Chapter 1.1

Introduction

Aim

To elaborate the meaning and nature of Ethical Hacking and various concepts involved in it.

Instructional Objectives

Objectives of this chapter are:

- Explain the concept of Ethical Hacking, with its scope
- List the skills required for an Ethical hacker
- Explain Penetration testing and its types
- Describe the various steps for Ethical hacking
- Outline the steps involved in footprinting
- Explain the process of Scanning

Learning Outcomes

At the end of this chapter, you are expected to:

- Define Ethical hacking
- Describe the scope of Ethical hacking in Information Security scenario
- Apply the most appropriate type of Penetration testing to a system, in order to gather information
- Outline the steps to develop a footprint for an Organization’s network and systems

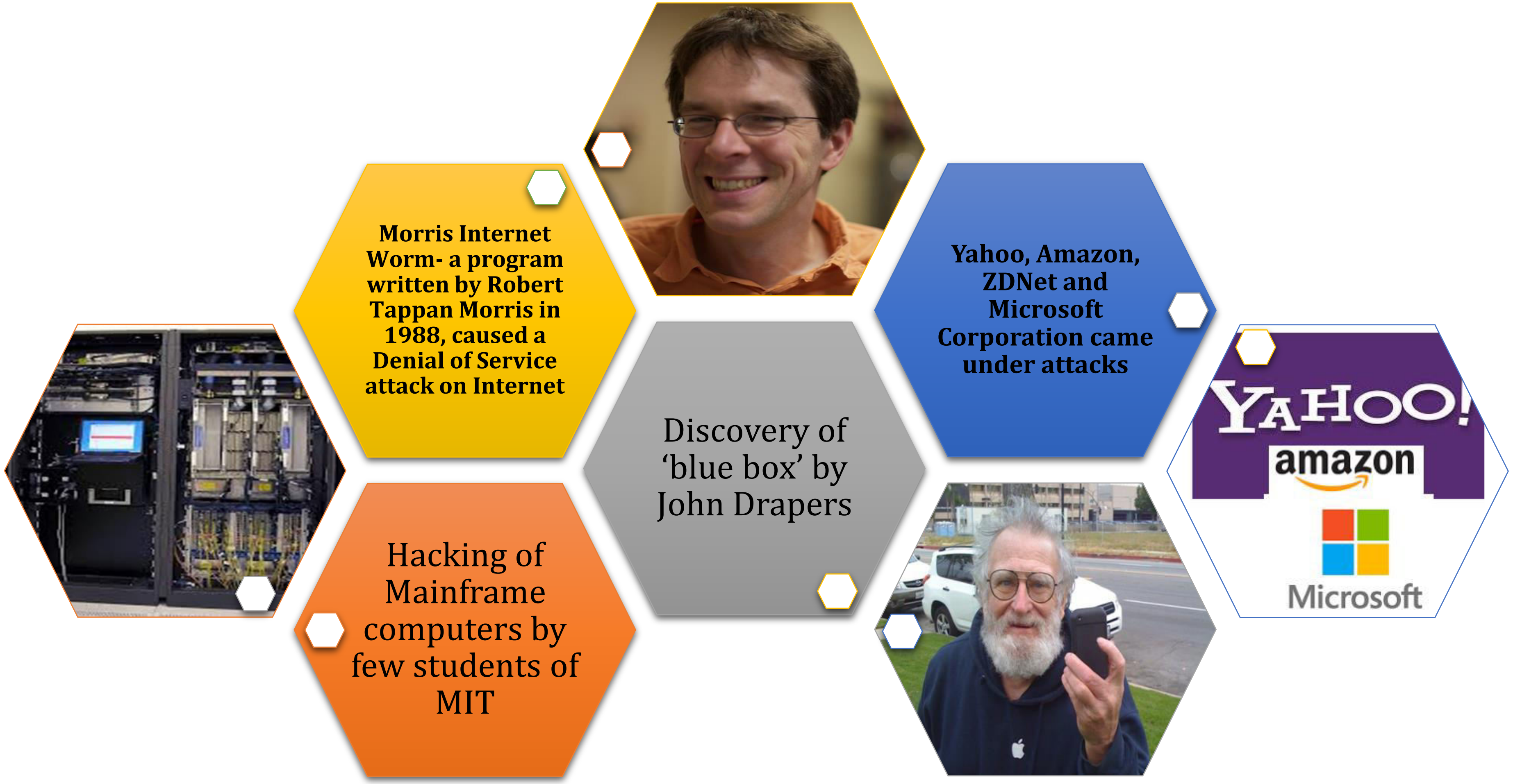
Ethical hacking and its scope

Introduction to hacking

It's a method of
Exploiting vulnerabilities.

Who gain unauthorized
access to system.

Some hacking incidents



Hacking of Mainframe computers by few students of MIT

Discovery of 'blue box' by John Drapers

Morris Internet Worm- a program written by Robert Tappan Morris in 1988, caused a Denial of Service attack on Internet

Yahoo, Amazon, ZDNet and Microsoft Corporation came under attacks

Ethical Hacking Concept

So, Hacking... When or how it can be Ethical???

"It is the process of gaining authorized access in to an Information System of an Organization or individual, in order to identify and evaluate the possible threats to it".

- Help the organization or individuals to improve their security system

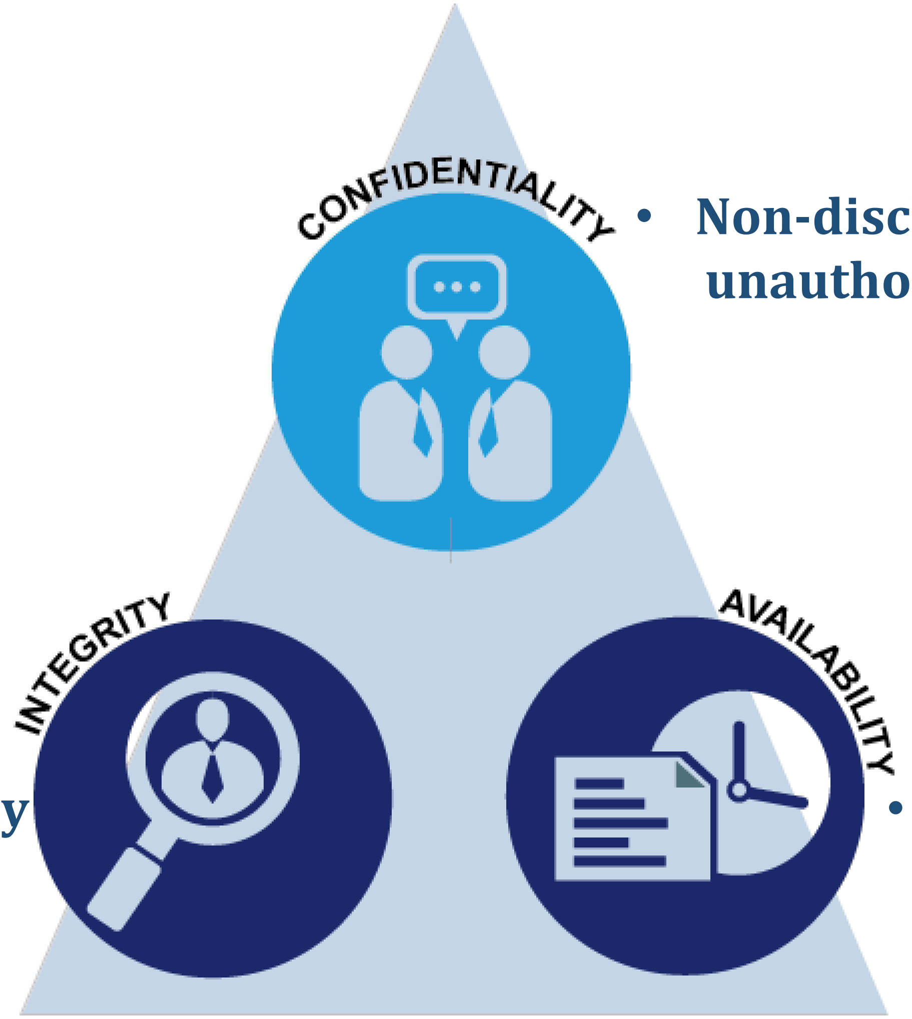
Who are ethical hacker?

Is an Information Security Professional

Project Management
Evaluate
Design
Develop
Analyze

Skills Required by an ethical hacker

CIA Triad



- Non-disclosure of information to either unauthorised persons or processes

- Ensuring safety and accuracy of data

- Uninterrupted and timely access of data to valid users

Terms used in Ethical hacking

TERMS	MEANING
Threat	***Activity or occurrence that is capable of causing potential damage to the information system or networks***
Vulnerability	***Weak point or a loophole which turns out to be an entry point for a threat to enter and exploit the system***
Risk	***Probability of a possible threat becoming successful***
Attack	***The very result of a threat which has materialized***
Exploit	***Using the vulnerability of a system or a network so that it may be attacked***

Quiz / Assessment

1) A person who steals information via communication system like credit card information, attacks PBXs, or is able to make calls free of cost, is called as a

a) Hacker	b) Ethical hacker	c) Whacker	d) Phreaker

2) A person who steals information via communication system like credit card information, attacks PBXs, or is able to make calls free of cost, is called as a

a) Threat	b) A Virus attack	c)Cyber terrorism	d)Hacktivism

3) What is the definition of Steganography

a) Attacking computer systems with an intention to weaker the economic or military strength of a nation

b) The practice of concealing messages or information within other non-secret text or data

c) Operating in a double blind environment to ethically hack into an organization

d) Study of technology and tools required to be an expert ethical hacker

Quiz / Assessment

4) A computer system or a Software that will go through a security evaluation is called as a

a) Target b) Security threat c) Risk d)Target of evaluation

5) If confidentiality and Integrity constitute two factors in a CIA triad, _______________is the third factor.

a) Accessibility b) Authentication c) Availability d)Authorization

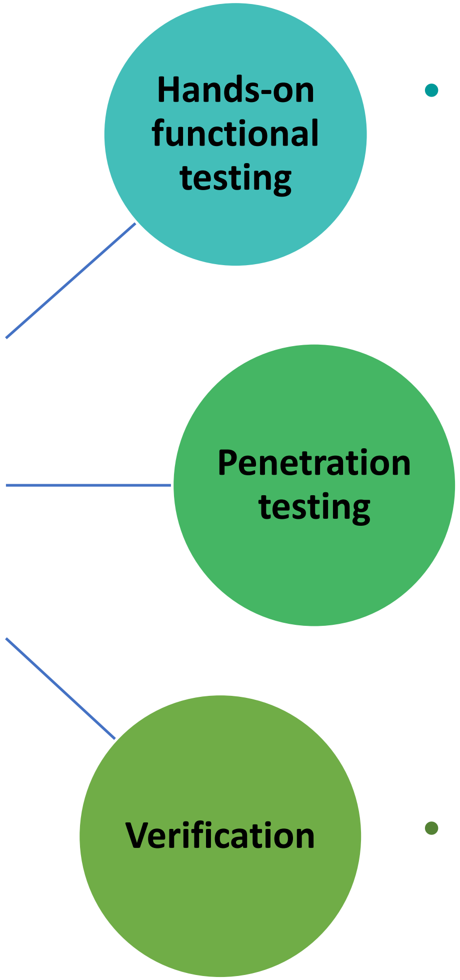
6) The term used for the protection of an individual's information that is identifiable is ______________

a) Identification b) Privacy c) Authentication d) Evaluation

Security Testing

Security testing may be defined as ***"a process that is used to determine that the security features of a system are implemented as par design".***

Security Testing consists of



Hands-on functional testing

- User performs this test to check the intended outcomes of the product.

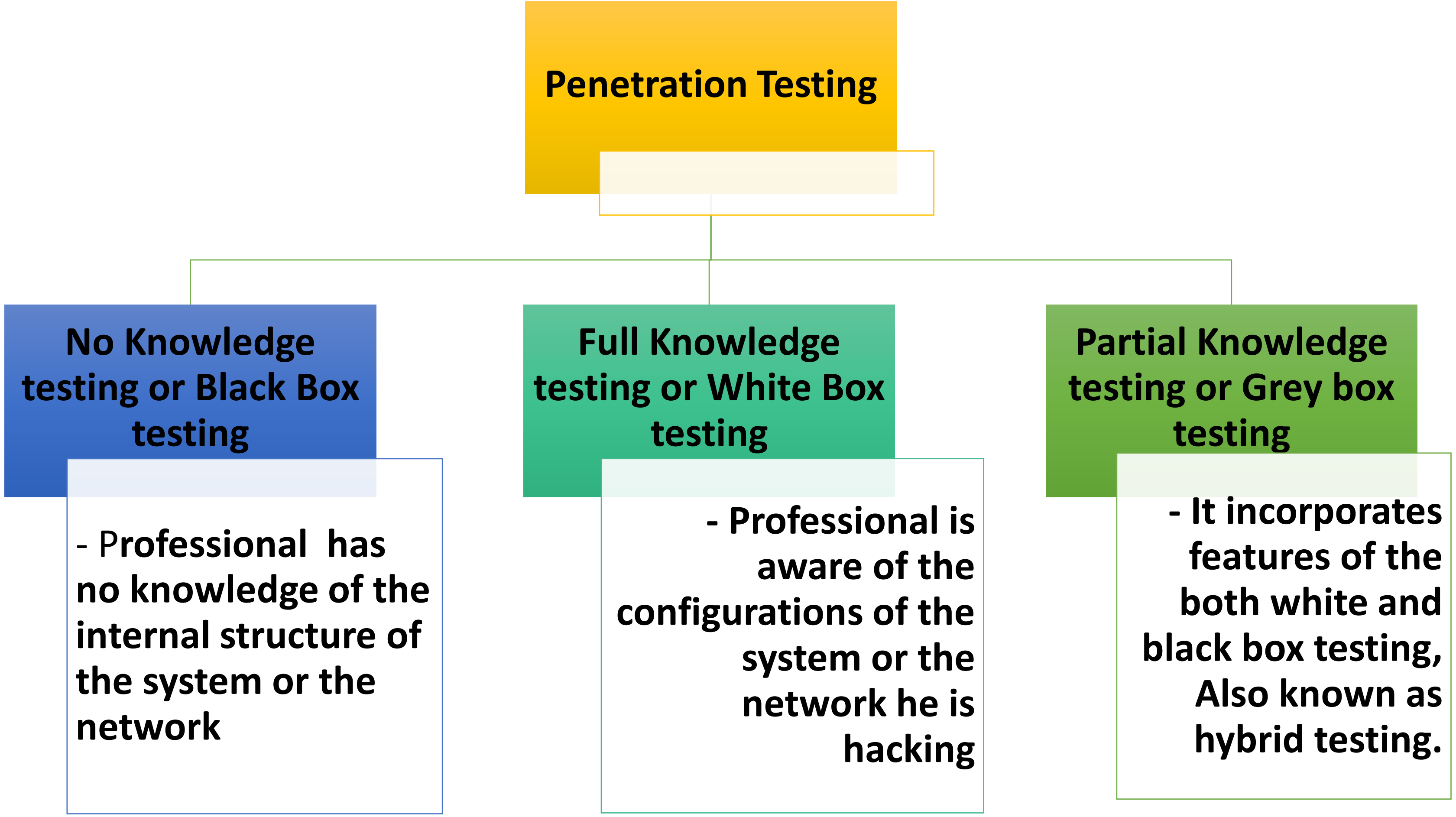
Penetration testing

- Method of identifying vulnerabilities present in a computer or a network.

Verification

- Process of evaluating a product in the development stage, against specified requirements.

Penetration Testing and its classifications



Penetration Testing

No Knowledge testing or Black Box testing

- Professional has no knowledge of the internal structure of the system or the network

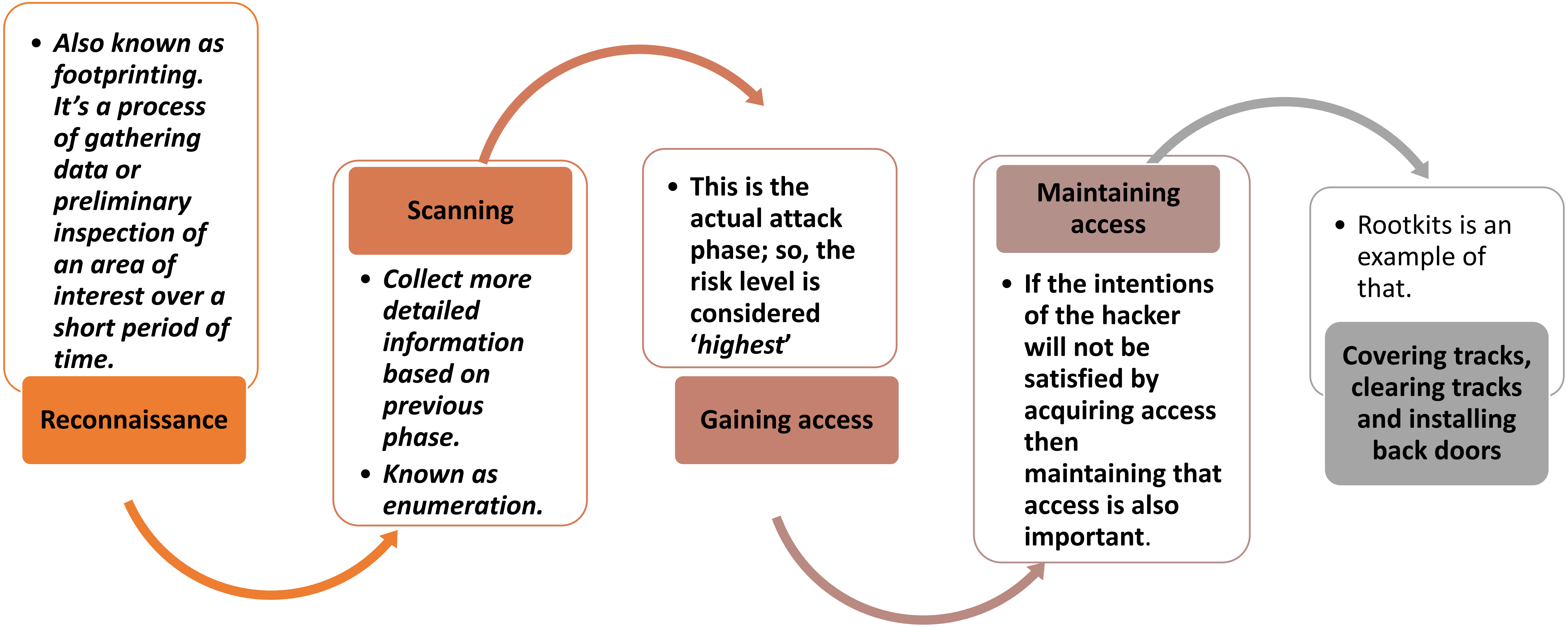
Full Knowledge testing or White Box testing

- Professional is aware of the configurations of the system or the network he is hacking

Partial Knowledge testing or Grey box testing

- It incorporates features of the both white and black box testing, Also known as hybrid testing.

Steps of Malicious Hacking



Reconnaissance

- ***Also known as footprinting. It’s a process of gathering data or preliminary inspection of an area of interest over a short period of time.***

Scanning

- ***Collect more detailed information based on previous phase.***
- ***Known as enumeration.***

Gaining access

- **This is the actual attack phase; so, the risk level is considered *‘highest’***

Maintaining access

- **If the intentions of the hacker will not be satisfied by acquiring access then maintaining that access is also important.**

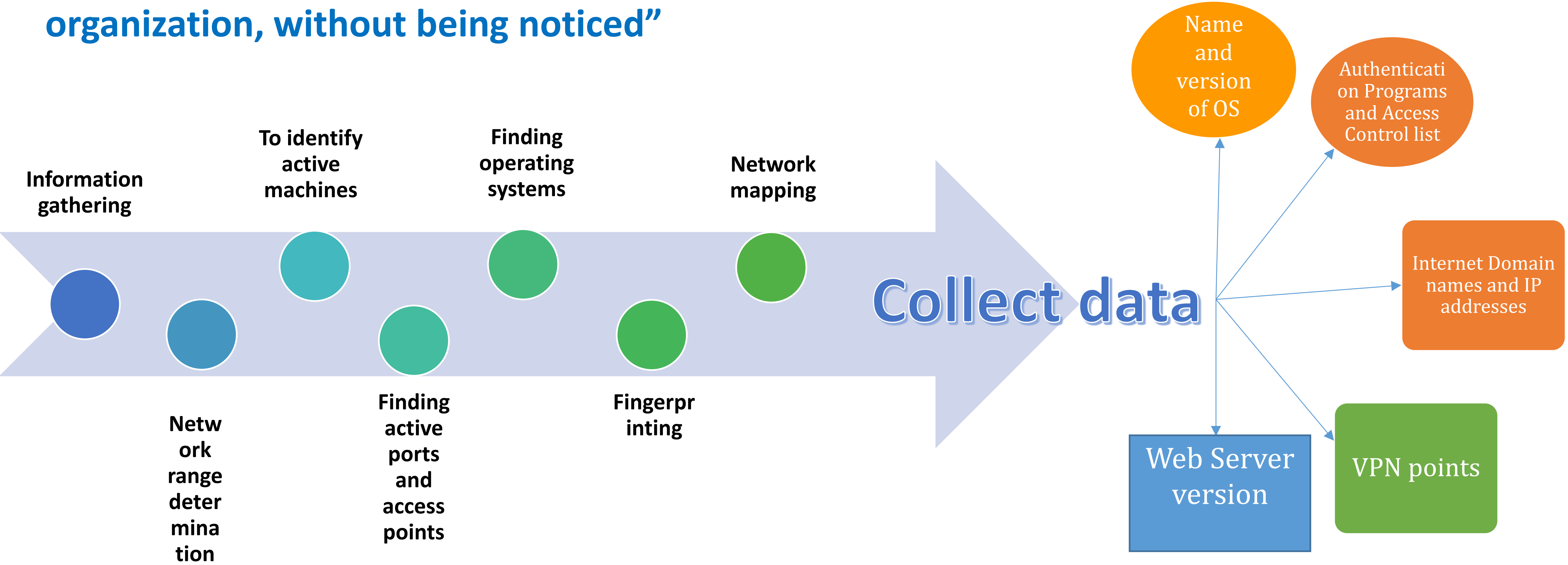
Covering tracks, clearing tracks and installing back doors

- Rootkits is an example of that.

Steps of Footprinting

7 Steps of Footprinting

"Its is a method used by the attacker to collect all the information about the organization, without being noticed"



Information gathering

Network range determination

To identify active machines

Finding active ports and access points

Finding operating systems

Fingerprinting

Network mapping

Collect data

Name and version of OS

Authentication Programs and Access Control list

Internet Domain names and IP addresses

VPN points

Web Server version

Types of Footprinting

Internet footprinting	Gather information from Internet
Organizational or Private footprinting	Collect data from an organization’s Web-based calendars email accounts
Pseudonymous footprinting	publishing information under a false name
Google hacking	Uses advanced operators in Google
Network footprinting	Active footprinting and Passive footprinting
DNS footprinting	DNS server is targeted to retrieve IP addresses
Website and E-mail footprinting	Phone numbers, e-mails and names are gathered from a company’s website after mirror imaging

Quiz/Assessment

7) In what is called as the actual attack phase, the hacker can gain access to the system at four levels. OS level, Application level, Network level and ___________________.

Physical layer	Denial of Service	Transport layer	Penetration layer

8) What is the full form of EC Council- a member supported organization which is known for Professional certifications in the field of IT Security

a) International council of e-Commerce Consultants	b) International Congregation of Electronic Commerce Consultants	c) International Council of Electronic Commerce Consultants	d) None of the above

9) Black box testing, White box testing and Grey box testing are the three types of Security testing. Among this, Grey box testing is also called as

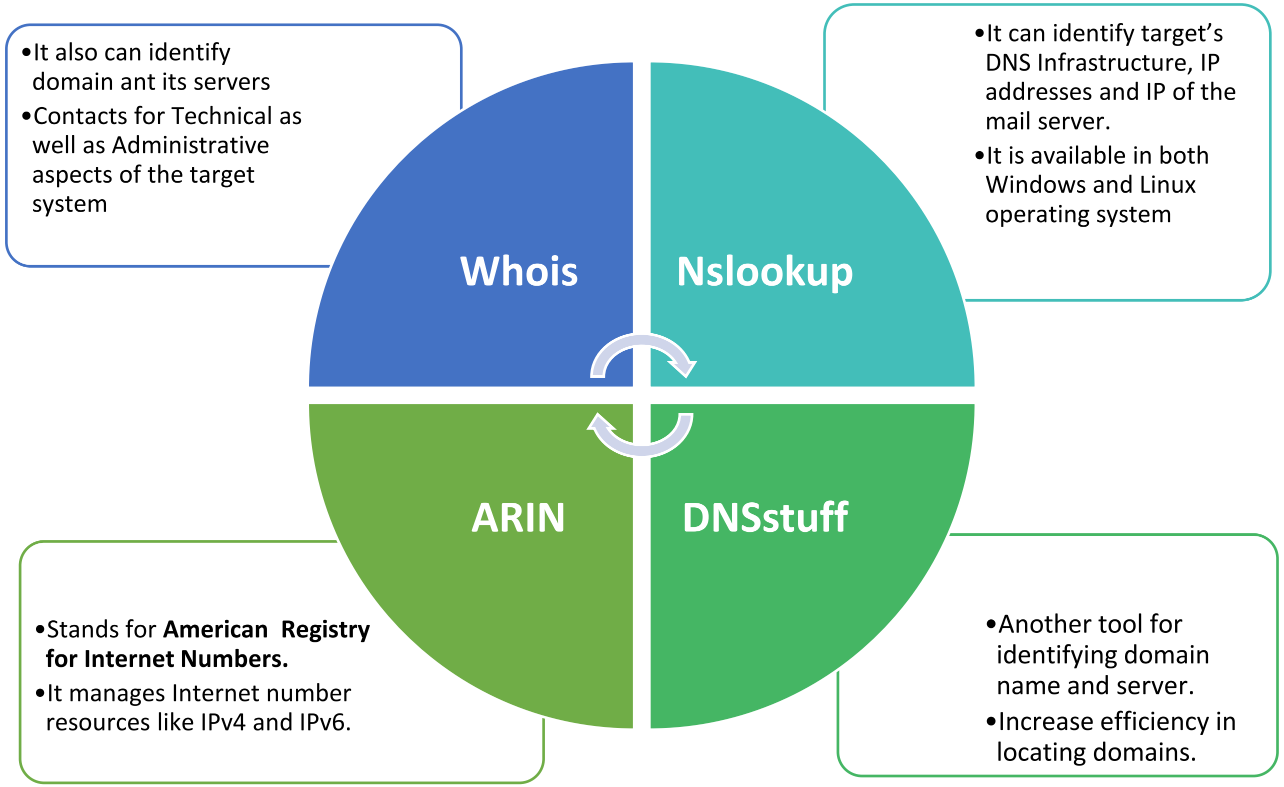
a) Penetration testing	b) Hybrid testing	c) Hybrid testing	d) Pink testing

DNS Footprinting

DNS footprinting is used to retrieve all information about DNS servers and any corresponding records of the target organization or computer system.

Tools used for DNS footprinting are:

- **Nslokup**
- **DNSstuff**
- **ARIN**
- **Whois**



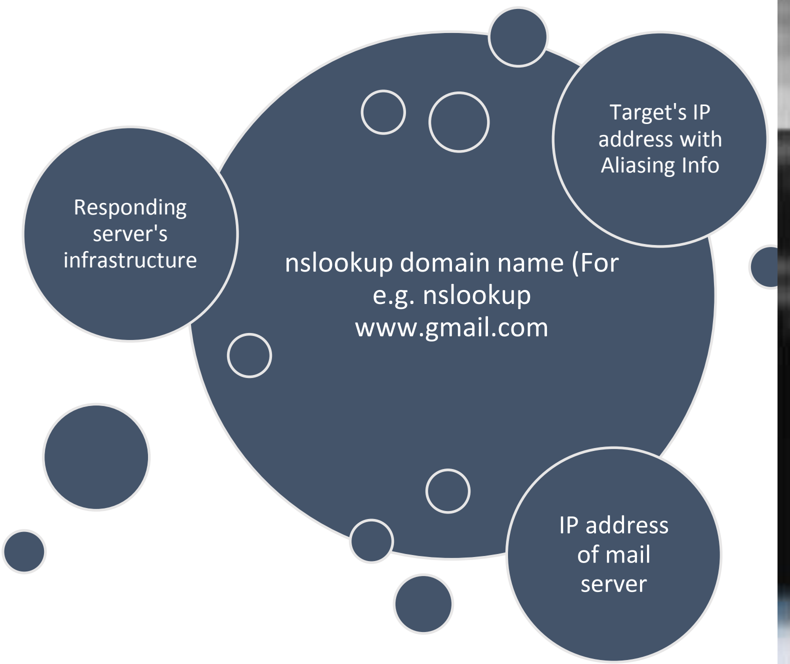
- It also can identify domain ant its servers
- Contacts for Technical as well as Administrative aspects of the target system

- It can identify target's DNS Infrastructure, IP addresses and IP of the mail server.
- It is available in both Windows and Linux operating system

- Stands for **American Registry for Internet Numbers.**
- It manages Internet number resources like IPv4 and IPv6.

- Another tool for identifying domain name and server.
- Increase efficiency in locating domains.

DNS Footprinting using Nslookup

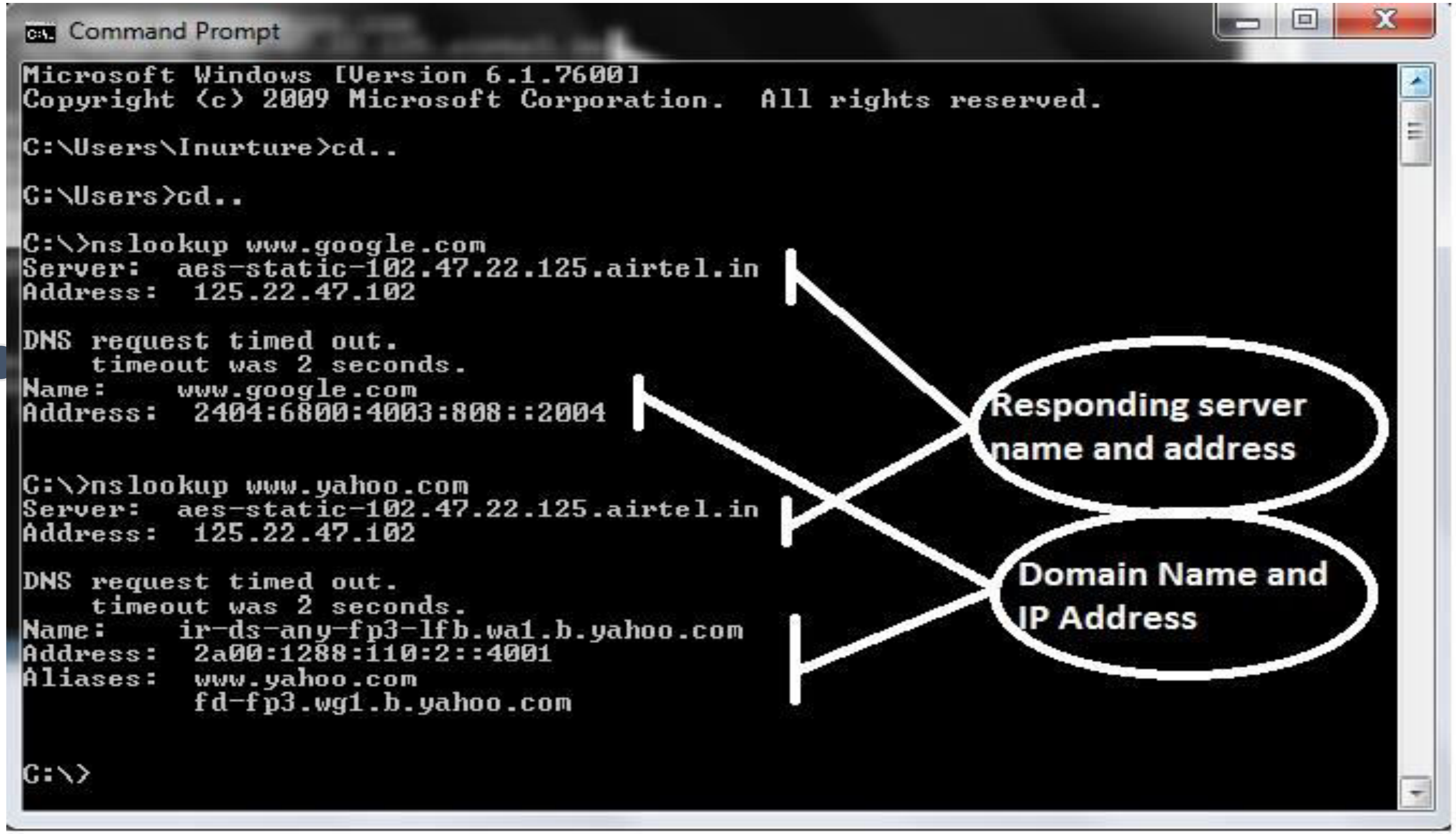


nslookup domain name (For e.g. nslookup www.gmail.com

Responding server's infrastructure

Target's IP address with Aliasing Info

IP address of mail server

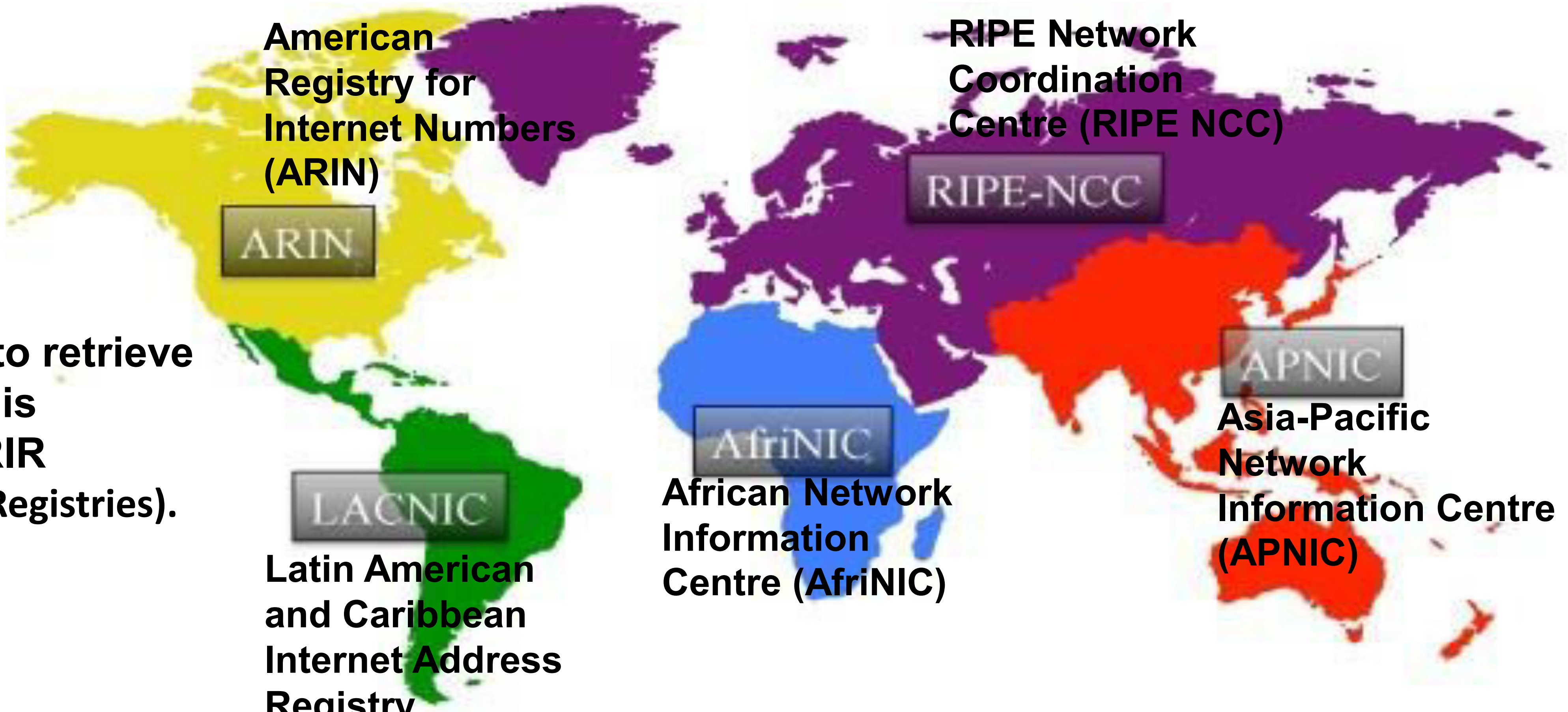


Command Prompt
Responding server name and address
Domain Name and IP Address

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Inurture>cd..

C:\Users>cd..

C:\>nslookup www.google.com
Server:  aes-static-102.47.22.125.airtel.in
Address:  125.22.47.102

DNS request timed out.
    timeout was 2 seconds.
Name:    www.google.com
Address:  2404:6800:4003:808::2004


C:\>nslookup www.yahoo.com
Server:  aes-static-102.47.22.125.airtel.in
Address:  125.22.47.102

DNS request timed out.
    timeout was 2 seconds.
Name:    ir-ds-any-fp3-lfb.wa1.b.yahoo.com
Address:  2a00:1288:110:2::4001
Aliases:  www.yahoo.com
          fd-fp3.wg1.b.yahoo.com


C:\>
```

DNS Footprinting using Whois

Whois searches to retrieve DNS information is available for all RIR (Regional Internet Registries).



American Registry for Internet Numbers (ARIN)

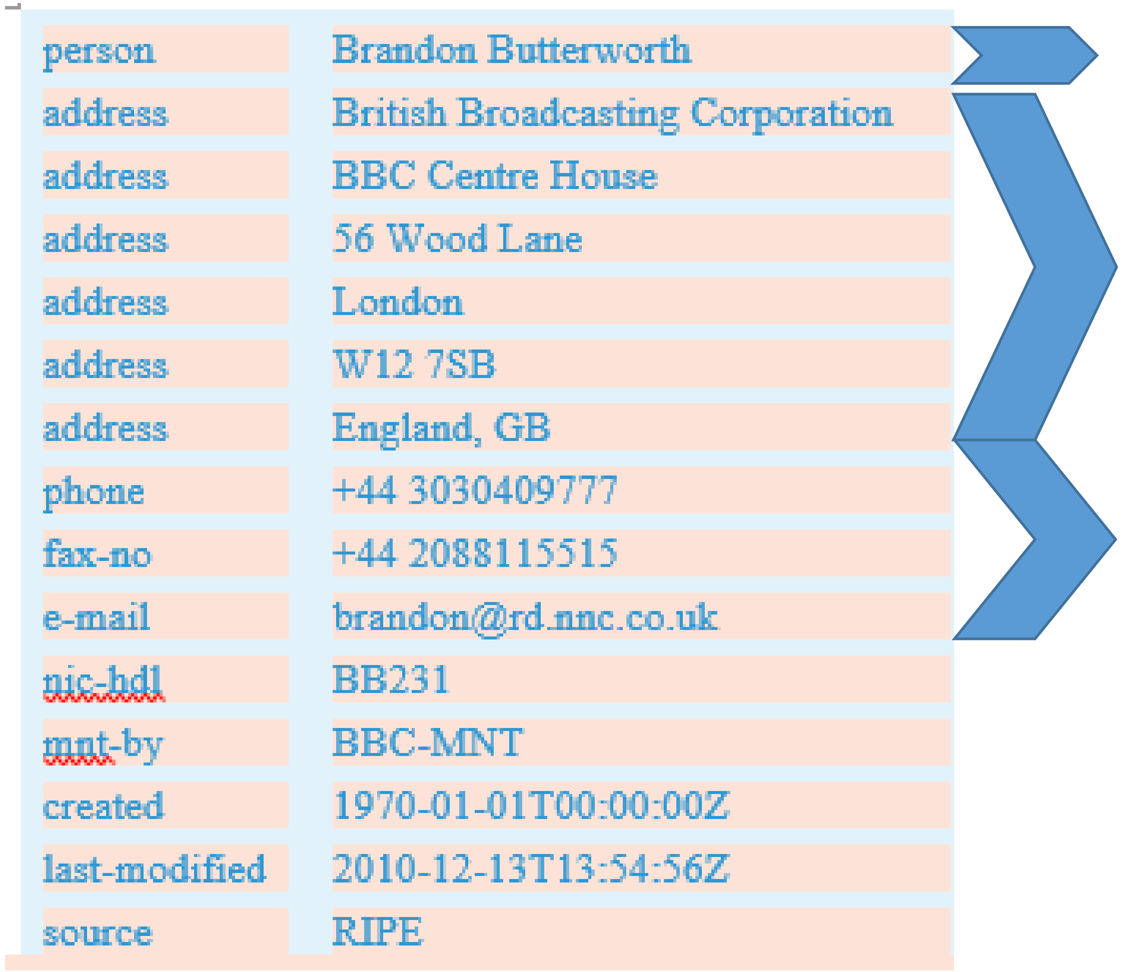
RIPE Network Coordination Centre (RIPE NCC)

Asia-Pacific Network Information Centre (APNIC)

African Network Information Centre (AfriNIC)

Latin American and Caribbean Internet Address Registry (LACNIC)

Whois Example



person	Brandon Butterworth
address	British Broadcasting Corporation
address	BBC Centre House
address	56 Wood Lane
address	London
address	W12 7SB
address	England, GB
phone	+44 3030409777
fax-no	+44 2088115515
e-mail	brandon@rd.nnc.co.uk
nic-hdl	BB231
mnt-by	BBC-MNT
created	1970-01-01T00:00:00Z
last-modified	2010-12-13T13:54:56Z
source	RIPE

Domain owner

Address Details

Contact Information

Locating the Network Range

It is the second phase 7 steps footprinting.

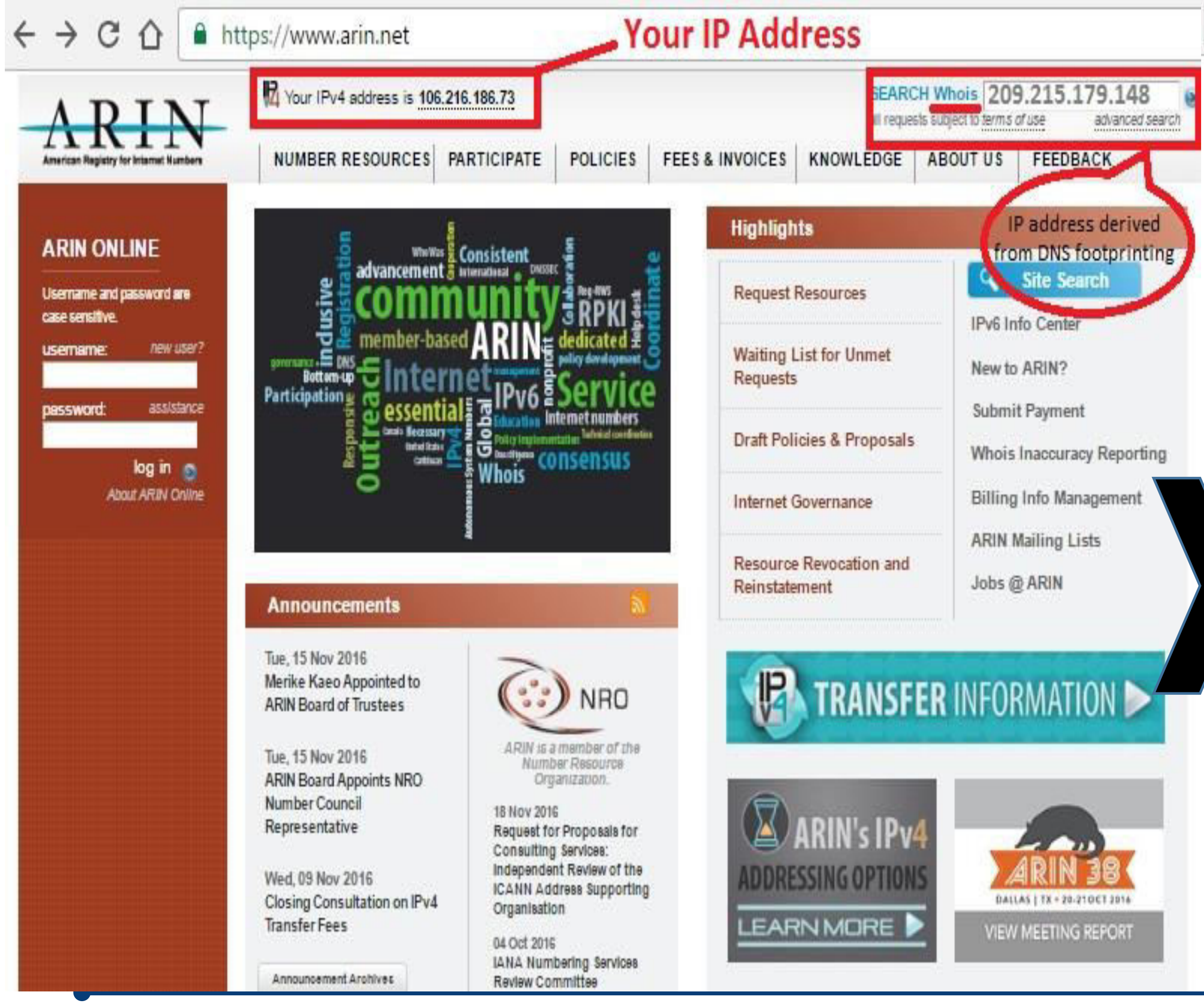
Network range can be located using:

- **ARIN**(American Registry for Internet Numbers) (www.arin.net)
- **Traceroute** and **TTL**

Using ARIIN:

- **Type www.arin.net in the address bar of browser.**
- **Type the IP address (retrieved by the method of DNS fotprinting) for which network range needs to be located**
- **Report with all network details will be generated.**

Locating the Network Range using ARIN



https://www.arin.net

Your IP Address

Your IPv4 address is 106.216.186.73

SEARCH Whois 209.215.179.148

all requests subject to terms of use — advanced search

IP address derived from DNS footprinting

Announcements

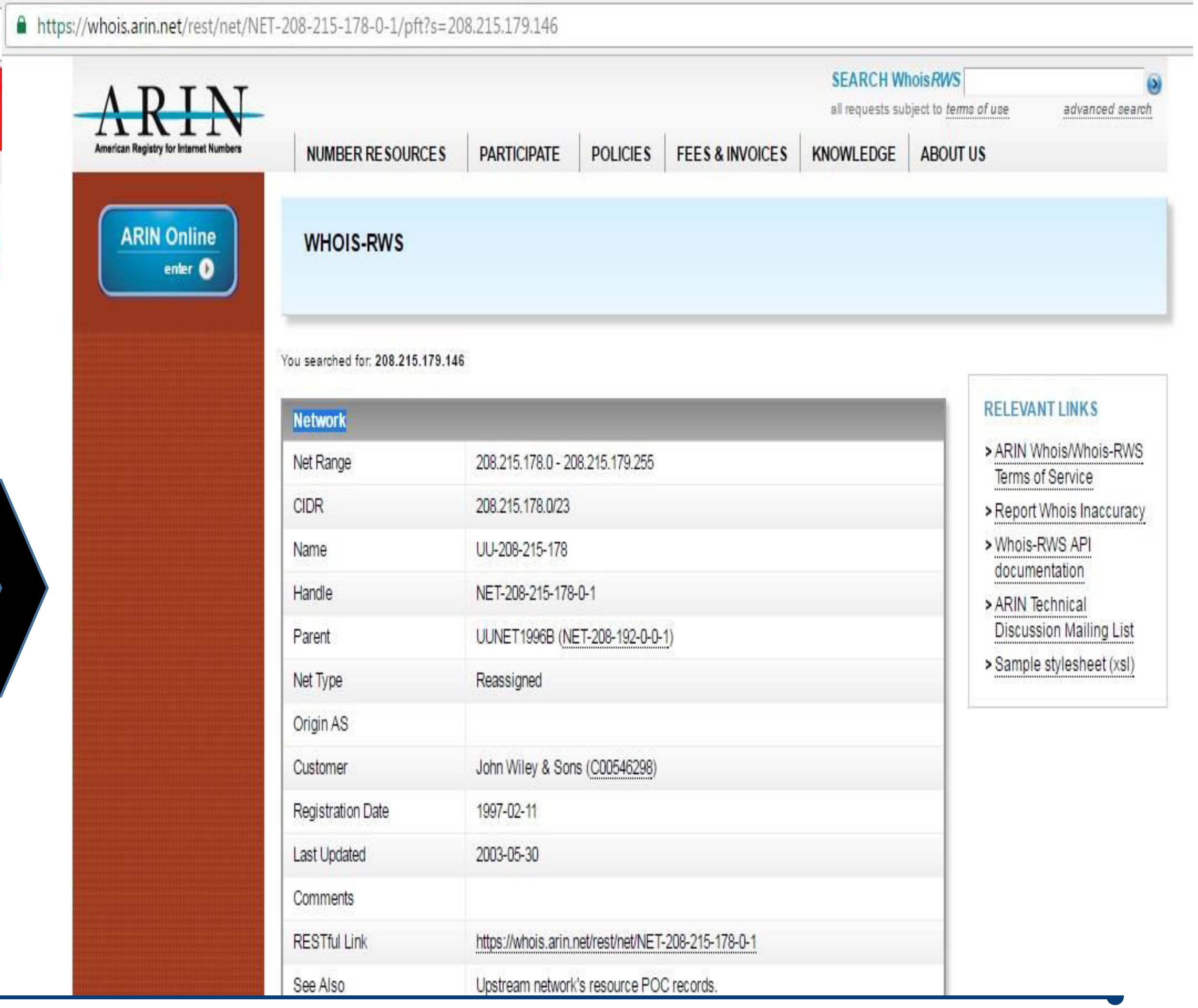
Tue, 15 Nov 2016
Merike Kaeo Appointed to ARIN Board of Trustees

Tue, 15 Nov 2016
ARIN Board Appoints NRO Number Council Representative

Wed, 09 Nov 2016
Closing Consultation on IPv4 Transfer Fees

18 Nov 2016
Request for Proposals for Consulting Services: Independent Review of the ICANN Address Supporting Organisation

04 Oct 2016
IANA Numbering Services Review Committee



https://whois.arin.net/rest/net/NET-208-215-178-0-1/pft?s=208.215.179.146

WHOIS-RWS

You searched for: **208.215.179.146**

Network	
Net Range	208.215.178.0 - 208.215.179.255
CIDR	208.215.178.0/23
Name	UU-208-215-178
Handle	NET-208-215-178-0-1
Parent	UUNET1996B (NET-208-192-0-0-1)
Net Type	Reassigned
Origin AS	
Customer	John Wiley & Sons (C00546298)
Registration Date	1997-02-11
Last Updated	2003-05-30
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-208-215-178-0-1
See Also	Upstream network's resource POC records.

RELEVANT LINKS

- ARIN Whois/Whois-RWS Terms of Service
- Report Whois Inaccuracy
- Whois-RWS API documentation
- ARIN Technical Discussion Mailing List
- Sample stylesheet (xsl)

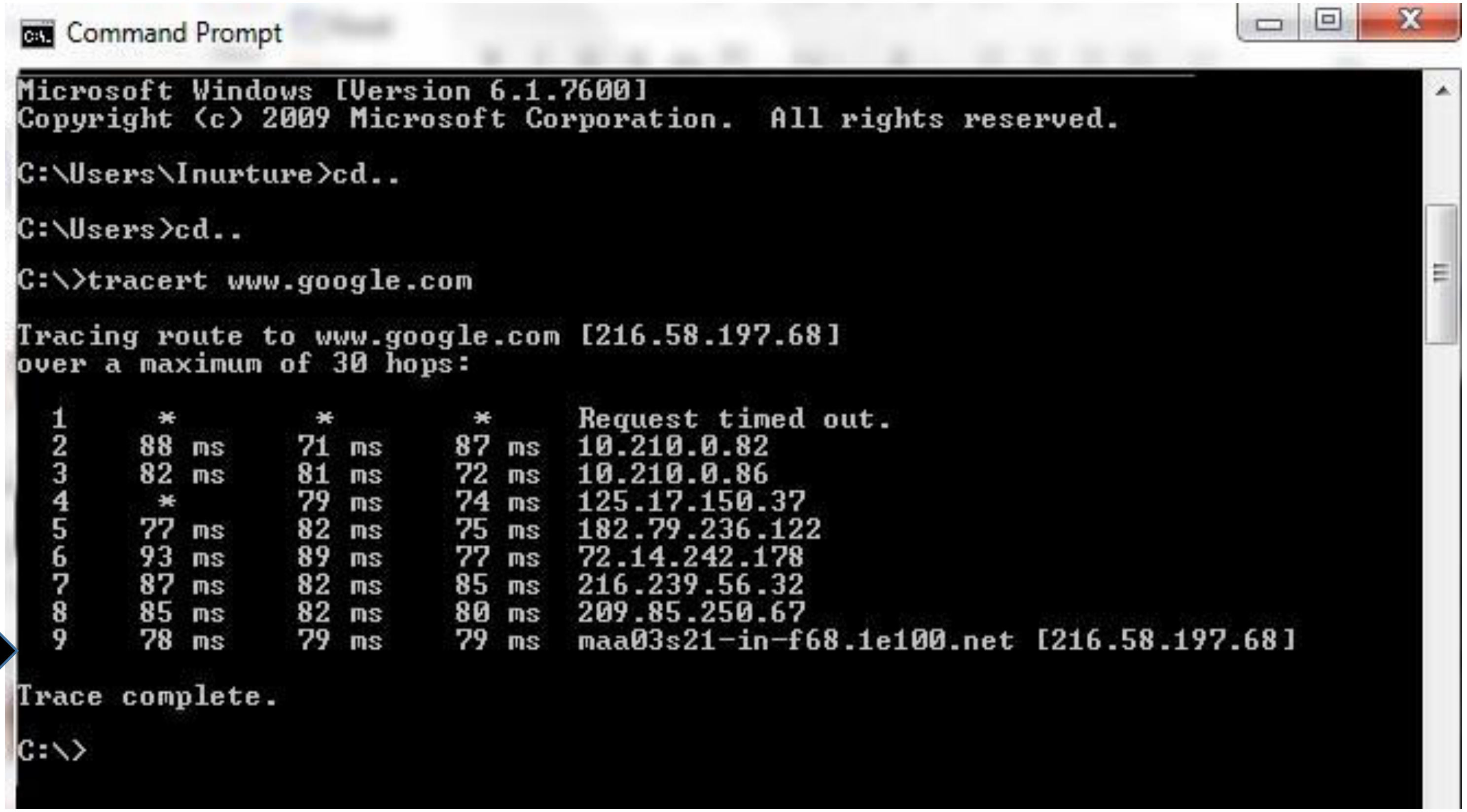
Locating the Network Range using Traceroute

Traceroute

1. Identify active machines in the network
2. Traces the path travelled by data packets

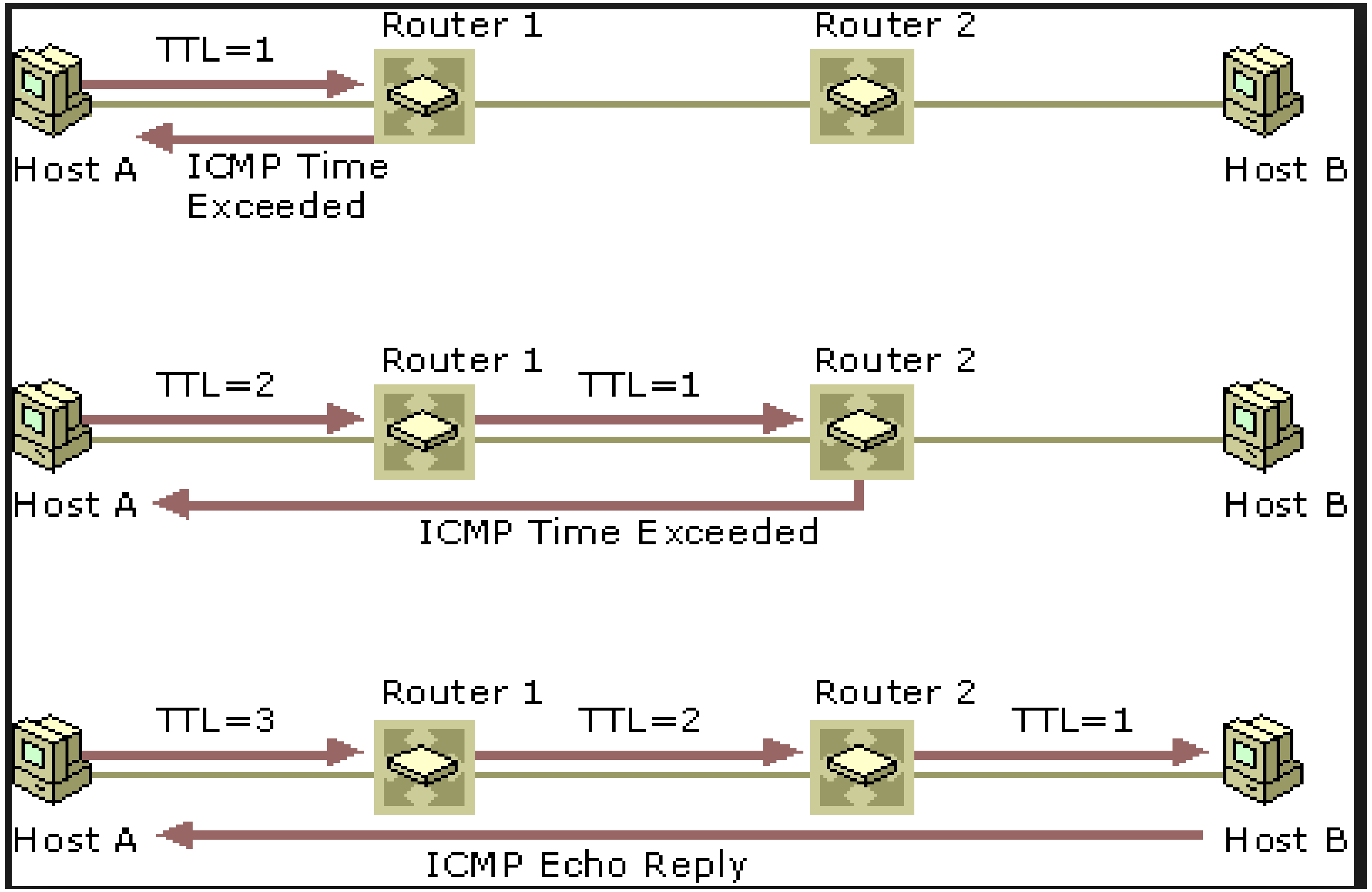
To do that:

- Go to command prompt →
- Type **tracert** followed by **domain name or IP address**



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Inurture>cd..

C:\Users>cd..

C:\>tracert www.google.com

Tracing route to www.google.com [216.58.197.68]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2    88 ms    71 ms    87 ms  10.210.0.82
  3    82 ms    81 ms    72 ms  10.210.0.86
  4     *       79 ms    74 ms  125.17.150.37
  5    77 ms    82 ms    75 ms  182.79.236.122
  6    93 ms    89 ms    77 ms  72.14.242.178
  7    87 ms    82 ms    85 ms  216.239.56.32
  8    85 ms    82 ms    80 ms  209.85.250.67
  9    78 ms    79 ms    79 ms  maa03s21-in-f68.1e100.net [216.58.197.68]

Trace complete.

C:\>
```

How Traceroute works…



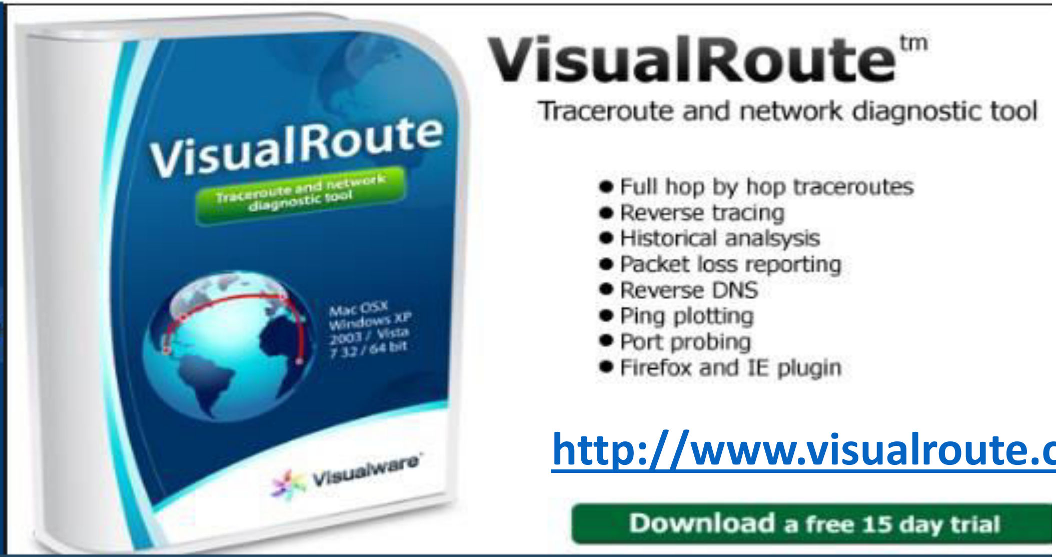
Outcome of Traceroute:

- Retrieve information like network topology,
- trusted routers and firewall positioning.

Intention of Hacker:

- Visualize network structure.
- Prepare a blueprint of network for hacking
- To know about the geographical location of the router

Traceroute Visual Interface



VisualRoute™

Traceroute and network diagnostic tool

- Full hop by hop traceroutes
- Reverse tracing
- Historical analsysis
- Packet loss reporting
- Reverse DNS
- Ping plotting
- Port probing
- Firefox and IE plugin

http://www.visualroute.com/

Download a free 15 day trial

https://www.pingplotter.com/

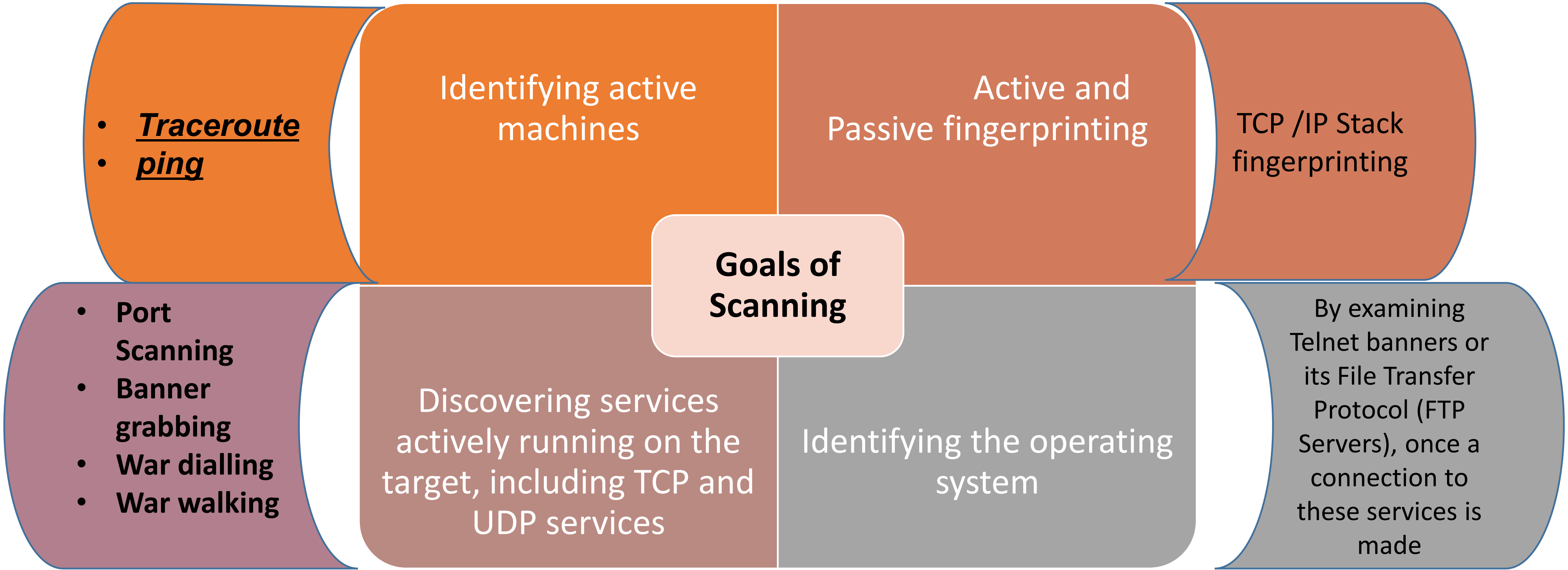
Visual Proof of Network Problems

Proving the cause of connection issues
is easier when everyone can see

Scanning

Scanning

It is defined as the 'investigation of an information system or network to identify any lapses in its security, using tools and techniques'.



Goals of Scanning

Identifying active machines

- ***Traceroute***
- ***ping***

Active and Passive fingerprinting

TCP /IP Stack fingerprinting

Discovering services actively running on the target, including TCP and UDP services

- **Port Scanning**
- **Banner grabbing**
- **War dialling**
- **War walking**

Identifying the operating system

By examining Telnet banners or its File Transfer Protocol (FTP Servers), once a connection to these services is made

Scanning Tools

1) Hping
2) Nessus
3) NMAP
4) SNORT
5) TCPview

Get started with the world's most powerful detection software

Download Snort and the rules you need to stay ahead of the latest threats

Keep up-to-date with the latest changes and documentation

Quiz / Assessment

10) Which are the utilities used for identifying active machines on a network?			
a) ping and Traceroute	b)Nslookup and Whois	c)Net view and Nbtscan	d)None of the above
11) Which of the below options best define Ping Sweeps?			
Detecting live machines on the target network	Identifying the operating system	Process where ping is executed on a batch of devices	Identifying specific applications
12) A port can be found in either ‘open’, ‘closed’ or -------- state			
a) filtered	b) active	c) Inactive	Null

Quiz / Assessment

13) TCP/IP stack fingerprinting exploits the fact that the ---------- protocol is implemented differently by OS and vendor			
a) UDP	b) POP3	c) SNMP	d) TCP/IP
14) -------------- is a free security auditing tool for			
a) HPing	b) Legion	c) Nessus	d)NMap

Summary

- ✓ Ethical Hacking is study of tools and techniques required to add more protection to computer systems and networks, from the threats hacking
- ✓ Confidentiality, Integrity and Availability form what is called CIA triad
- ✓ Black Box testing, White box testing and Grey box testing are the three types of Penetration testing used be security professionals, with their own set of features
- ✓ Five stages on malicious hacking are Reconnaissance, Scanning, gaining access, maintaining access and covering tracks
- ✓ EC- Council has defined seven steps in footprinting which is followed by every ethical hacker
- ✓ Precise use of tools is a very important requirement for ethical hacker to conduct his analysis and presenting the facts

e-References & External Resources

- introduction to ethical hacking, types of security testing, skills of ethical hacker and job responsibilities of an ethical hacker https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390
- www.telegraph.co.uk/technology/6670127/Top-10-**most-famous-hackers**.html

1. *The CEH Prep Guide, the comprehensive guide to Certified Ethical Hacking by Ronald L. Krutz and Russell Dean Vines*
2. *Official Certified Ethical Hacker Review Guide by Kimberly Graves*
3. *Unofficial Guide to Ethical Hacking by Ankit Fadia*

Activity

Brief description of activity

Online Activity
(30in)

Description:

1. Assume that you are a part of an ethical hacking team that recently conducted a white box testing for a firm and you have your results with you. Prepare a report to present your facts before the firm using one of the templates available on the internet or a sample report.

Note: You may make necessary assumptions as applicable