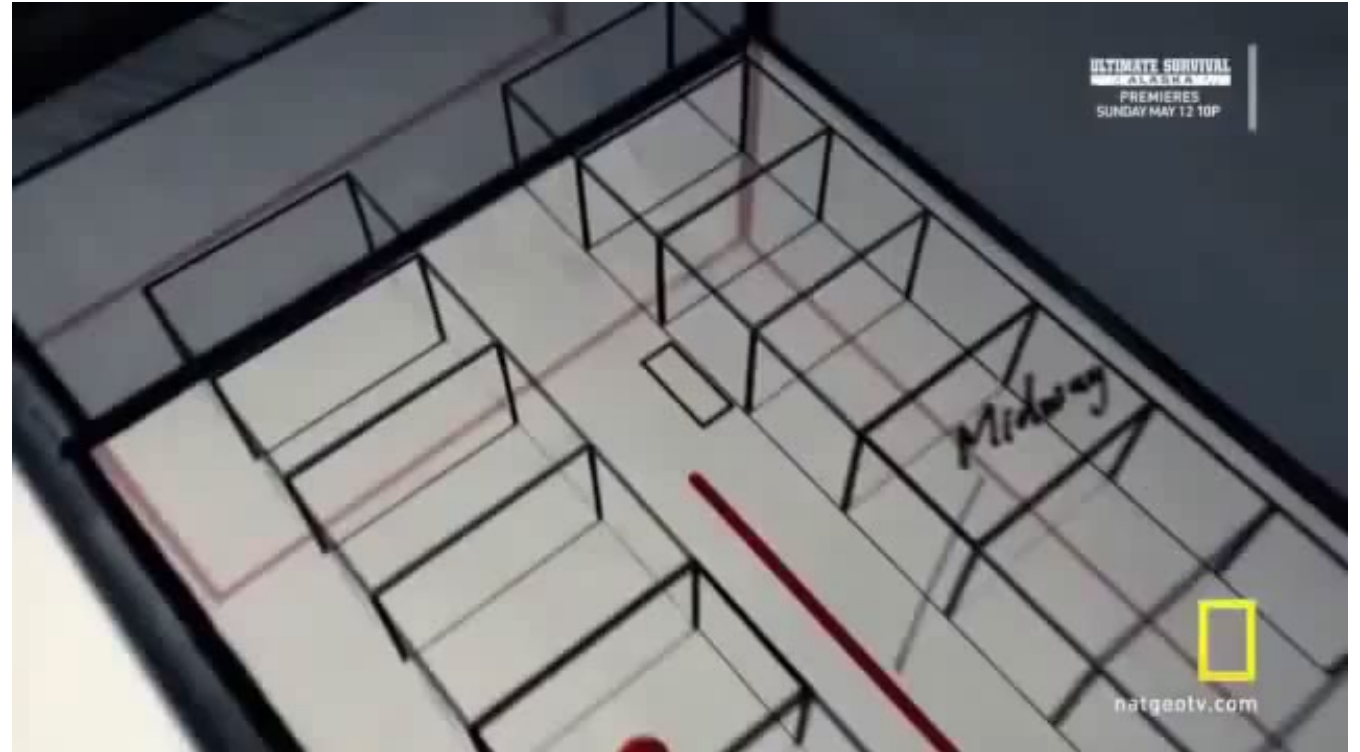
Countermeasures:

- Set False banners.
- Turn off Services that are not used/required
- Hide file extensions.

Scanning Networks –

Map the Infrastructure

- Logical/ Physical path.
 - Intranet
 - DMZ
 - Intranet



Scanning Networks – Security Perspective!!!

As a Security Professional, look at your Network's security.

- Look for
 - ✓ Live systems
 - ✓ Open Ports
 - ✓ Services Running
 - ✓ System Banners
 - ✓ Etc....
- Act on
 - ✓ Close all the unused ports
 - ✓ Disable Services that are not used
 - ✓ Hide Banners
 - ✓ Fix configuration errors
 - ✓ Check Firewall rules.

Scanning Networks – Steps

HOST

- Identify Host
- Nmap, IP Scanner, NetScanTools etc

SCAN

- Scan for open ports
- Bypass Security Infrastructure
- Packet Fragmentation, IP address spoofing etc

BG

- Banner Grabbing
- Craft packets and capture the response

MAP

- Map the Target Network
- Mapper, OpManager, NetBrain etc
- Record/ Document the information

Enumeration

- Like, **Reconnaissance** is the method of collecting information about a target system without alerting it, also known as **Footprinting**, it is the first step in any form of hacking that helps in understanding the target system and identify potential attack vectors & vulnerabilities followed by **network scanning** to identify hosts, ports and services in the network.
- Enumeration is when you try and connect to the system and do deliberate actions to gather more information.



Enumeration

- The main objectives of Enumeration
 - ✓ Use the earlier gathered information to look out the weak points to initiate system attack and gain access on the target system

Further get more information, ***but this time from an intranet environment.***

- ✓ Network Resources
- ✓ Shared Folders
- ✓ Routing Information
- ✓ System/ Security Settings
- ✓ Names, Users, Groups
- ✓ Applications
- ✓ SNMP, FQDN Information etc

Enumeration

- **NetBIOS**

- What it is?
- Used to identify the network devices
- Uses TCP/IP



- Enumerate NetBIOS information to
- List the computers of the domain.
- List the shares on the hosts
- Look for Policies and Passwords



Communication using NetBIOS Name



NetBIOS Name:

16 Digits

15 Digits – Device Name

1 Last Digit – Service/ Name Record Type

Enumeration

○ NetBIOS

- What it is?
- Used to identify the network devices
- Uses TCP/IP



NetBIOS Name:

16 Digits

15 Digits – Device Name

1 Last Digit – Service/ Name Record Type

- Enumerate NetBIOS information to
- List the computers of the domain.
- List the shares on the hosts
- Look for Policies and Passwords



Communication using NetBIOS Name

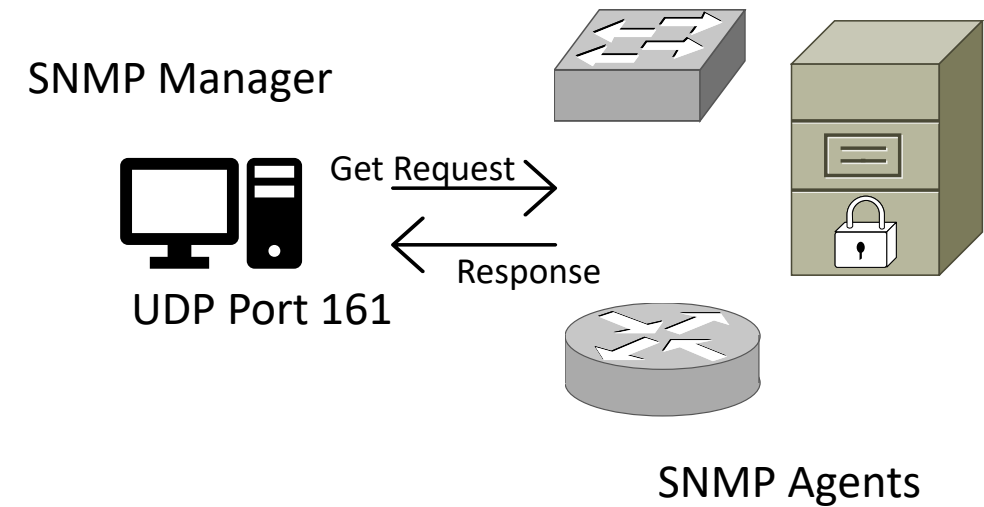


Name	NetBIOS Code	Type	Information
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain Name
<host name>	<03>	UNIQUE	Messenger Service for the computer
<user name>	<03>	UNIQUE	Messenger Service for the user logged in
<host name>	<20>	UNIQUE	Server services running
<domain>	<1D>	GROUP	Master Browser name for the subnet
<domain>	<1B>	UNIQUE	Domain Master browser name: identifies the primary domain controller (PDC) for that domain

Enumeration

○ SNMP

- SNMP has Manager (NMS) and Agent (Each Network Device)
- SNMP Manager uses 2 passwords to access and configure its Agents.
 - Read Community String: Public. View device Configuration
 - Read/Write community String: Private. Edit Configuration
- Enumerating user accounts and devices on a Target System
 - Gathers default community strings information and gets details like hosts, intermediate devices, shares, routing tables, ARP tables, network traffic etc.
- Community Strings are stored in MIB (Management Information Base) which needs to be matched. If not, an error message will be sent to the pre-configured SNMP Manager.
 - MIB is a virtual database with information related to network objects (*Scalar Objects – define a single object instance; Tabular Objects – Multiple related object instances are grouped*) managed used SNMP
 - MIB database is hierarchical, and they are addressed using Object Identifiers (OIDs). OIDs includes counter, string, address, access levels (not accessible, read-only, read-write), size restrictions, range information etc.
 - SNMP uses the MIB's hierarchical namespace containing Object Identifies (OIDs) to translate the OID numbers into a human-readable display.



Enumeration

○ LDAP

Active Directory LD Services

- **Manageability**
- **Security**
- **Interoperability**

- AD LDS is a hierarchical file-based directory store with directory information source and the service that makes the information available and usable

Network Devices

- Config
- QoS Policy
- Security Policy

Email Servers

- Mailbox Information
- Address Book

Windows User

- Account Information
- Privileges
- Profiles
- Policies

Application

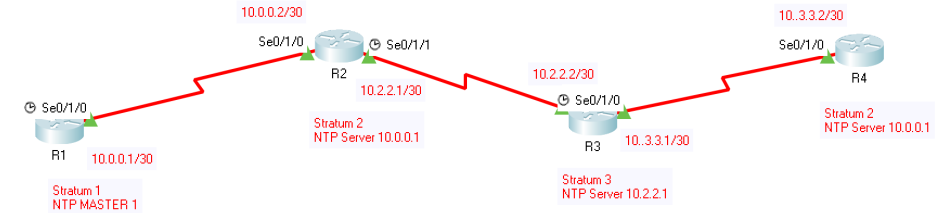
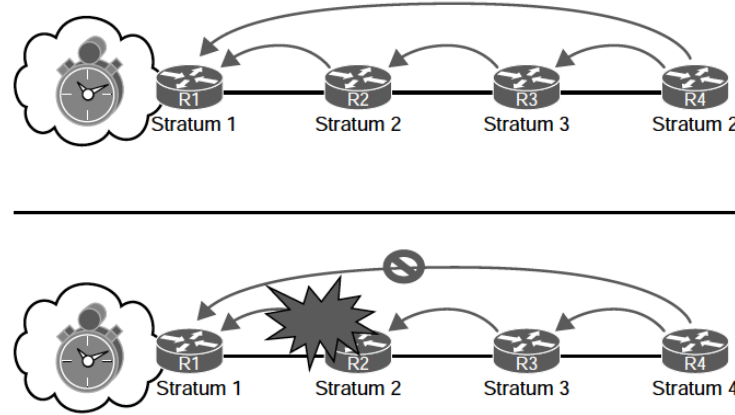
- Server Config
- SSO
- App-Specific Directory Info



- Queries LDAP services and gets information like usernames, department details, address etc.
- Tools like LDAP Admi Tools, LDAP Search, Active Directory Explorer could be used to enumerated LDAP.

Enumeration

○ NTP



- **Network Time Protocol (NTP)** is used to *synchronize a set of network clocks in a distributed client/server architecture*.
- NTP is a *UDP-based protocol* that connects with *servers* on *port 123*. The *client* source *port* is *dynamic*. The Time zone in Cisco devices is *UTC*
- NTP is based on a *hierarchical concept* of communication.
 - At the top of the hierarchy are authoritative devices that operate as an *NTP server with an atomic clock*.
 - The *NTP client queries the NTP server* for its time and then updates its time based on the response.
- The NTP synchronization process is *not fast*, gaining an *accuracy* of tens of milliseconds *requires hours or days of comparisons*.



- Attacker targets NTP server to look for the connected hosts to it, IP Addresses, System Names and Operating Systems.
- Internal IP Address can also be obtained if NTP Server is located in DMZ

Enumeration

- SMTP
- **Simple Mail Transfer Protocol** (SMTP) is used to *send emails*.
- SMTP has commands to validate users (vrfy), give actual deliver address and mailing lists (expn) and give the receivers details (rcpt to).
- The response to valid users and invalid users differs in SMTP servers.



➤ Attacker uses telnet connection to get the list of valid users from an SMTP Server

```
# smtp-user-enum -M VRFY -u rot -t 192.168.1.47
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

-----
| Scan Information |
-----

Mode ..... VRFY
Worker Processes ..... 5
Target count ..... 1
Username count ..... 1
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....

##### Scan started at Sun Feb 20 07:31:15 2022 #####
##### Scan completed at Sun Feb 20 07:31:20 2022 #####
0 results.

1 queries in 5 seconds (0.2 queries / sec)

(root@SC-205-03)-[/home/ethical]
#
```

Enumeration

DNS

- Enumerating DNS is a process of finding out the DNS Server of the target.
- Enumerating DNS can give an attacker information like DNS Server Names, usernames, IP Address, Host name, machine names etc.
- **DNS Zone Transfer enumeration** is used to get a copy of entire zone file for the domain from DNS Server

IPsec

- A scan for ISAKMP in UDP port (???) can indicate the presence of a VPN Gateway.
- Using various available tools, attackers can get information like encrypting & hashing algorithms, authentication type, SA life duration etc.

VoIP

- VoIP (SIP) uses UDP/TCP ports (???)
- Using various available tools, attackers can get information like VoIP gateway/servers, IP-PBX Systems, client softwares/ VoIP Phones, user-extensions etc.
- Later, these information may be used to attack the target.

RPC

- By enumerating RPC endpoints, attackers gather information on vulnerable services on the ports.

SNMP

- Turn Off SNMP Service
- If not, change community names
- Upgrade to SNMP3
- Implement Group Policy Security Option
- Restrict access to null session pipes, null session shares, IPsec Filtering

DNS

- Disable DNS Zone transfers to the untrusted hosts
- Don't publish private IP addresses in DNS Zone Files of Public DNS Server
- Use DNS registration services that hides sensitive information
- Use generic network admin contact for DNS Registrations

SMTP

- Ignore emails from unknown recipients
- Restrict mail responses
- Disable Open relay feature
- Limit no. of accepted connections

```
C:\Users\nitheesh>nslookup
Default Server: tttrouter
Address: 192.168.1.1

> server 31.3.96.40
Default Server: web.mmebvba.com
Address: 31.3.96.40

> set type=any
> ls -d itsecgames.com
ls: connect: No error
*** Can't list domain itsecgames.com: Unspecified error
The DNS server refused to transfer the zone itsecgames.com to your computer. If this
is incorrect, check the zone transfer security settings for itsecgames.com on the DNS
server at IP address 31.3.96.40.

>
```

Enumeration - Countermeasures

LDAP

- Encrypt LDAP traffic
- Enable lockout account

SMB

- Disable SMB protocol on Web & DNS Servers, Internet Facing servers, TCP Ports.
- Restrict anonymous access

Enumeration - Countermeasures



Enumeration – Steps

Network

- Identify Network Range, Calculate Subnet Mask, Discover Host, Scan the Ports
- Whois Lookup, Nmap etc

ENM

- Start with NetBIOS Enumeration, SNMP Enumeration, LDAP Enumeration, NTP Enumeration, SMTP Enumeration, DNS Enumeration, Ipsec, VoIP, RPC

Doc

- Document all the findings



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Any Questions?

*Advanced Cybersecurity
(ACCB6000)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

References

- EC-Council CEH
- Cisco Networking Academy
- Tevel Cyber Corps
- Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd edition
- Wikipedia
- Other website sources given in this presentation
- * The intension of usage is for Educational Purpose Only

Advanced Cybersecurity
(ACCB6000)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk