CYBER SECURITY

MODULE - 1

Introduction to Ethical Hacking

Module Duration : 1 hour

What is hacking ?

Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator’s original purpose.

(or)

The activity of illegally using a computer to access information stored on another computer system or to spread a computer virus

Hacker Classes

- Script Kiddies
  - Novice Hackers, Little Technical Knowledge
  - Uses other People's Pre-made Tools
- Black Hats
  - Uses Hacking Skills Purely For Offensive and Malicious Purposes.
  - Motivated By Money, revenge, Crime, Terrorism, Activism, etc.
- White Hats
  - Uses Hacking Skills to help defend against network attacks and makes system more secure.
  - Often called security consultants, analysts or Engineers

Hacker Classes

- Script Kiddies
  - Novice Hackers, Little Technical Knowledge
  - Uses other People's Pre-made Tools
- Black Hats
  - Uses Hacking Skills Purely For Offensive and Malicious Purposes.
  - Motivated By Money, revenge, Crime, Terrorism, Activism, etc.
- White Hats
  - Uses Hacking Skills to help defend against network attacks and makes system more secure.
  - Often called security consultants, analysts or Engineers

Hacker Classes

- Grey Hats
  - Can Be good or bad or both.
  - Often Reformed black hats or Rouge white hats.
- Cyber terrorists
  - Organized Groups intent on spreading fear of data disruption as a means of meet their Goals.
  - Could be for religious, political, nationalistic or activist goals .
- State sponsored hacker
  - Trained, funded and supported agents of nation-state or government.
  - Goals are espionage, cyber warfare

Hacker Classes

- Hacktivists
  - Hackers who launch attacks to spread their particular message about a Cause.
  - May deface website, cause denial of service attacks, disclose data.

- Corporate hackers
  - Target an organization's property data or intellectual properties
  - Goal is to get a competitive advantage, blackmail, or make money

What is Ethical Hacking?

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network.

GOALS:

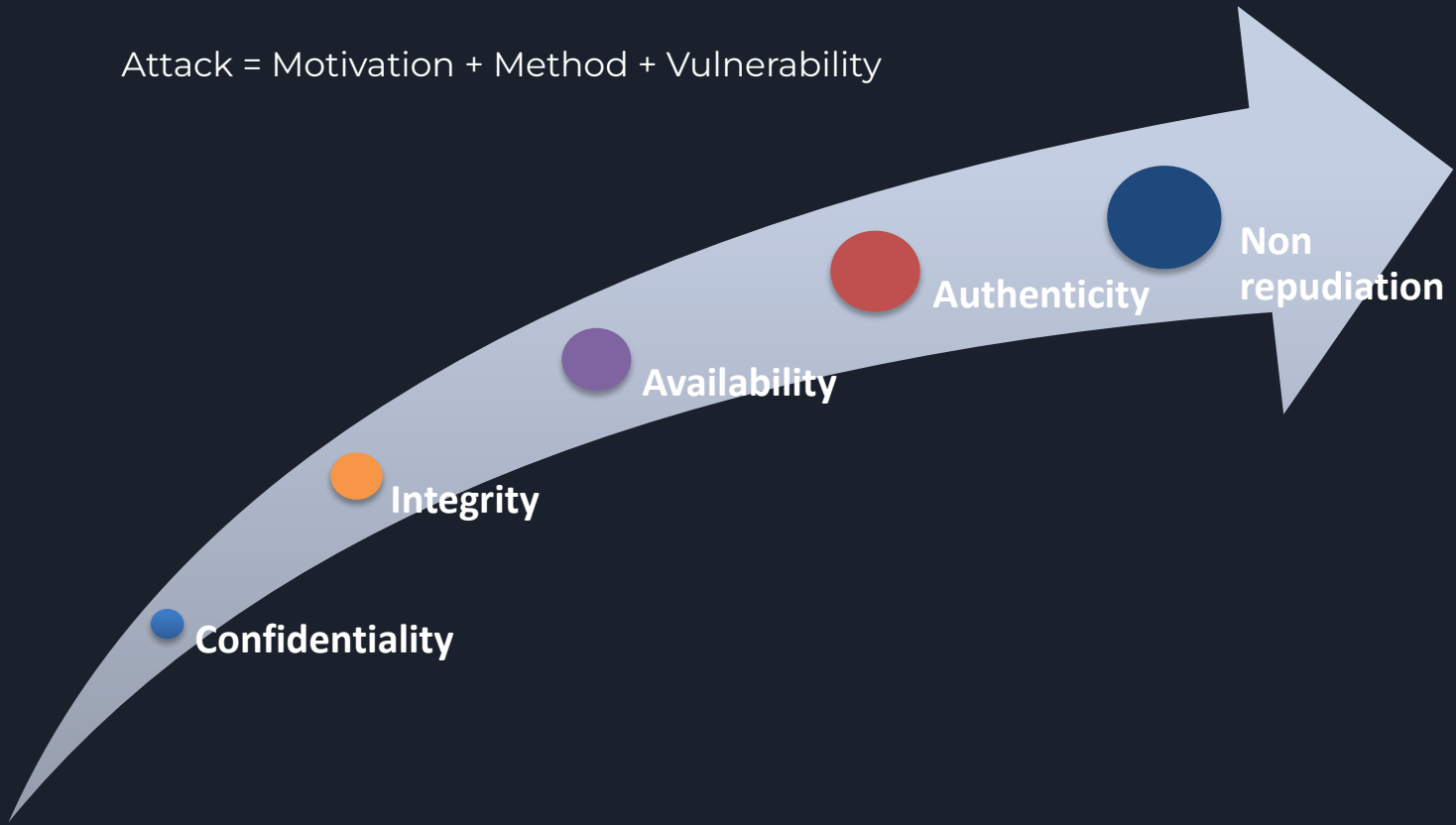
- To determine flaws and Vulnerabilities
- To provide quantitative metrics for evaluating systems and networks
- To determine risk to the organization
- To design mitigating controls
- Create security policies

Terms used in Ethical hacking

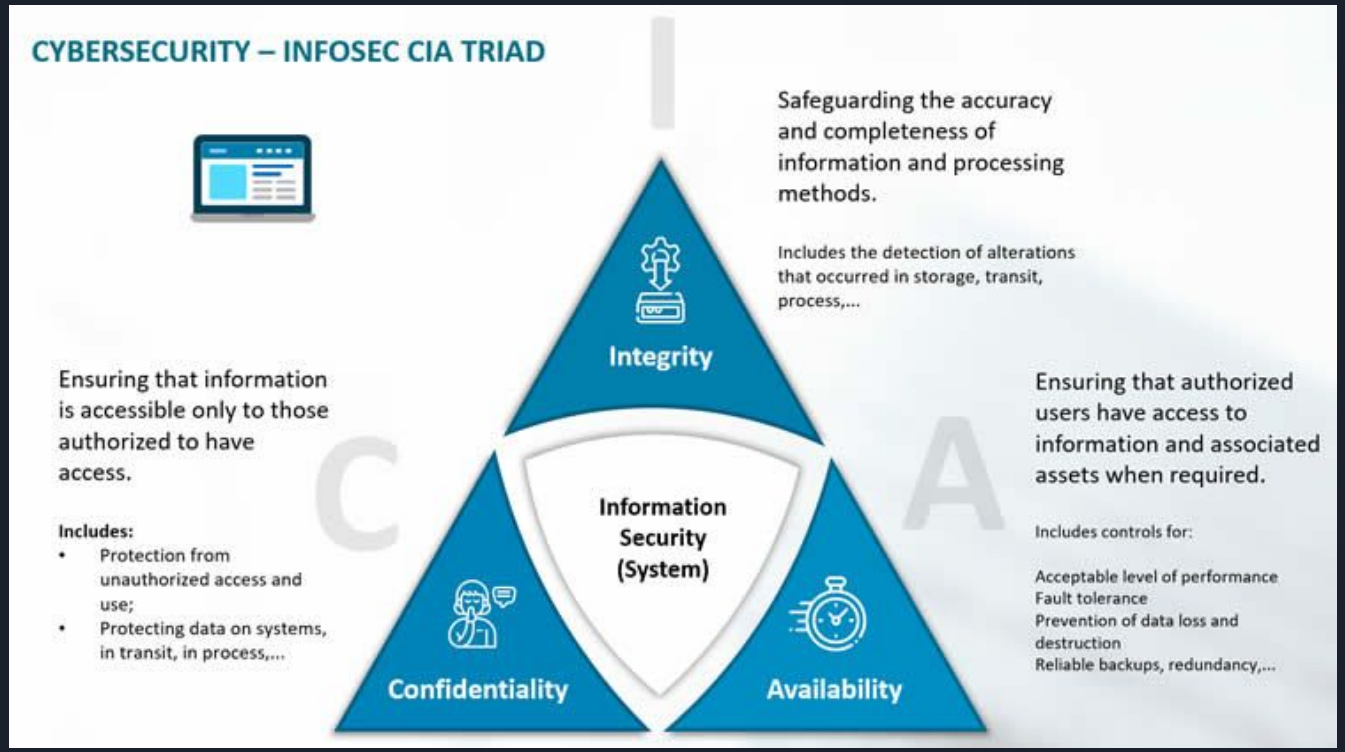
TERMS	MEANING
Threat	*Activity or occurrence that is capable of causing potential damage to the information system or networks*
Vulnerability	*Weak point or a loophole which turns out to be an entry point for a threat to enter and exploit the system*
Risk	*Probability of a possible threat becoming successful*
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*

Importance of Information Security

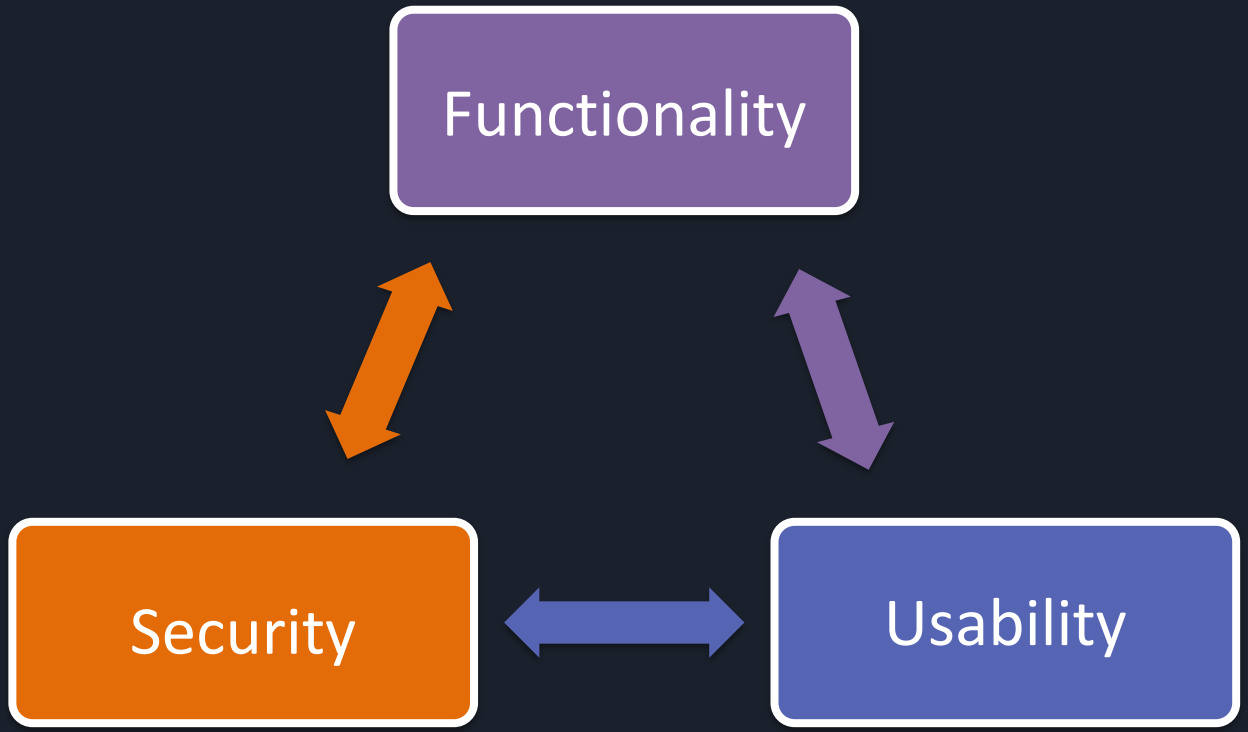
Attack = Motivation + Method + Vulnerability



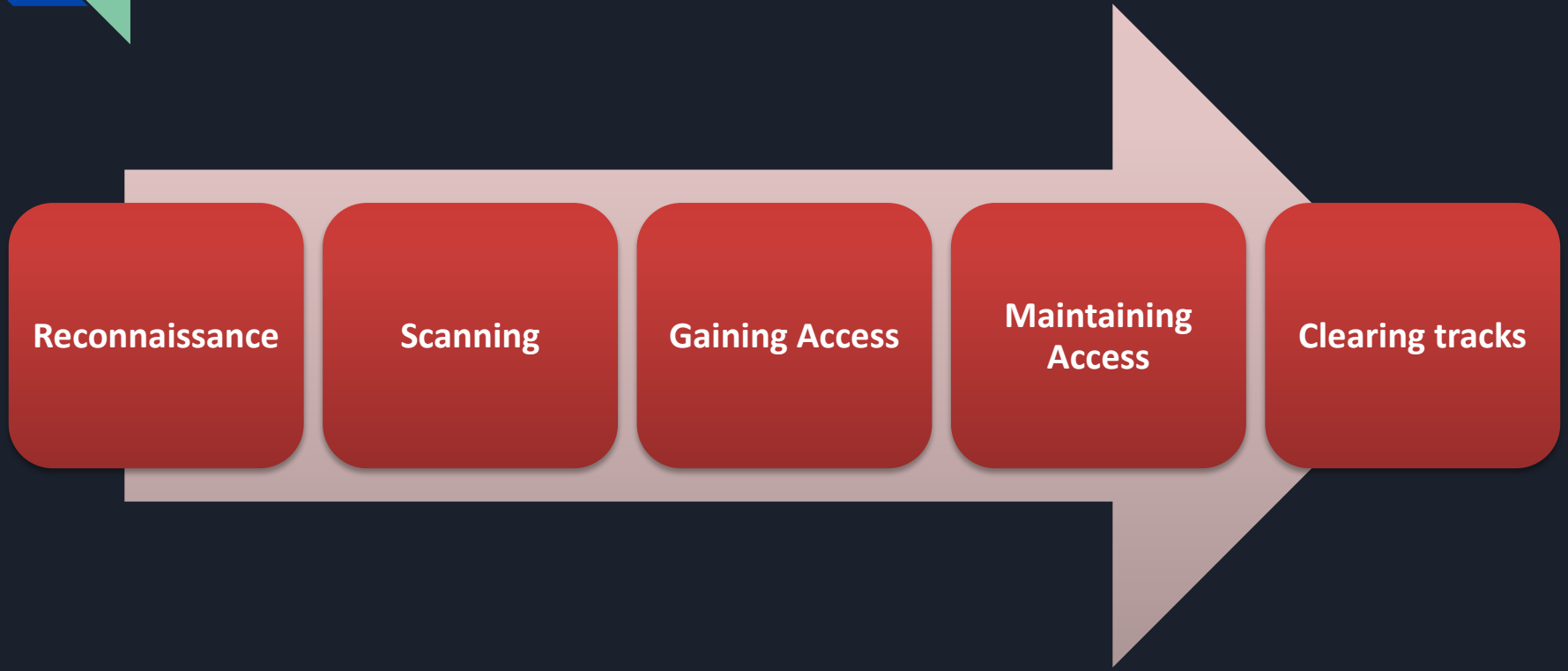
CIA Triad


CYBERSECURITY – INFOSEC CIA TRIAD
Safeguarding the accuracy and completeness of information and processing methods.
Includes the detection of alterations that occurred in storage, transit, process,...
Integrity
Ensuring that information is accessible only to those authorized to have access.
Includes:
• Protection from unauthorized access and use;
• Protecting data on systems, in transit, in process,...
Information Security (System)
Confidentiality
Availability
Ensuring that authorized users have access to information and associated assets when required.
Includes controls for:
Acceptable level of performance
Fault tolerance
Prevention of data loss and destruction
Reliable backups, redundancy,...

Security, Functionality and Usability Triangle



Hacking Methodology



Hacking Methodology

- Reconnaissance: Preparing Phase-attacker gathers information about the target.
- Scanning: attacker gathers information and vulnerability information.
- Gaining access: Attacker actually penetrates system.
- Maintaining access: attacker tries to keep, extend, and escalate access to systems.
- Clearing tracks: attackers tries to avoid detection.

CYBER SECURITY

MODULE - 2

Reconnaissance

Module Duration : 2 hours

Reconnaissance

- Footprinting, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment.

- Using footprinting you can find various ways to intrude into the target organization's network system.

- It is considered ″methodological" because critical information is sought based on a previous discovery.

Reconnaissance

Know Security Posture

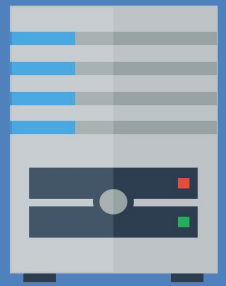
Reduce attack Area

Build Information Database

Draw Network Map

Reconnaissance

Collect Elementary Intel

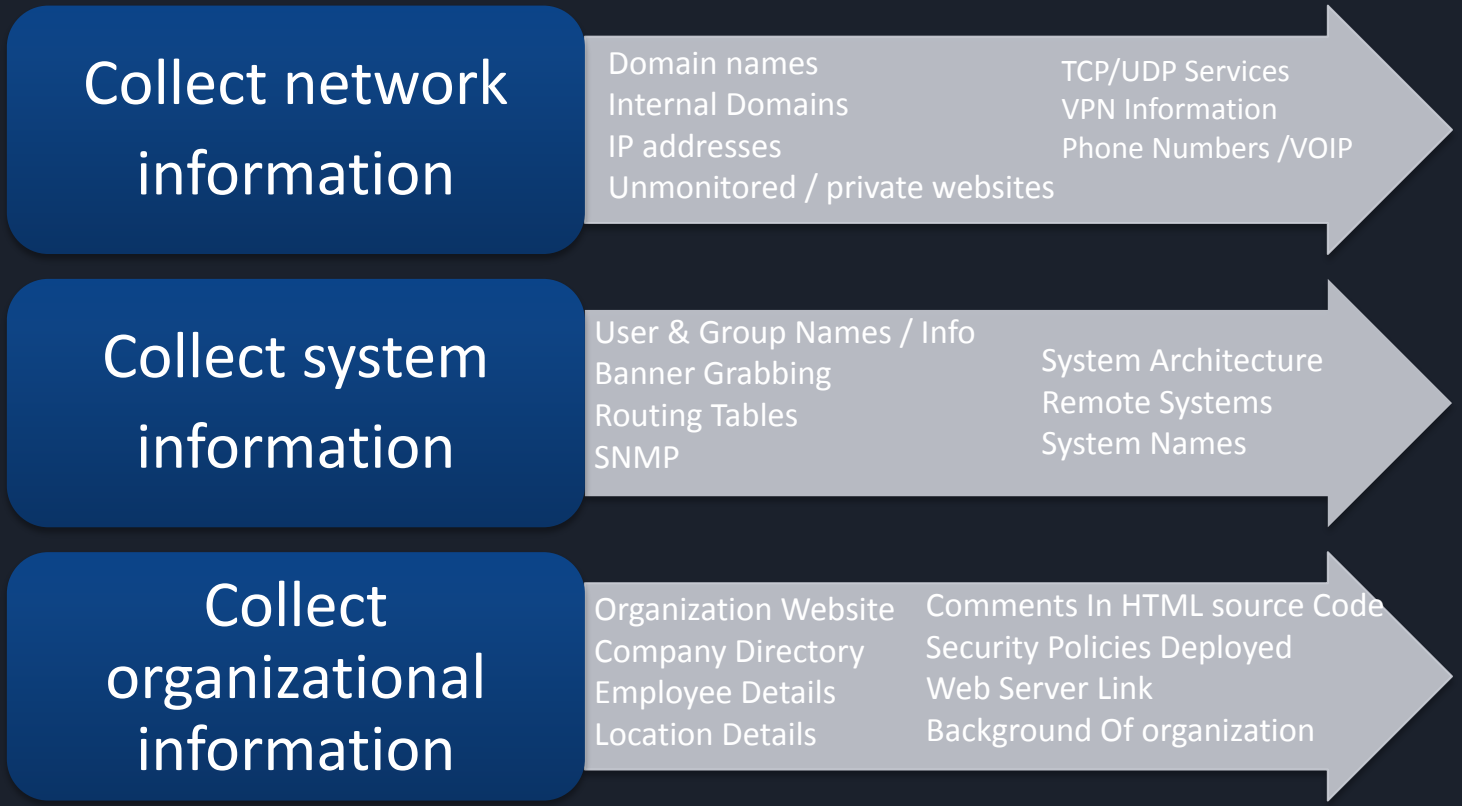


Discover OS, Web Servers & Platforms

Perform Queries

Discover Vulnerabilities

Reconnaissance



Reconnaissance

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting Through Social Engineering
- Footprinting Through Social Networking Site
- Footprinting Using Shodan
- Footprinting Through Searching
- Website Footprinting
- Email Footprinting
- Competitive intelligence
- Footprinting Using Google

Reconnaissance

You can use the public record websites to find information about people's

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of private residences

Footprinting through Job Sites

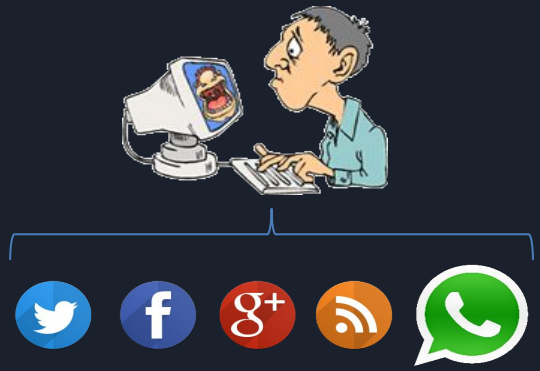
http://www.peekyou.com/

http://www.intelius.com/

http://www.peoplelookup.com/

Reconnaissance

Passive foot printing requires no direct contact with organization e.g. Internet



Active foot printing may mean some kind of direct contact or interaction with organization E.g..

- Social engineering
- Entering premises
- Taking photos and video

Reconnaissance

CYBER SECURITY

MODULE - 3

Network & Vulnerability Scanning

Module Duration : 2 hours

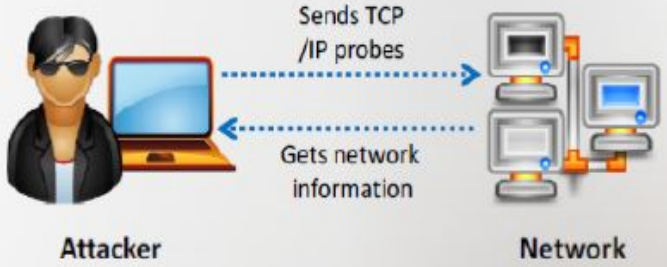
Scanning

Pre-attack phase

Port Scanning

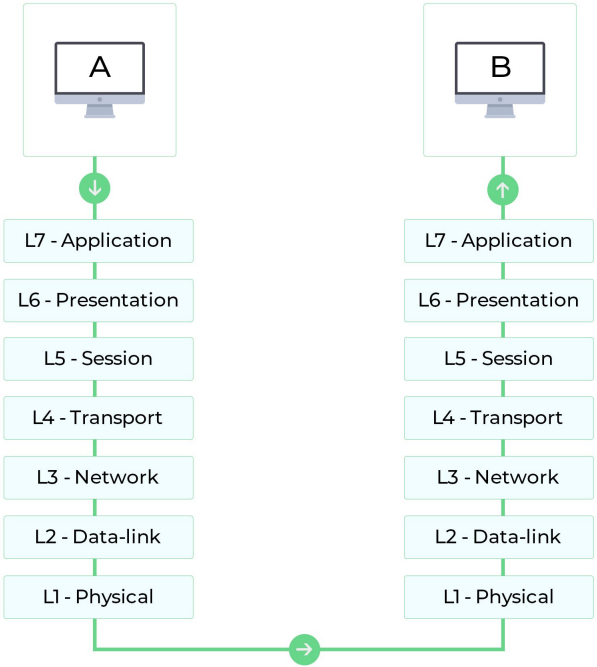
Extract information

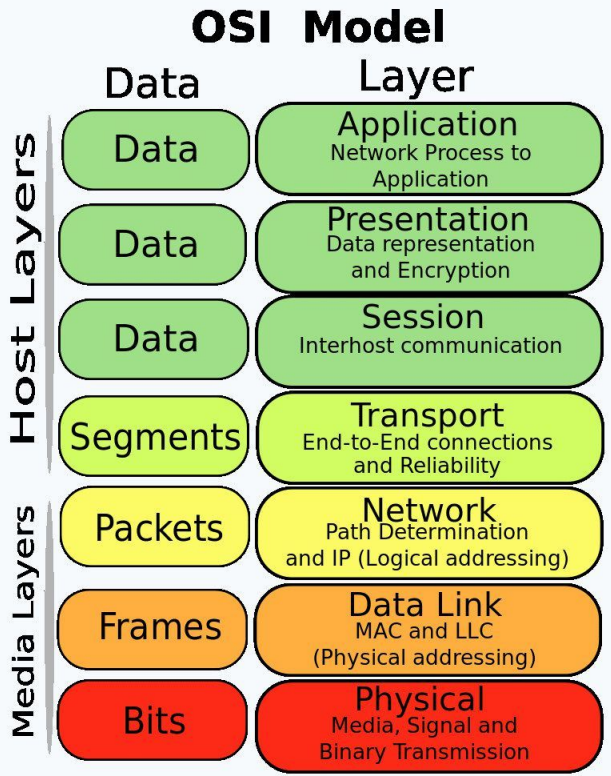
- Network scanning refers to a set of procedures for **identifying hosts**, **ports**, and **services in a network**
- Network scanning is one of the **components of intelligence gathering** an attacker uses to create a profile of the target organization

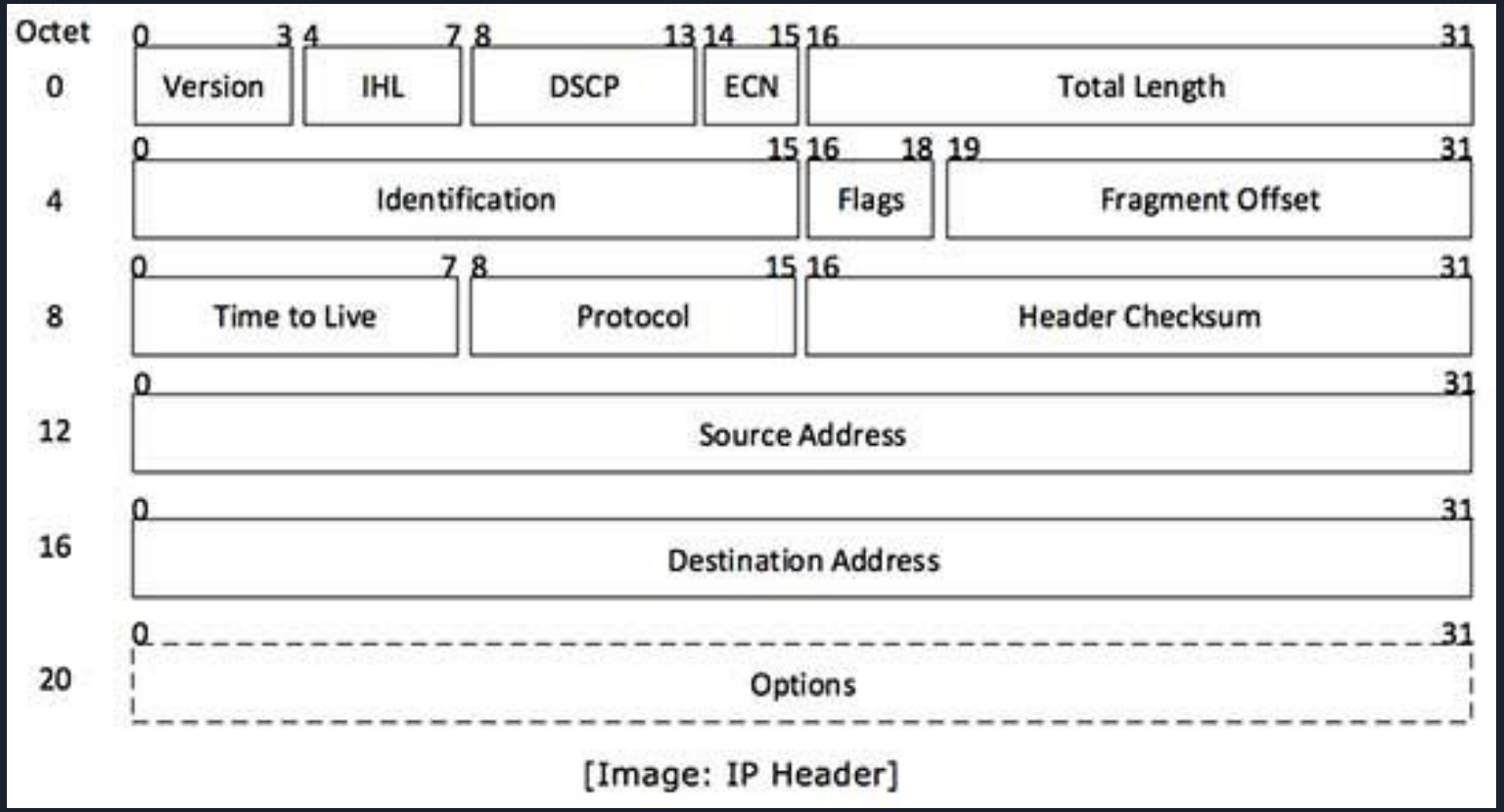


Objectives of Network Scanning

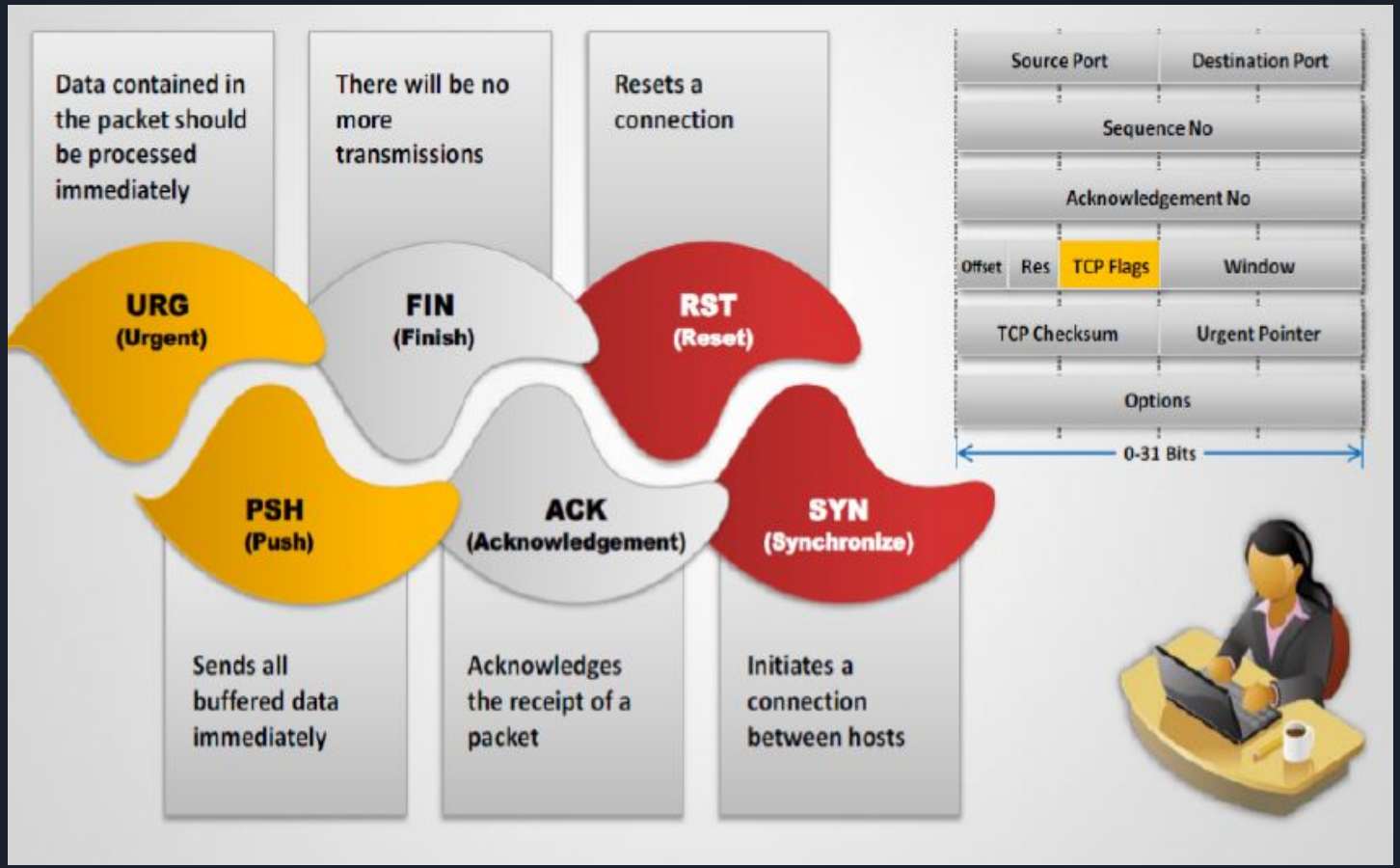
- To discover live hosts, IP address, and open ports of live hosts
- To discover operating systems and system architecture
- To discover services running on hosts
- To discover vulnerabilities in live hosts


A
B
L7 - Application
L6 - Presentation
L5 - Session
L4 - Transport
L3 - Network
L2 - Data-link
L1 - Physical
L7 - Application
L6 - Presentation
L5 - Session
L4 - Transport
L3 - Network
L2 - Data-link
L1 - Physical


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission



[Image: IP Header]


Data contained in the packet should be processed immediately
There will be no more transmissions
Resets a connection
URG (Urgent)
FIN (Finish)
RST (Reset)
PSH (Push)
ACK (Acknowledgement)
SYN (Synchronize)
Sends all buffered data immediately
Acknowledges the receipt of a packet
Initiates a connection between hosts
Source Port
Destination Port
Sequence No
Acknowledgement No
Offset
Res
TCP Flags
Window
TCP Checksum
Urgent Pointer
Options
0-31 Bits

TCP uses a **three-way handshake** to establish a connection between server and client

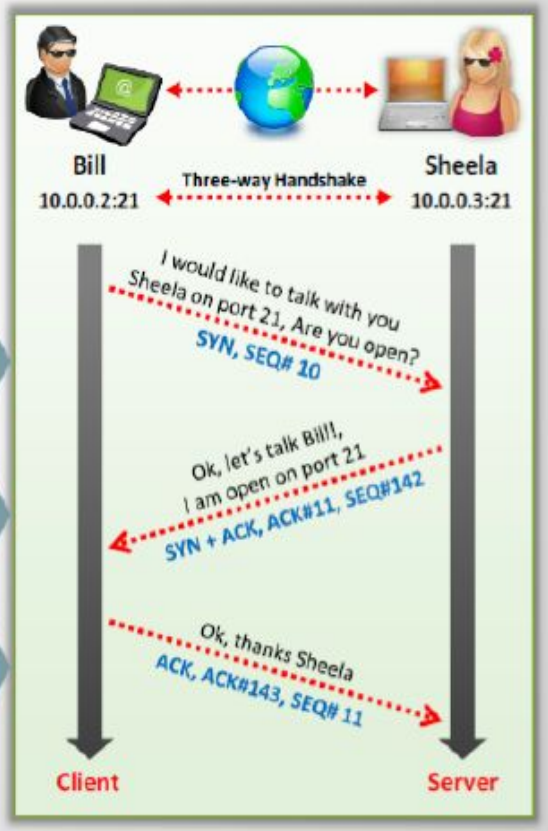
Three-way Handshake Process

1. The Computer A (10.0.0.2) initiates a connection to the server (10.0.0.3) via a packet with only the SYN flag set
2. The server replies with a packet with both the SYN and the ACK flag set
3. For the final step, the client responds back to the server with a single ACK packet
4. If these three steps are completed without complication, then a TCP connection is established between the client and the server

Step 1

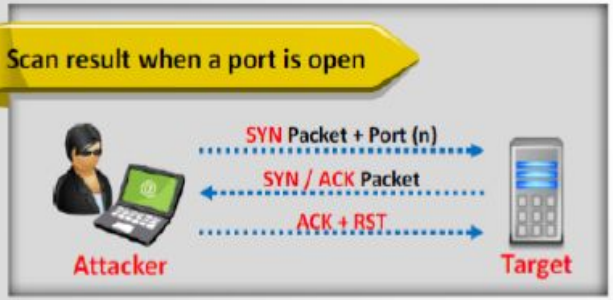
Step 2

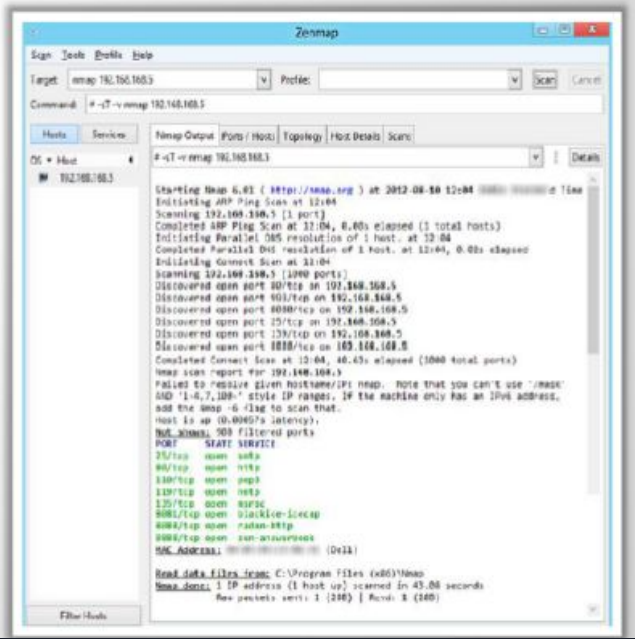
Step 3



Full Open Scan

- TCP Connect scan detects when a port is open by completing the three-way handshake
- TCP Connect scan establishes a full connection and tears it down by sending a RST packet



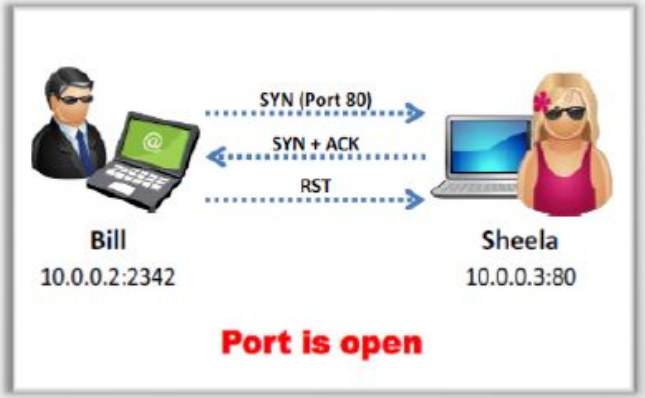


Stealth Scan/Half Open Scan

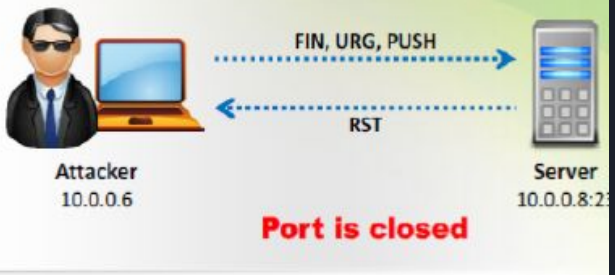
Attackers use stealth scanning techniques to **bypass firewall rules**, **logging mechanism**, and hide themselves as usual network traffic

Stealth Scan Process

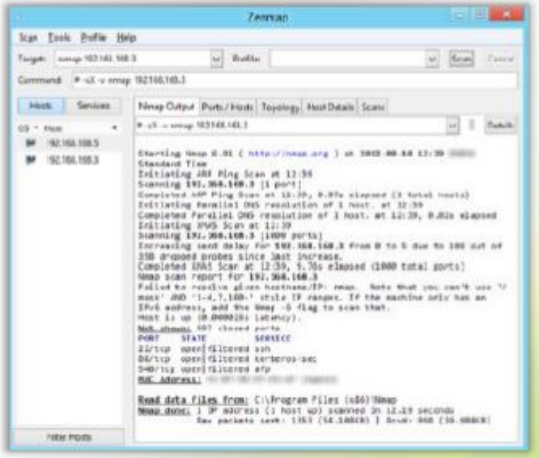
1. The client sends a single SYN packet to the server on the appropriate port
2. If the port is open then the server responds with a SYN/ACK packet
3. If the server responds with an RST packet, then the remote port is in the "closed" state
4. The client sends the RST packet to close the initiation before a connection can ever be established



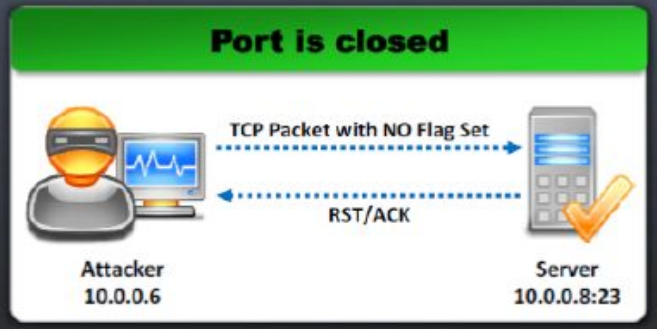
XMAS Scan



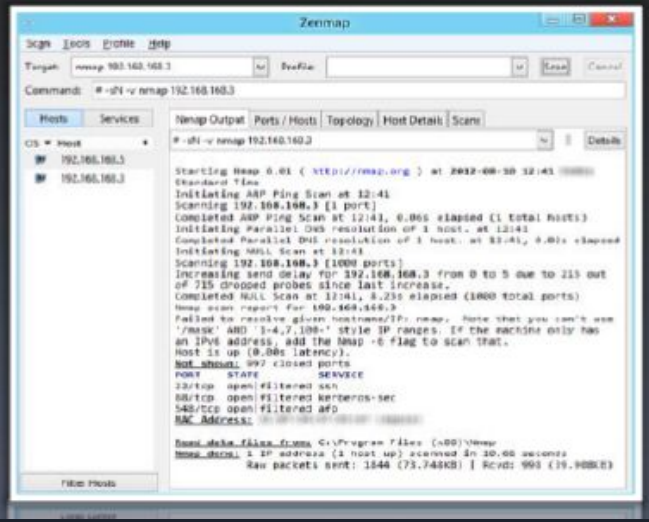
- In Xmas scan, attackers send a TCP frame to a remote device with URG, ACK, RST, SYN, PSH, and FIN flags set
- FIN scan only with OS TCP/IP developed according to RFC 793
- It will not work against any current version of Microsoft Windows



Null Scan



- In NULL scan, attackers send a TCP frame to a remote host with **NO Flags**
- NULL scan only works if OS' TCP/IP implementation is developed according to **RFC 793**
- It will not work against any current version of **Microsoft Windows**



UDP(User Datagram Protocol) Scan

UDP Port Open

- There is no three-way TCP handshake for UDP scan
- The system does not respond with a message when the port is open

UDP Port Closed

- If a UDP packet is sent to closed port, the system responds with ICMP port unreachable message
- Spywares, Trojan horses, and other malicious applications use UDP ports

TCP Scan	Flags	Host Response	Result
Full scan	SYN (and ACK)	SYN & ACK	Host is alive
SYN (Half open) scan	SYN	SYN&ACK	Host is alive
XMAS scan	FIN,URG, PSH	RST	Port is closed
ACK scan	ACK	No response or RST	Port is filtered or port is not filtered
SYN/FIN (Fragmented) scan	SYN, FIN	No response or RST	Port is filtered or port is not filtered
Inverse TCP Flag scan	FIN, URG, PSH (or NULL)	No response or RST/ACK	Port is open or port is not open

CYBER SECURITY

MODULE - 4

Gaining and Maintaining Access

Module Duration : 2 hours

Foot printing

Scanning

Enumeration

System Hacking

Cracking Password

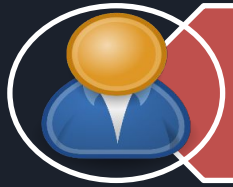
Escalating privilege

Executing application

Hiding Files

Covering tracks

Gaining Access



In this phase attacker gains access of the operating system or an application

Attacker gains access OS level or application level or network level

privilege escalation to obtain complete control of the system.

Example : password cracking ,buffer over flow, DOS and session hijacking etc…

Maintaining Access

- In this phase the attacker tries to retain his or her ownership of the system

- Attacker prevents the system from being owned by other attacker by securing their exclusive access with Backdoors, Rootkits or Trojans

- Attacker can upload, download or manipulate data, applications and configurations on the owned system

- Attacker uses the compromised system to launch further attacks.

Clearing Tracks

This are the activity's carried out by an attacker to hide malicious acts

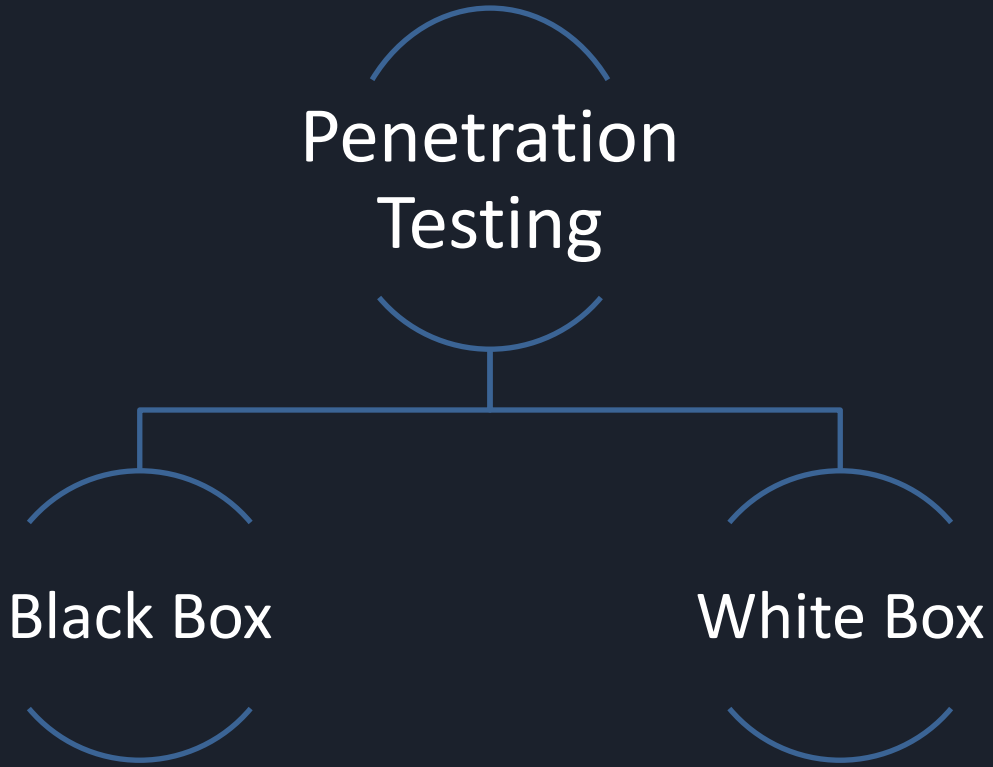
Continuing access to the victims system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution

The attacker overwrites the server, system , and application logs to avoid suspicion

Hacking Stage	Goal	Technique
Gaining Access	To collect enough information to gain access	Password Eavesdropping
Escalation Privileges	To create a privileged user account	Password cracking known exploits
Executing Applications	To create and maintain backdoor access	Trojans
Hiding files	To hide malicious activities	Rootkits
Covering tracks	To hide the presence of compromise	Clearing logs

Penetration Testing

- Penetration testing is a method of evaluating security levels of a particular system or network.
- This helps you determine the flaws related to hardware and software.
- The early identification helps protect the network.
- If the vulnerabilities aren't identified early, then they become an easy source for the attacker for the intrusion.


Penetration Testing
Black Box
White Box

Enumeration

- Enumeration is defined as the process of extracting user names, machine names, network resources, shares, and services from a system
- Attacker use system information to identify system attack point and perform different attack to gain unauthorized access to information system resources.
- Enumeration techniques conducted in an Internet Environment.

Information Enumerated

- Users and Groups
- Networks and shared paths
- Hostnames
- Route Tables
- Service Settings
- SNMP port scanning and DNS Details

Significance of enumeration:

Enumeration is often considered as a critical phase in Penetration testing as the outcome of enumeration can be used directly for exploiting the system.

Types of Enumeration

- NetBIOS Enumeration
- SNMP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration

Enumeration Tools

In windows Operating System, the use of many tool is done to enumerate NetBIOS names with commands like:

- Net accounts
- Net config server
- Net config workstation
- Net view

Tools Used:

- DUMPSEC
- NBTSTAT
- SUPER SCAN

Enumeration Tools

Tools Used for SNMP:

- SNMPUtil
- OpUtils
- Solar Winds IP
- SNMP Scanner

NTP Enumeration Tools:

- Ntptrace

SMTP Enumeration Tools:

- NetScan Tools

DNS Enumeration Tools:

- Nslookup Tools

CYBER SECURITY

MODULE - 9

Vulnerability Mitigation & Report Writing

Module Duration : 1 hour

Key Terminologies

- Threat: Potential for a specific vulnerability be exercised either intentionally or accidentally.
- Vulnerability: A flaw or weakness in system security procedures, design, implementation, architecture or internal controls that may result in a security breach or a violation or risk
- Risk: Combination of threats and vulnerabilities resulting in exposure of CIA
- Control: measures taken to prevent, detect, minimize, or eliminate risk to protect the C, I and A of information – Types: People; Process & Technology
- Ethical Hacking: a trusted attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker with an objective of identifying vulnerabilities/ weaknesses that can be exploited by various threats resulting in information security risks

Vulnerability Assessment

- Can be done both internally and externally
- Part of Ethical Hacking or PT based on mutually agreed terms or stand-alone
- Vulnerabilities are not exploited
- Attacks like DOS and Buffer Overflow attacks are not used
- Automated VA tools like Nessus, Retina or ISS are used

Penetration Testing

- Can be done both internally (curiosity, bad intent) and externally (black, white, grey)
- Is provided as a service to organization envisioning to improve their security posture
- Dangerous attacks like DOS and Buffer Overflow attacks can be done if asked to do so
- Automated VA tools are run and exploits are used
- Black box – No previous knowledge of network; company name is provided; simulation of real-life hacking attempt
- White Box – knowledge of remote network is provided including user credentials

External Penetration Testing

- Inventory the company’s external infrastructure
- Create topological map of the network and Identify the IP address of the target machine
- Locate the traffic route that goes to the web servers. Locate TCP and UDP path to the Destination
- Identify the physical location of the target servers
- Examine the use of IPV6 at the remote location
- Lookup domain registry for the IP information
- Find IP block information about the target and locate the ISP servicing the client

Internal Penetration Testing

- Map the internal network; Scan the network for live host; Port scans individual machines
- Try to gain access using known vulnerabilities; Attempt to establish null sessions
- Enumerate users/identify domains on the network
- Sniff the network using Wireshark; Sniff POP3/FTP/Telnet passwords; Sniff email messages
- Attempt replay attacks; Attempt ARP poisoning; Attempt MAC flooding
- Conduct a man-in-middle attack; Attempt DNS poisoning
- Try a login to a console machine
- Attempt session hijacking on Telnet, Http, and FTP traffic
- Attempt to plant software keylogger to steal passwords
- Plant spyware on target machine; Plant Trojan on target machine
- Attempt to bypass antivirus software installed on target machine
- Escalate user privileges

Vulnerability Management

- Vulnerability Management comprises identification of vulnerabilities (Vulnerability Assessment – VA) and measures taken to mitigate/ remediate them – VM = VA + Remediation
- Proactive or reactive or ongoing using manual and/ or automated methods
- Examples of Vulnerabilities (CVE, CWE & OWASP)
    - Flaws in software; Faulty configuration
    - Inaccurate patching; Inadequate hardening
    - Weak passwords
    - Human error
    - Inappropriately assigned permission levels
    - System inappropriately placed in infrastructure/environment

VM - Assessment Phase

- Categories of Vulnerabilities
    - People – human errors, weak passwords
    - Process – inappropriate policy, incorrect design
    - Technology – N/W, OS, Apln (memory, input validation errors, privilege, harm codes)
- Harmful software codes such as Attack code, parasitic code, back-doors, trojans, self-propagating, spyware, logic/ time triggered code, root kit, distributed code
- How to identify Vulnerabilities?
    - People – Risk Assessment & Auditing
    - Process – Risk Assessment & Auditing
    - Technology – Ethical Hacking, Penetration Testing and Code Scanning using tools

VM - Remediation Phase

- How to remediate Vulnerabilities?
  - People – Awareness & Training
  - Process – Policies, Procedures, Standards and Guidelines
  - Technology – Patching, Configuration, Secure Dev, Security Alerts
- Goals of Vulnerability Remediation – SMART
  - Specific; Measurable; Attainable; Relevant; Time-bound
- Common challenges in Vulnerability Remediation
  - Unusual report size produced by automated scanners
  - False positives and false negatives
  - Exploitability trap
  - Response time in identifying a vulnerability, patch identification & deployment, emergency configuration or system changes

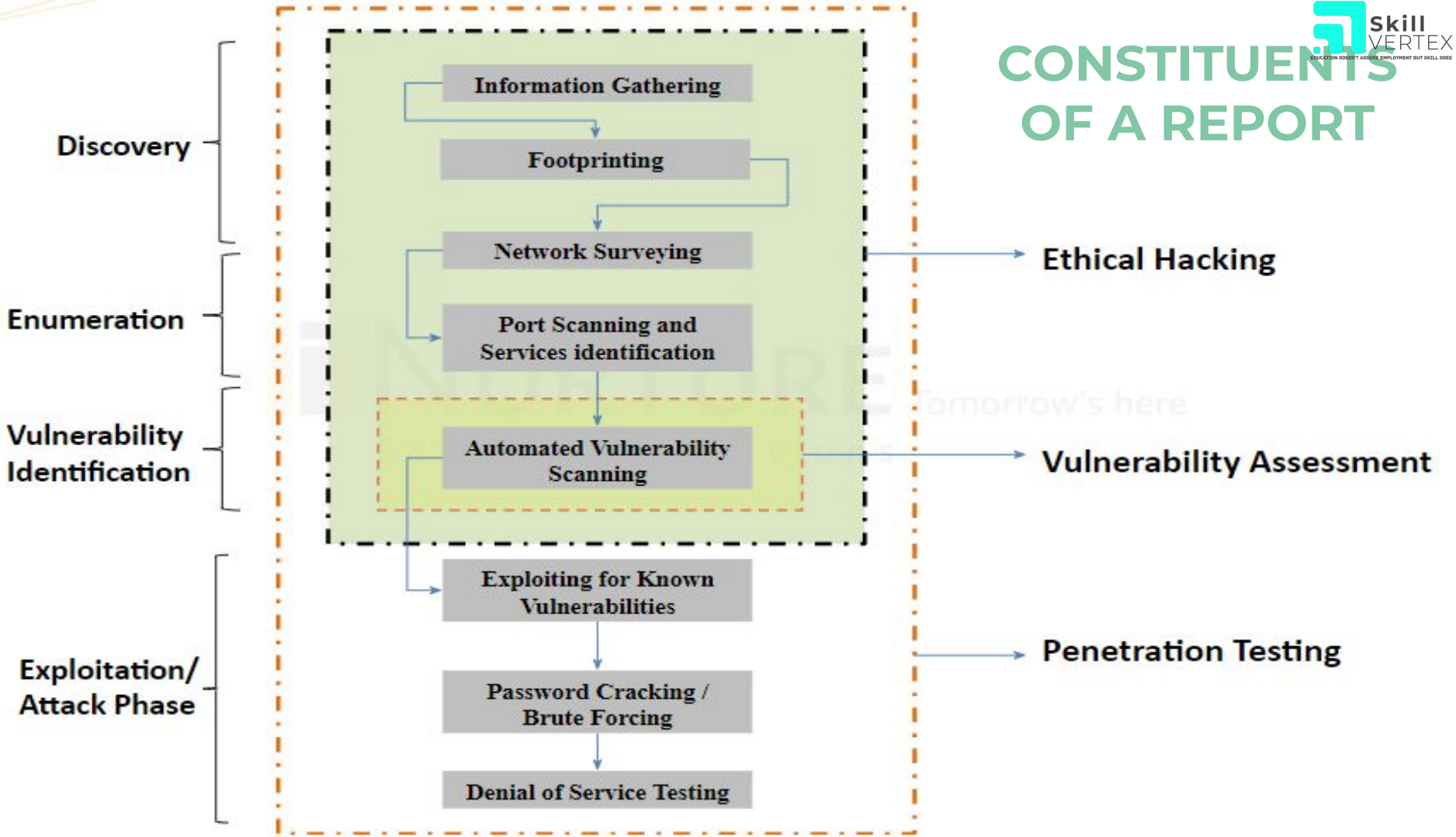
VM - Remediation Phase

- Remediation Techniques
    - Security Alerts ; Secure Software Standards – Application Remediation
    - OWASP Application Security Verification Standard (ASVS)
    - MS Security Development Lifecycle
    - Apple’s Secure Coding Guide; Android Security; Patching/ hardening
    - Design/architecture changes – anti-malware,IPS,DRM, encryption, etc
    - Configuration changes – reconfiguring network/ authentication

- Vulnerability Management Program

Asset inventory; Continuously monitor Vulnerabilities, Remediation & Threat; check patch levels/ logs; Prioritize remediation; Create organization specific remediation database; test remediation before deploying; educate and train everyone in the chain on vulnerabilities and remediation; explore automated deployment of patches; perform periodic scanning

CONSTITUENTS OF A REPORT



CYBER SECURITY

MODULE - 5

Sniffing and Passwords

Module Duration : 2 hours

System hacking Steps

Cracking Password

Escalating privilege

Executing application

Hiding Files

Covering tracks

Penetration testing

Password complexity

Password containing only alphabets

- Geetha

Password containing Alphabets , number & special character

- Geetha@123

Password that only containAlphabetsand special character

- Geetha@raj

Password with only number

- 8022248366

Password that contains only special character

- &**#$@

Password that contains only number & special character / only alphabets and number

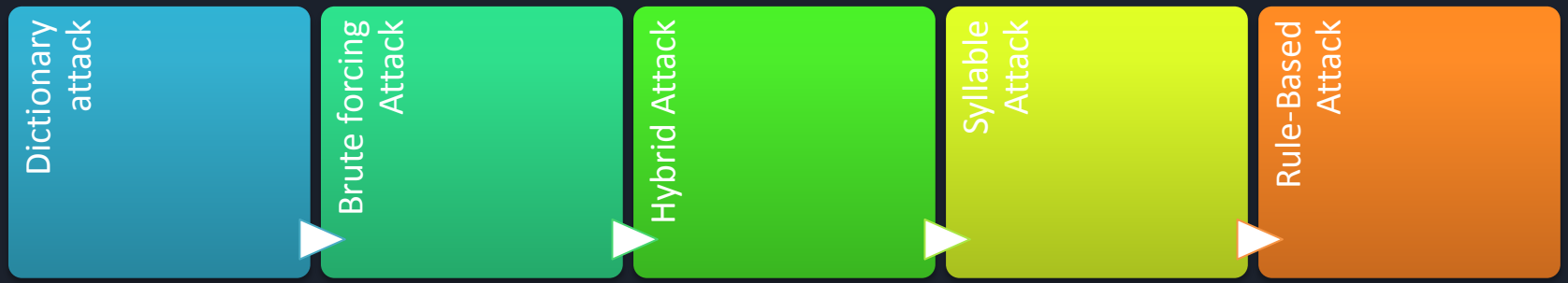
- 123456@123 / 123456geeta

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Password Cracking Techniques



A dictionary file is Loaded into the cracking Application that runs User accounts

The program tries every combination of character until the password is broken.

It is the combination of both brute force attack and the dictionary attack

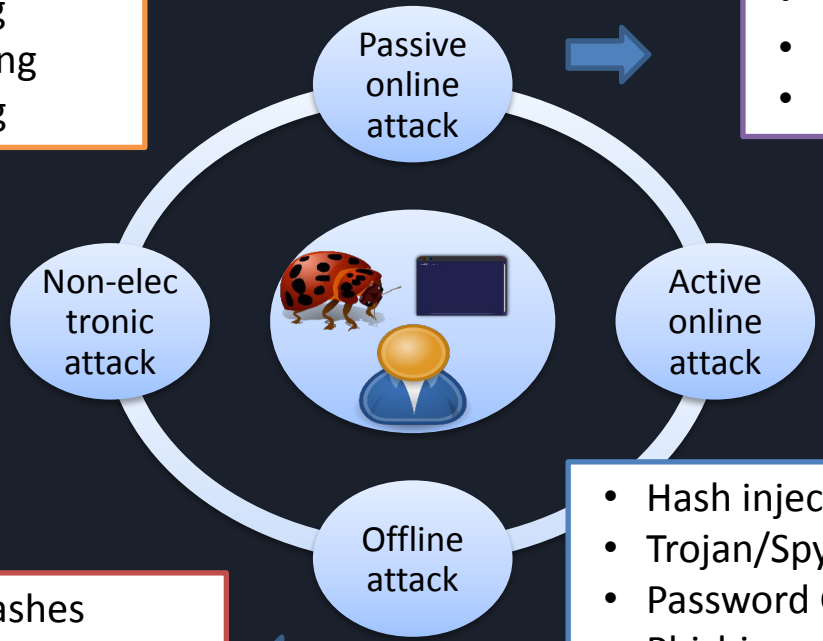
It Works like a hybrid attack, but adds some numbers and symbols to the work from the dictionary and tries to crack the password

This attack is used when the attacker gets some information about the password.

Password cracking methods

- Shoulder surfing
- Social Engineering
- Dumpster diving

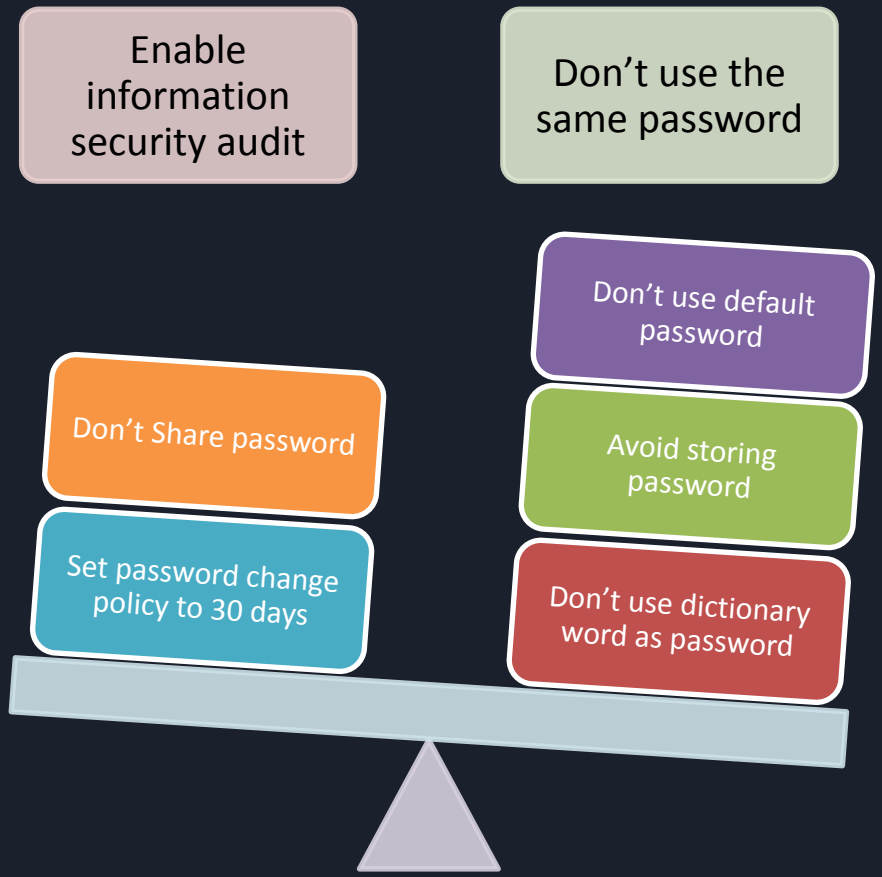
- Wire sniffing
- Man-in-the-middle
- Replay



- Hash injection
- Trojan/Spyware/ key loggers
- Password Guessing
- Phishing

- Pre-computed Hashes
- Rainbow

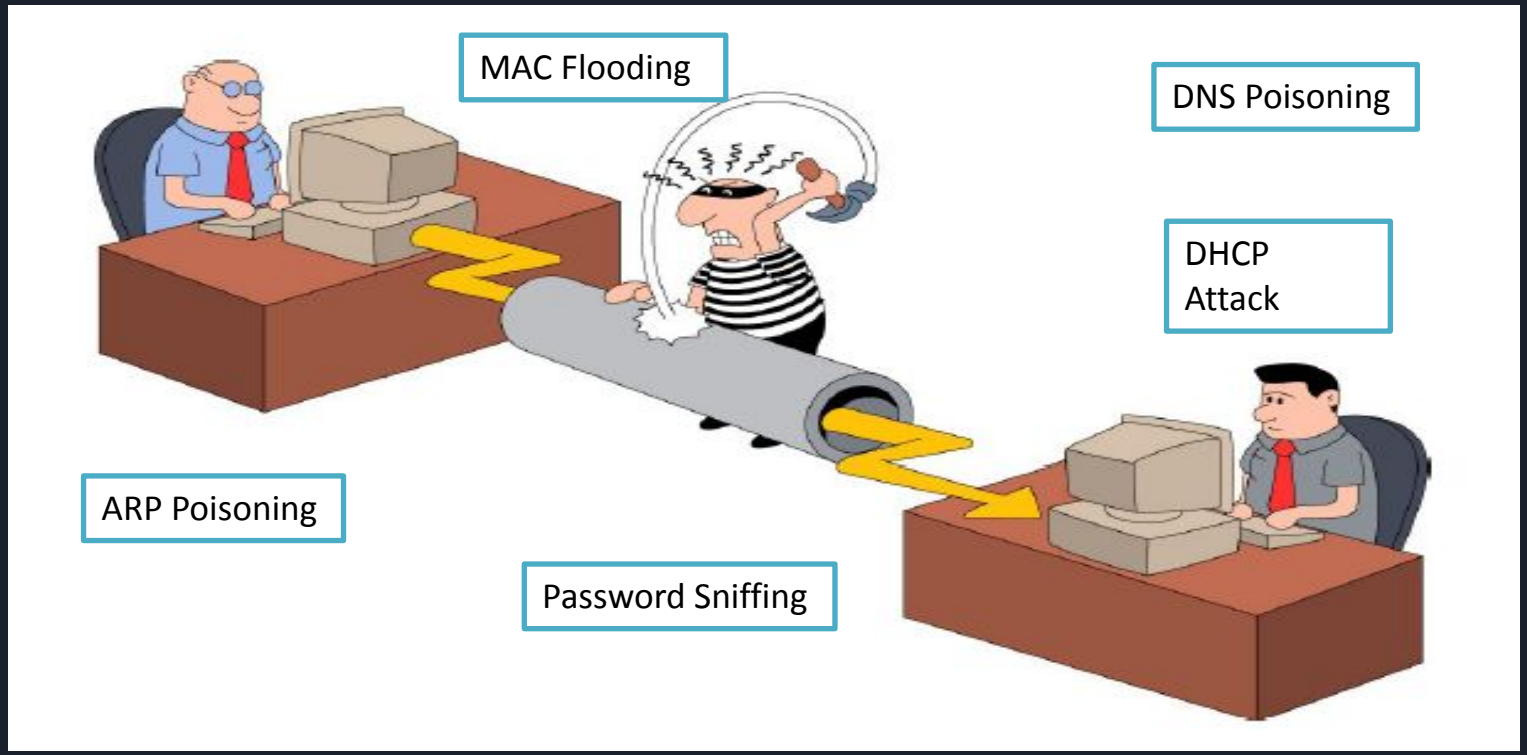
Defending Against Password Attacks



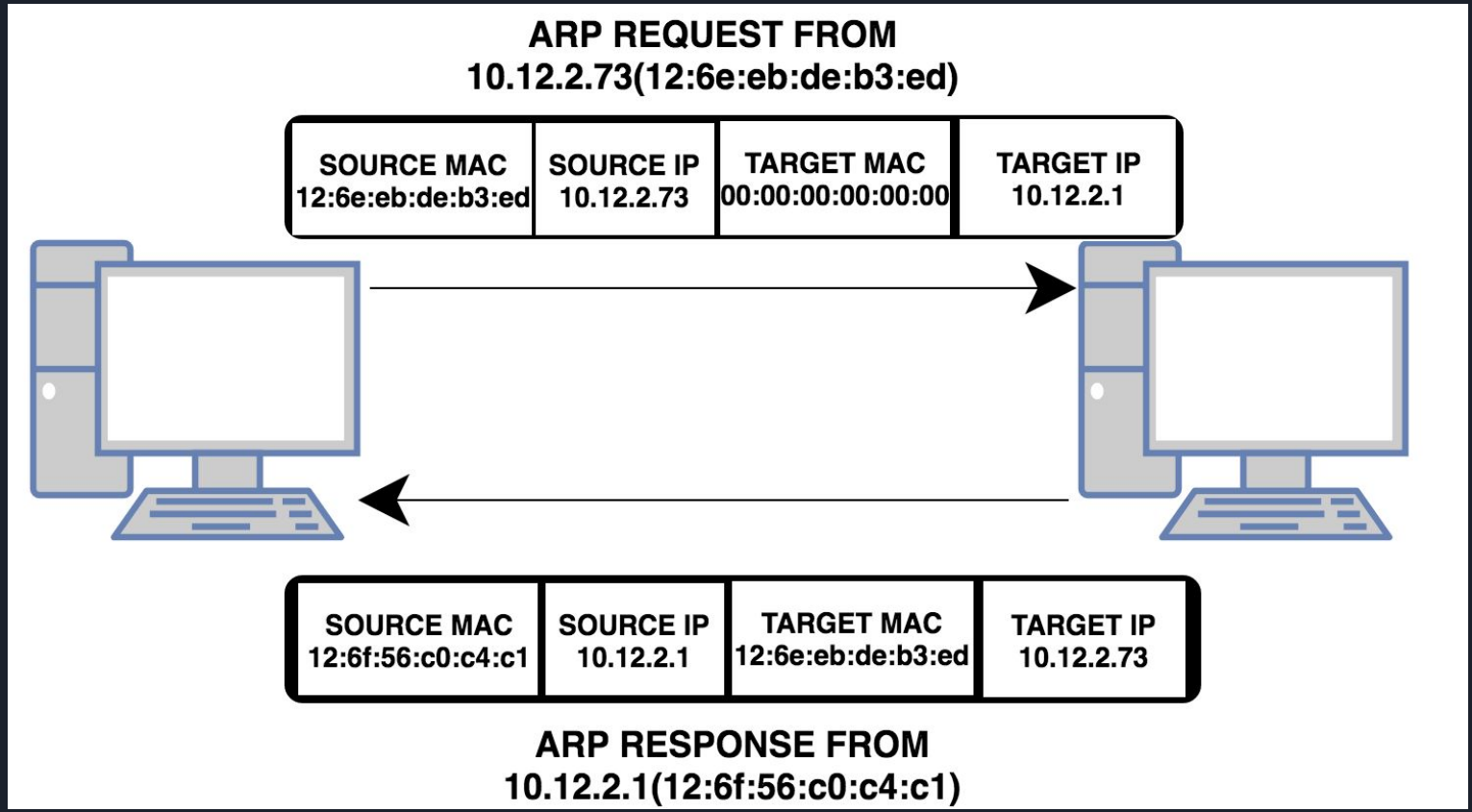
Sniffing

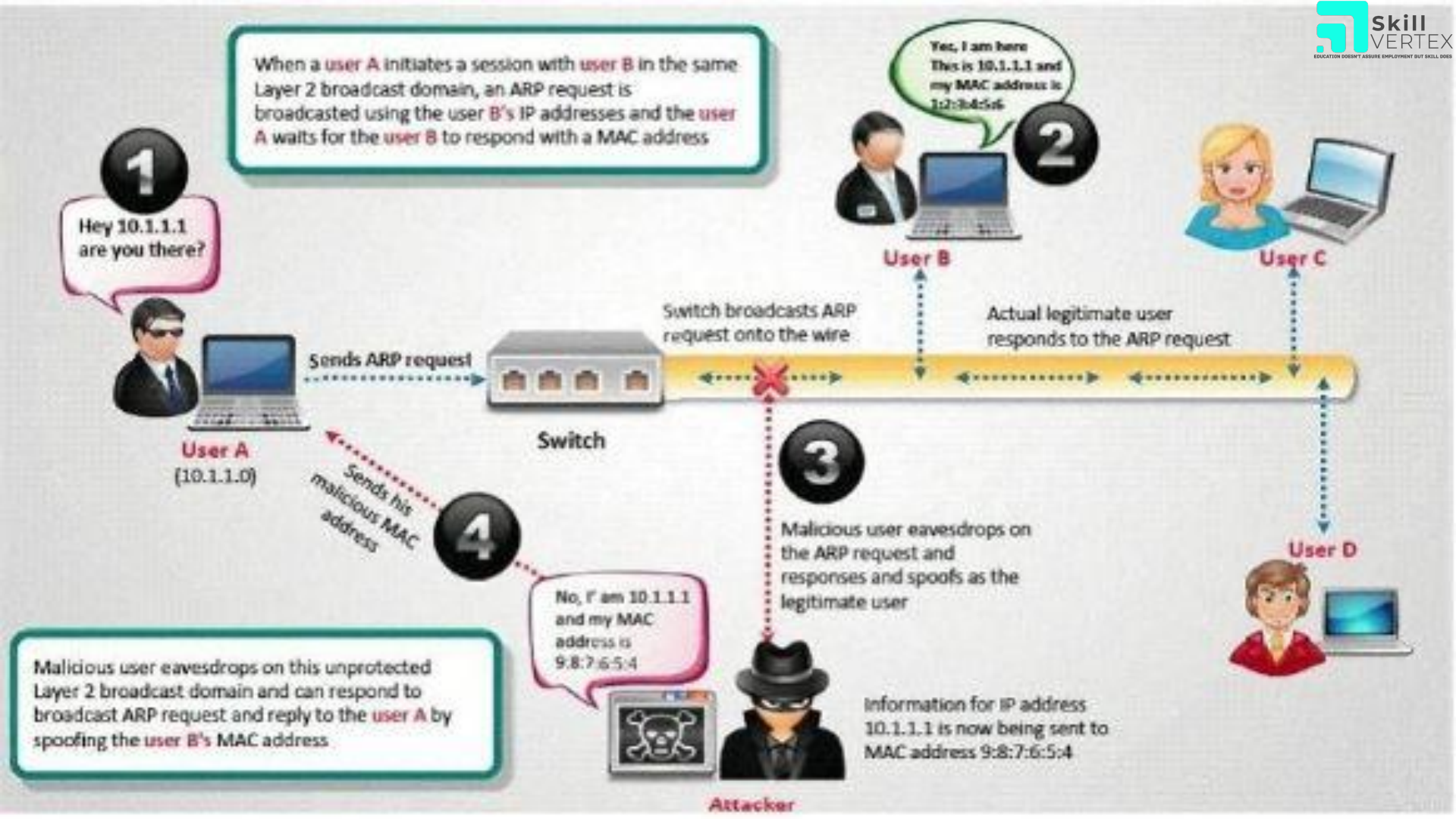
- A packet sniffer is a utility that has been used since the original release of Ethernet.
- Packet sniffing allows individuals to capture data as it is transmitted over a network.
- Packet sniffer programs are used by network professionals to diagnose network issues, and by malicious users to capture unencrypted data, like passwords and usernames.
- If this information is captured in transit, a user can gain access to a system or network.

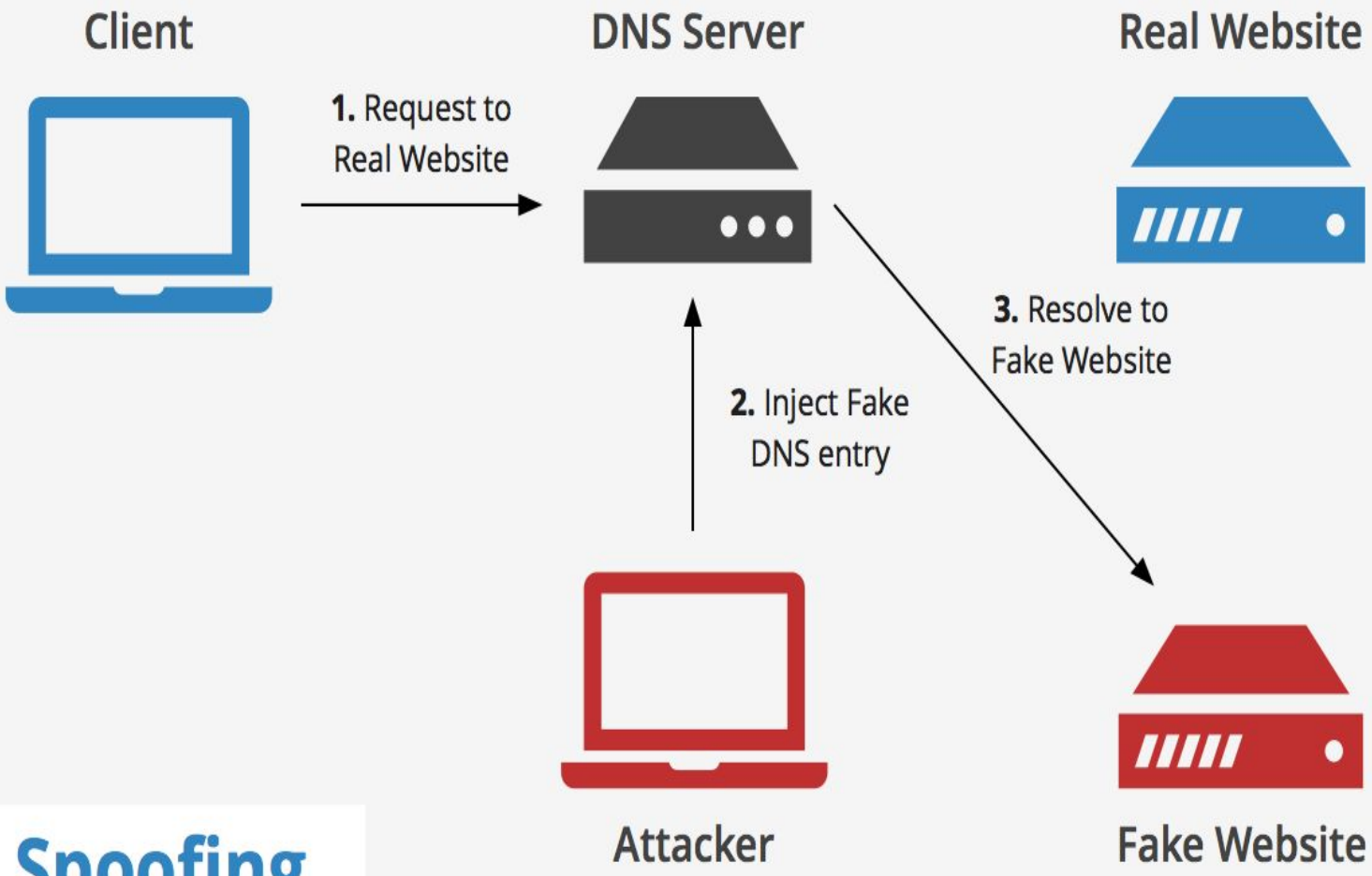
Types of Sniffing Attacks



ARP Spoofing/Poisoning/Sniffing

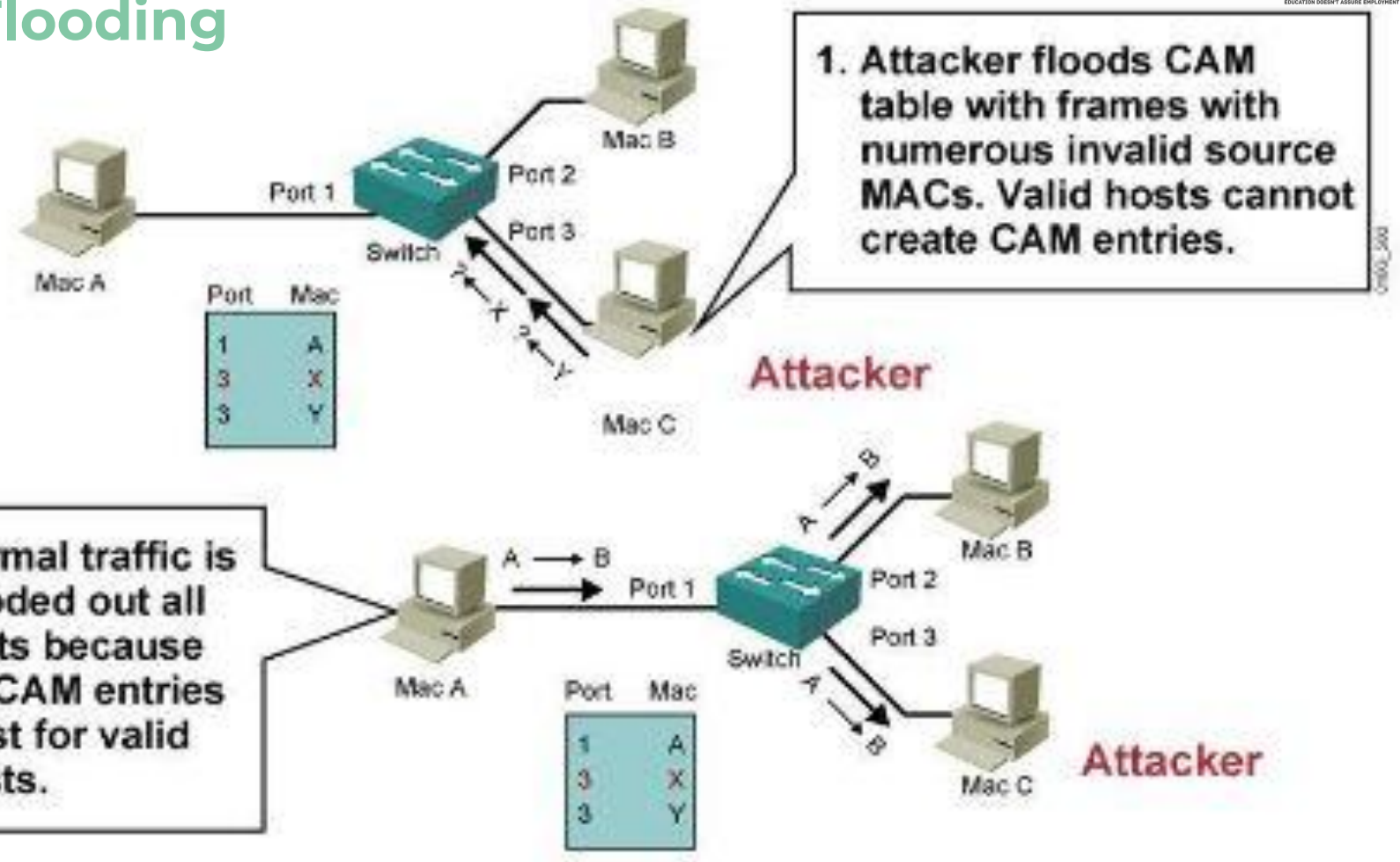



When a user A initiates a session with user B in the same Layer 2 broadcast domain, an ARP request is broadcasted using the user B's IP addresses and the user A waits for the user B to respond with a MAC address
1
Hey 10.1.1.1 are you there?
User A
(10.1.1.0)
Sends ARP request
Switch
Switch broadcasts ARP request onto the wire
2
Yes, I am here This is 10.1.1.1 and my MAC address is 1:2:3:4:5:6
User B
Actual legitimate user responds to the ARP request
User C
3
Malicious user eavesdrops on the ARP request and responses and spoofs as the legitimate user
User D
4
Sends his malicious MAC address
No, I' am 10.1.1.1 and my MAC address is 9:8:7:6:5:4
Attacker
Information for IP address 10.1.1.1 is now being sent to MAC address 9:8:7:6:5:4
Malicious user eavesdrops on this unprotected Layer 2 broadcast domain and can respond to broadcast ARP request and reply to the user A by spoofing the user B's MAC address

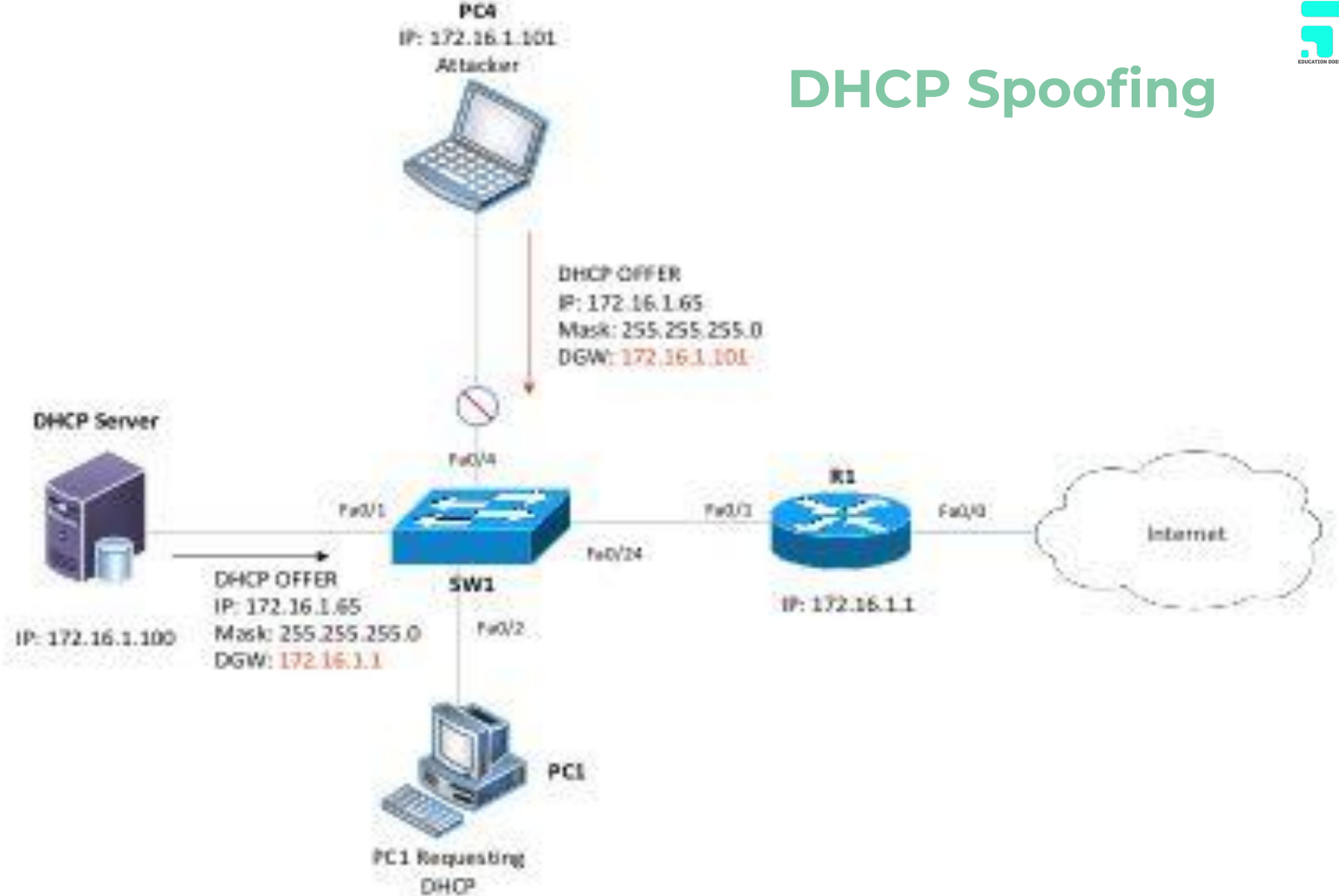


DNS Spoofing

MAC Flooding



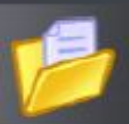
DHCP Spoofing



Sniffing Tools

- Wireshark
- Cascade Pilot
- TCP Dump/Windump
- Capsa Network Analyzer
- JitBit Network Sniffer

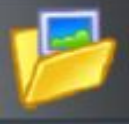
Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed



Use encryption to protect confidential information

Permanently add the MAC address of the gateway to the ARP cache

Use static IP addresses and static ARP tables to prevent attackers from adding the spoofed ARP entries for machines in the network



Turn off network identification broadcasts and if possible restrict the network to authorized users in order to protect network from being discovered with sniffing tools

Use IPv6 instead of IPv4 protocol

Use encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for email connection, etc. to protect wireless network users against sniffing attacks

CYBER SECURITY

MODULE - 6

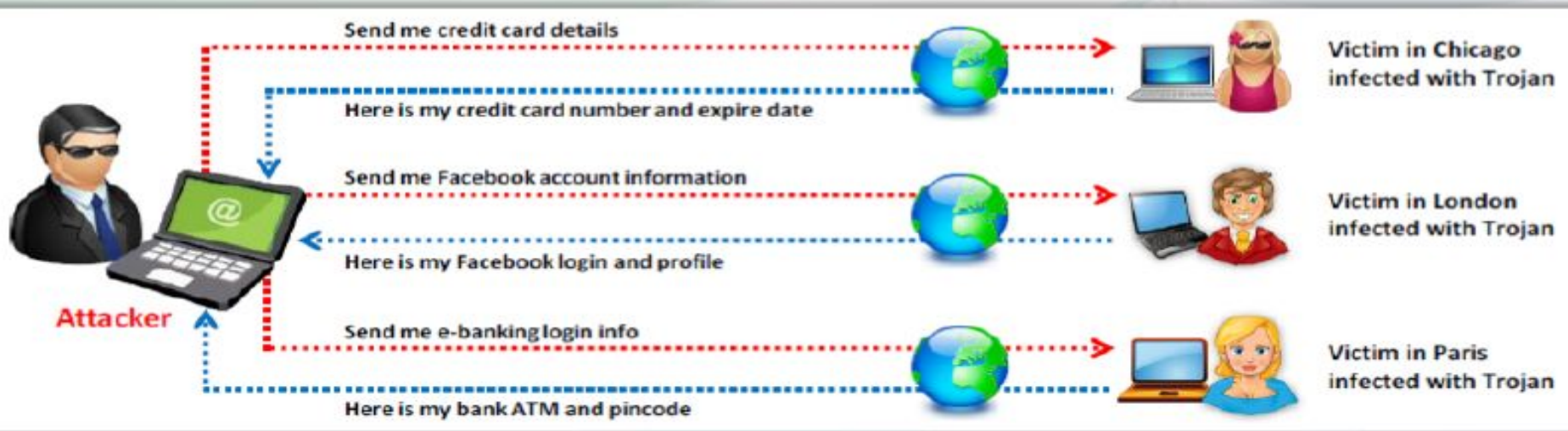
Worms, Viruses and Trojans

Module Duration : 2 hours

What is Trojan?

- It is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk
- Trojans replicate, spread, and get activated upon users' certain predefined actions

- With the help of a Trojan, an attacker gets access to the stored passwords in the Trojaned computer and would be able to read personal documents, delete files and display pictures, and/or show messages on the screen



Communication Channels

Overt Channel

- A legitimate communication path within a computer system, or network, for transfer of data
- Example of overt channel includes games or any legitimate programs

Poker.exe
(Legitimate Application)

Covert Channel

- An unauthorized channel used for transferring sensitive data within a computer system, or network
- The simplest form of covert channel is a Trojan

Trojan.exe
(Keylogger Steals Passwords)

What do hackers look for?

Credit card information

Financial data (bank account numbers, social security numbers, insurance information , etc.)

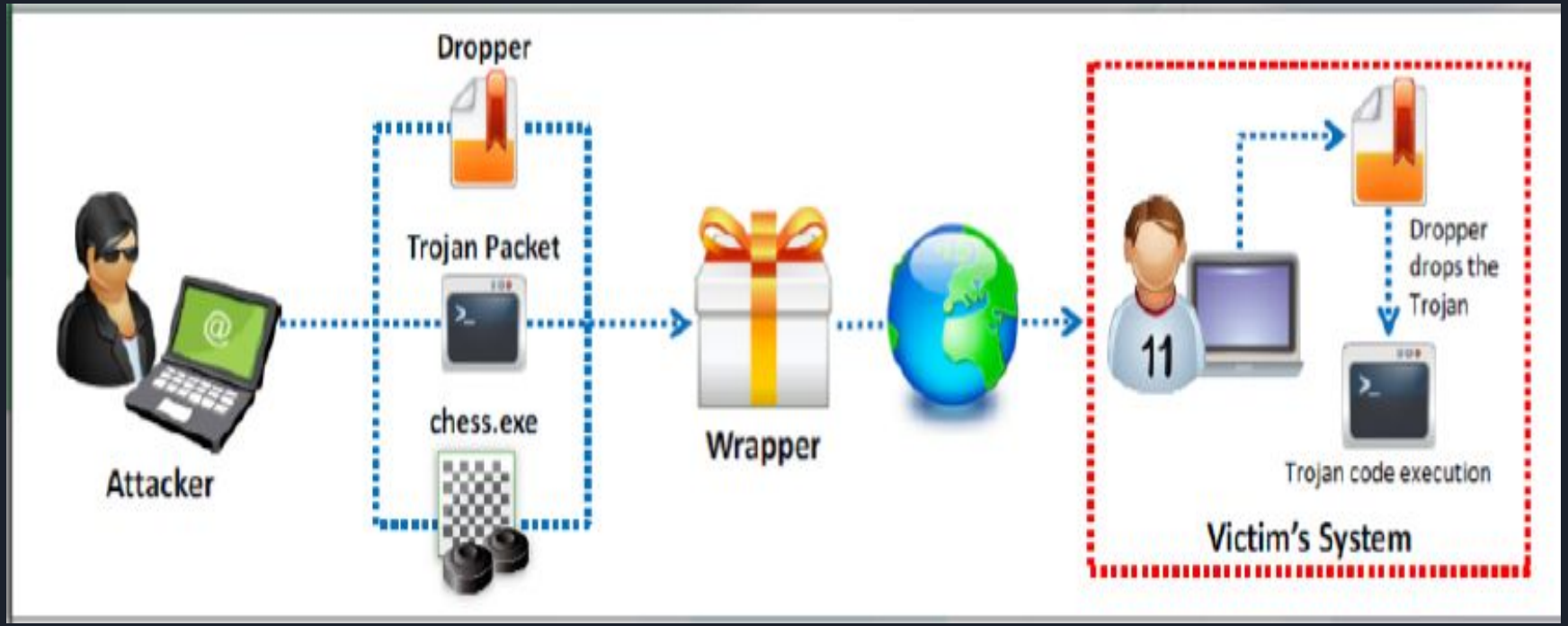
Using the victim's computer for illegal purposes, such as to hack, scan, flood, or infiltrate other machines on the network or Internet

Account data (email addresses, passwords, user names, etc.)

Calendar information concerning the victim's whereabouts

Confidential documents

Trojan Infection Process



Types of Trojans

Goal of Trojan

Delete or replace **operating system's critical files**

Disable **firewalls** and **antivirus**

Generate **fake traffic** to create DOS attacks

Create **backdoors** to gain remote access

Download **spyware**, **adware**, and malicious files

Infect victim's PC as a **proxy server** for relaying attacks

Record **screenshots**, **audio**, and **video** of victim's PC

Use victim's PC as a **botnet** to perform DDoS attacks

Steal information such as **passwords**, **security codes**, credit card information using keyloggers

Use victim's PC for **spamming** and **blasting email messages**

Indications of a Trojan Attack

CD-ROM drawer opens and closes by itself

Abnormal activity by the modem, network adapter, or hard drive

Computer browser is redirected to unknown pages

The account passwords are changed or unauthorized access

Strange chat boxes appear on victim's computer

Strange purchase statements appear in the credit card bills

Documents or messages are printed from the printer themselves

The ISP complains to the victim that his/her computer is IP scanning

Functions of the right and left mouse buttons are reversed

People know too much personal information about a victim

Trojan Creator Tools

- NetCat (Command Shell Trojan)
- MoSucker (GUI Trojan)
- RemoteByMail (Email Trojan)
- HTTP Rat (HTTP Trojan)

Computer Virus

- A virus is a **self-replicating program** that produces its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through **file downloads**, **infected disk/flash drives** and as **email attachments**

Virus Characteristics

Infects Other Program

Transforms Itself

Encrypts Itself

Alters Data

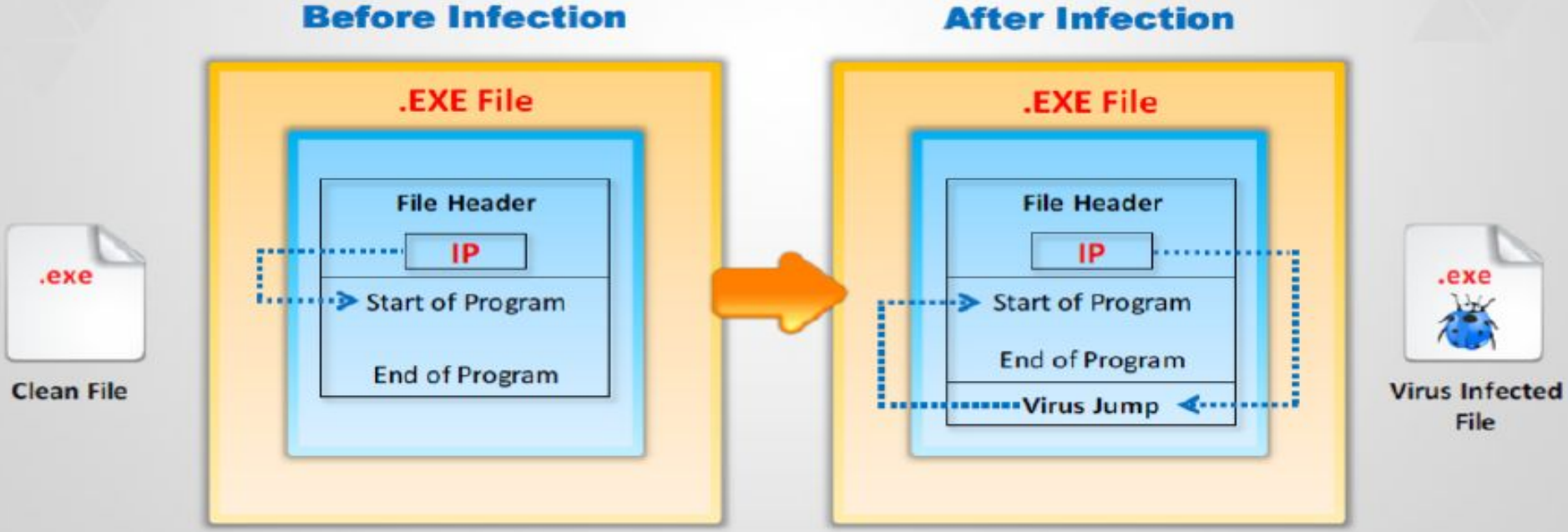
Corrupts Files and Programs

Self Propagates

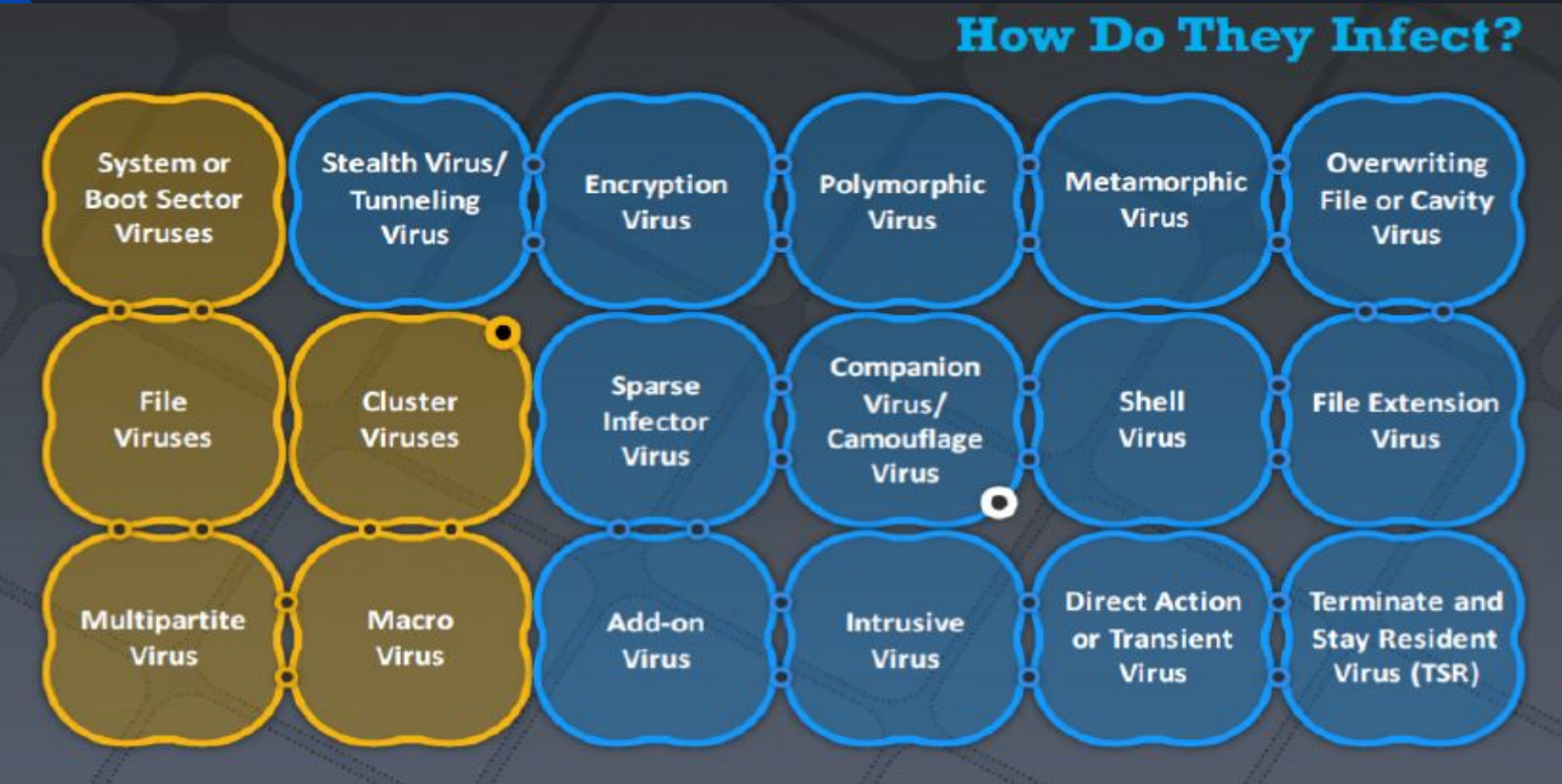
How Viruses Work

Infection Phase

- In the infection phase, the virus **replicates itself** and attaches to an .exe file in the system



Types of Viruses



Computer Worm

1

Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction

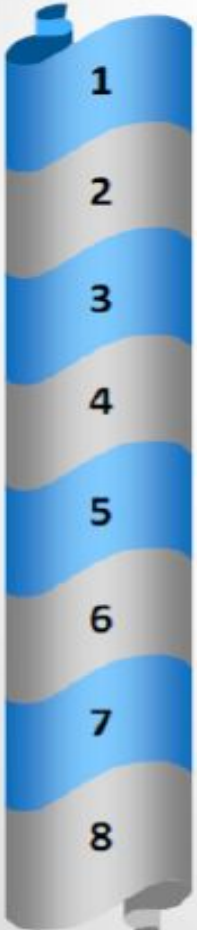
Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system

2

3

Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks

Counter Measures for Viruses and Worms



1. Install anti-virus software that detects and removes infections as they appear ✓
2. Generate an anti-virus policy for safe computing and distribute it to the staff ✓
3. Pay attention to the instructions while downloading files or any programs from the Internet ✓
4. Update the anti-virus software regularly ✓
5. Avoid opening the attachments received from an unknown sender as viruses spread via e-mail attachments ✗
6. Possibility of virus infection may corrupt data, thus regularly maintain data back up ✓
7. Schedule regular scans for all drives after the installation of anti-virus software ✓
8. Do not accept disks or programs without checking them first using a current version of an anti-virus program ✗

CYBER SECURITY

MODULE - 7

System Security

Module Duration : 1 hour

Session Hijacking

Session Hijacking refers to the exploitation of a valid computer session where an attacker takes over a session between two computers

The attacker steals a valid session ID which is used to get into the system and snoop the data

In TCP session hijacking, an attacker takes over a TCP session between two machines

Since most authentication only occurs at the start of a TCP session, this allows the attacker to gain access to a machine

Innocent User

Authentic Request

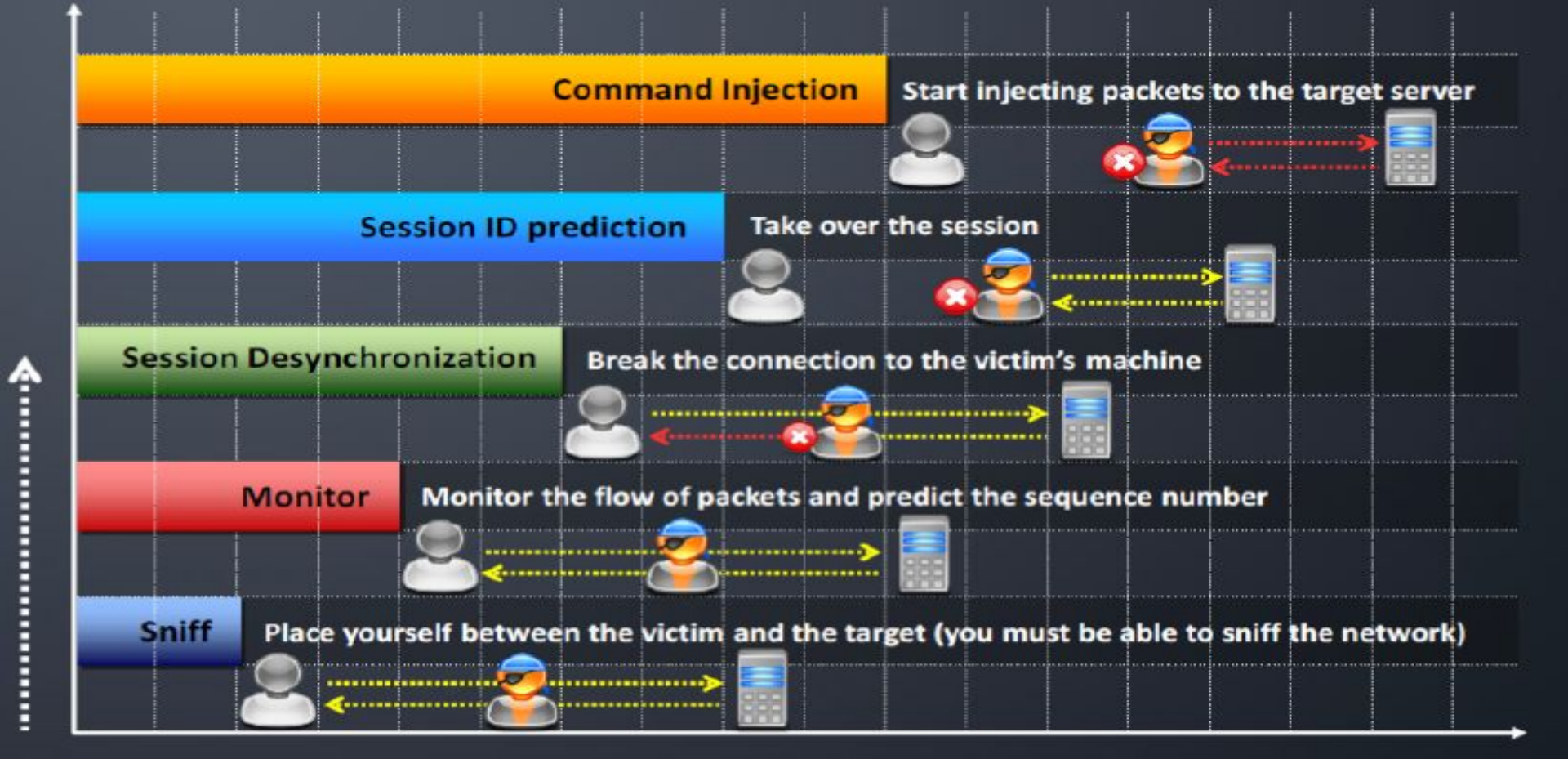
Hijacking Session ID

Website / Server

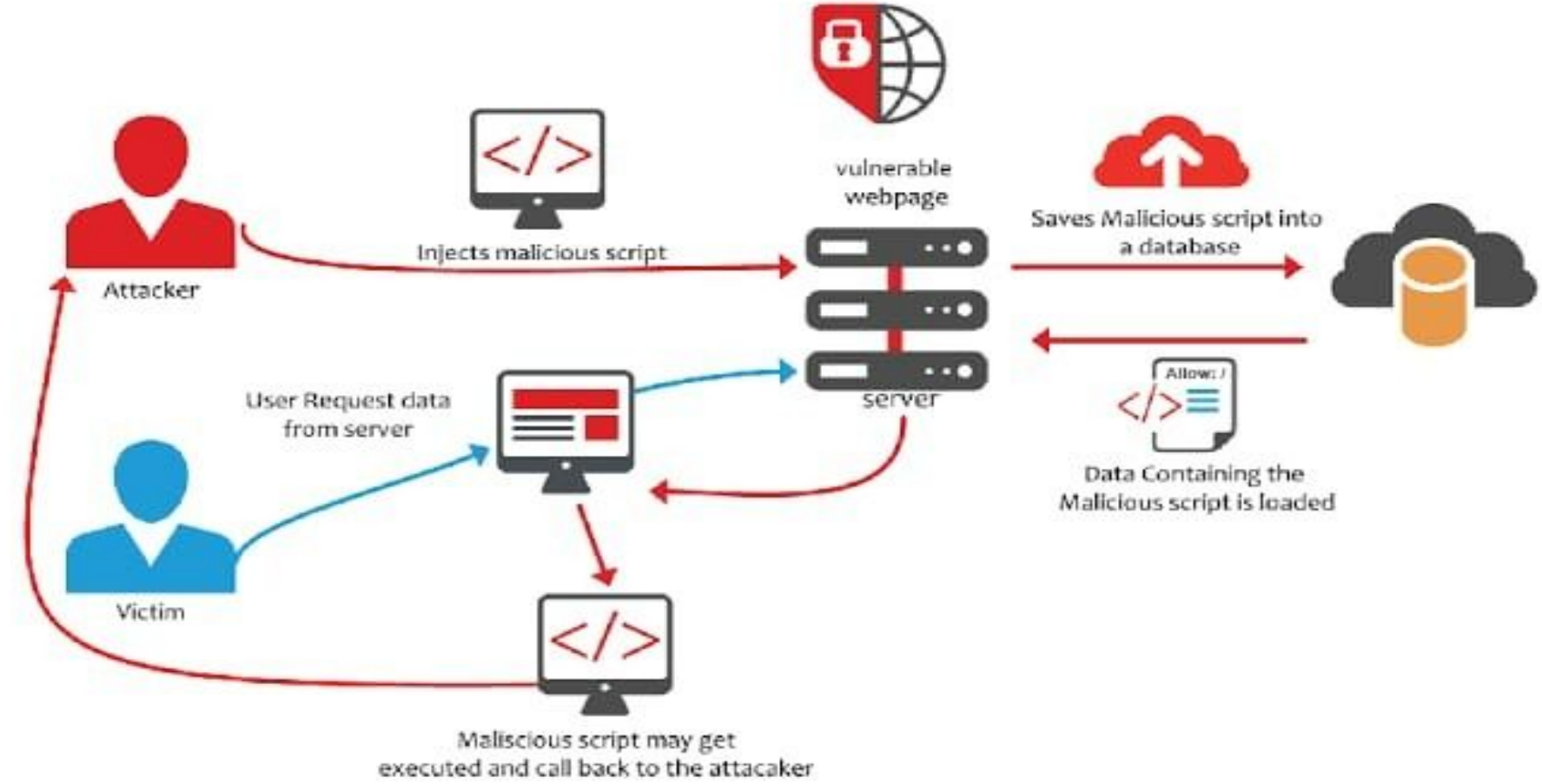
Impersonate Request

Black hat Hacker

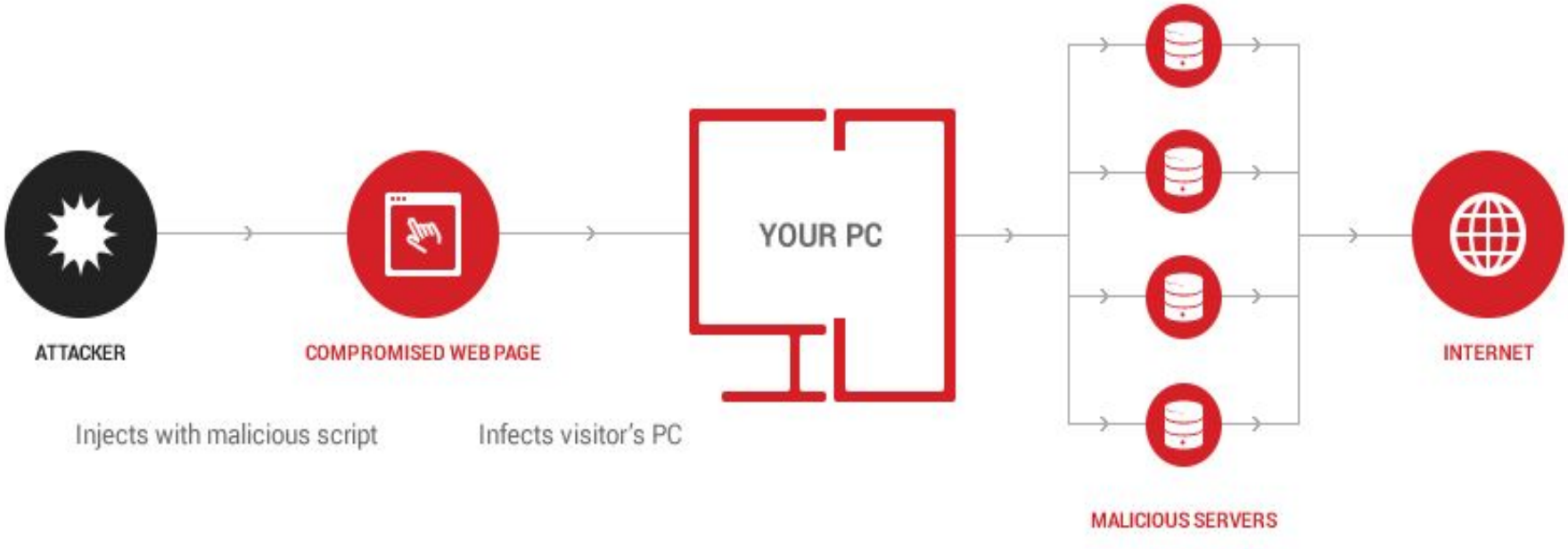
Steps in Session Hijacking



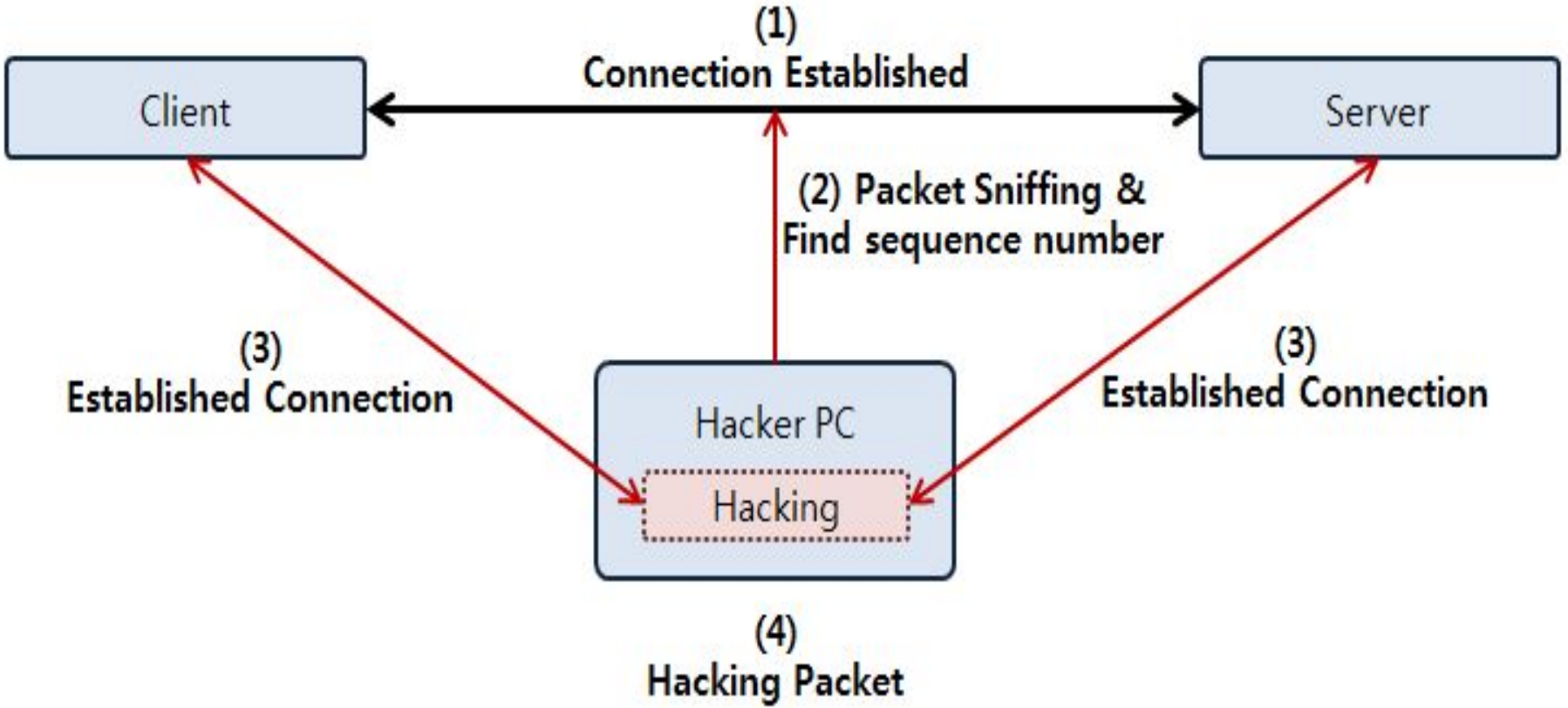
How an XSS Attack works



How an XSS Attack works



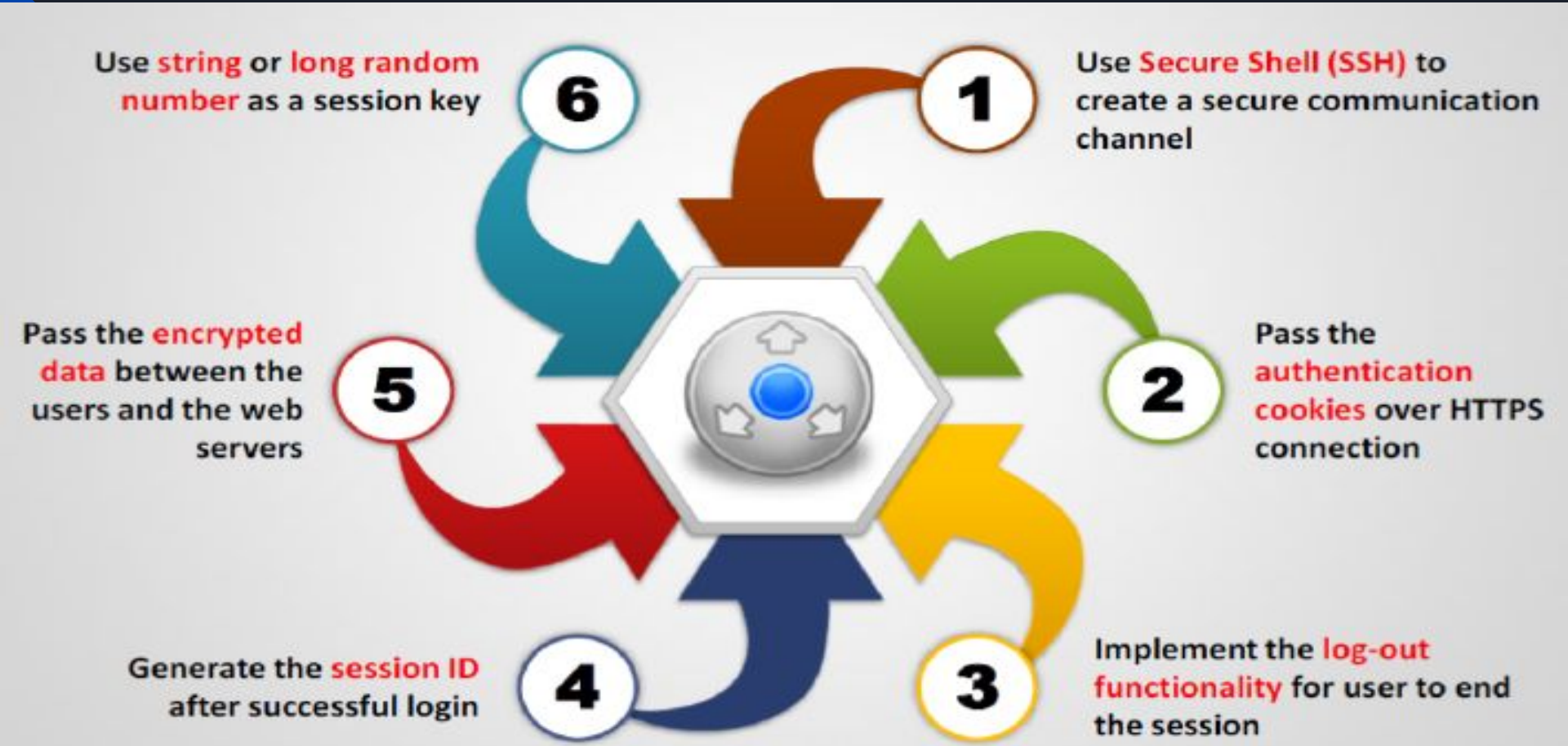
Man-in-the-middle Attack



Session Hijacking Prevention Method

- Create session keys with lengthy strings or random number so that it is difficult for an attacker to guess a valid session key
- Encrypt the data and session key that is transferred between the user and the web servers
- Prevent Eavesdropping within the network
- Regenerate the session id after a successful login to prevent session fixation attack
- Expire the session as soon as the user logs out
- Reduce the life span of a session or a cookie

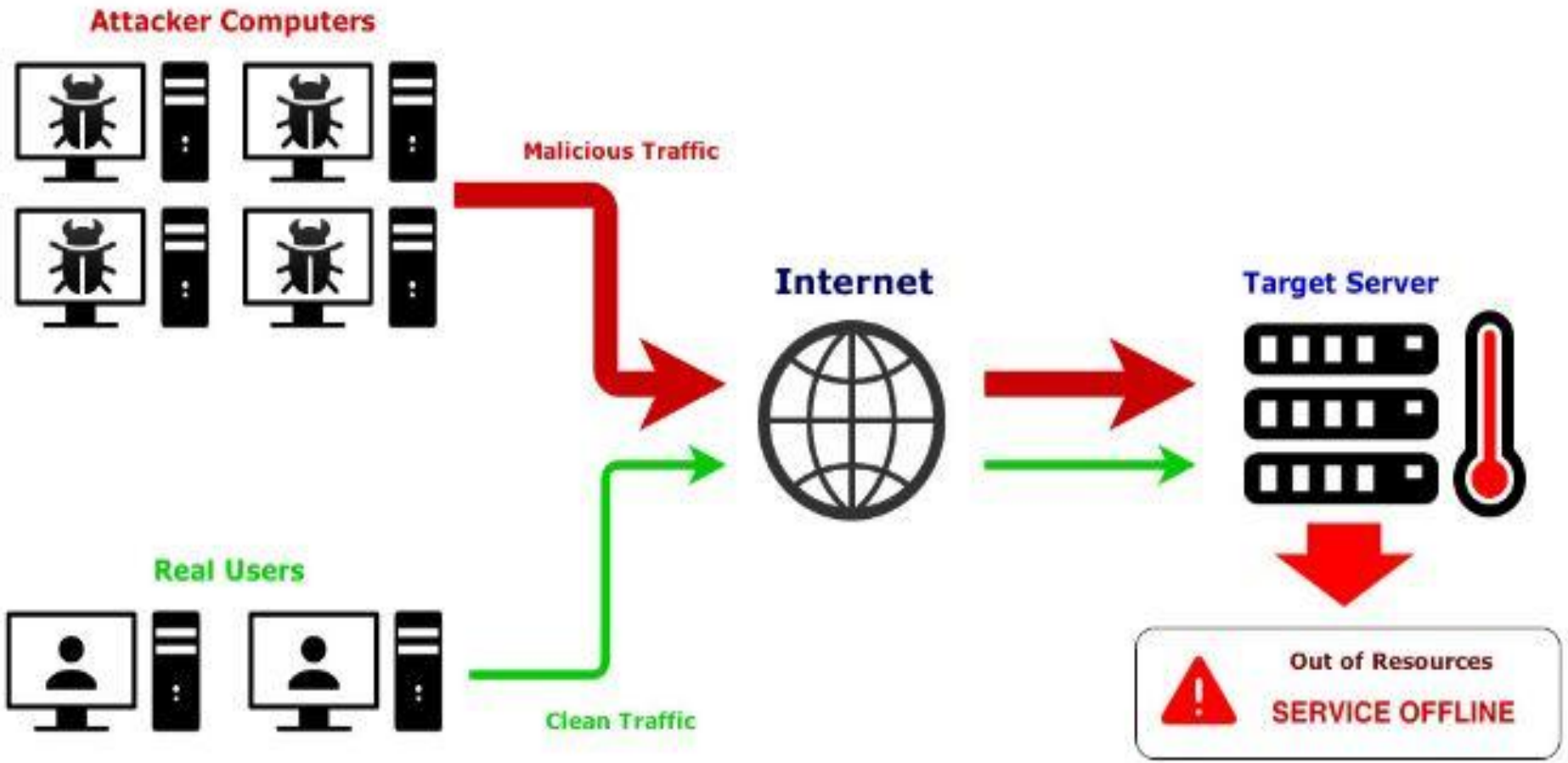
Session Hijacking Prevention Method



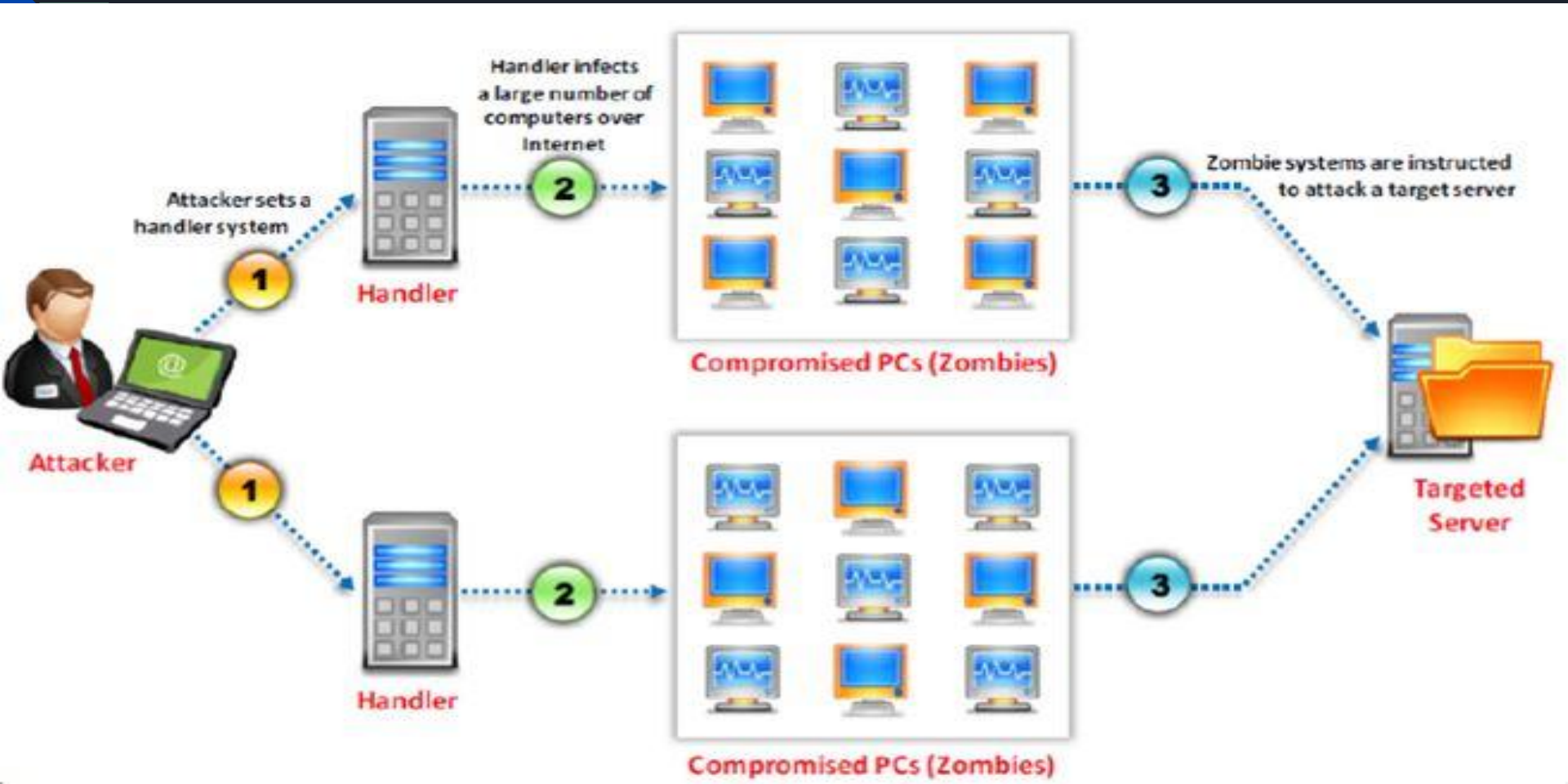
What is DOS attack ?

- Denial-of-service (DoS) Is an attack on a computer or network that reduces or prevents authorized users from accessing a computer or network.
- DoS Attacks target the network bandwidth or connectivity to overload its resources.
- A distributed denial-of-service (DDoS) attack is a large-scale, coordinated attack on the availability of service on a target's system or network resource, launched indirectly through many compromised computers on the internet.

DOS Attack


Attacker Computers
Malicious Traffic
Internet
Target Server
Real Users
Clean Traffic
Out of Resources
SERVICE OFFLINE

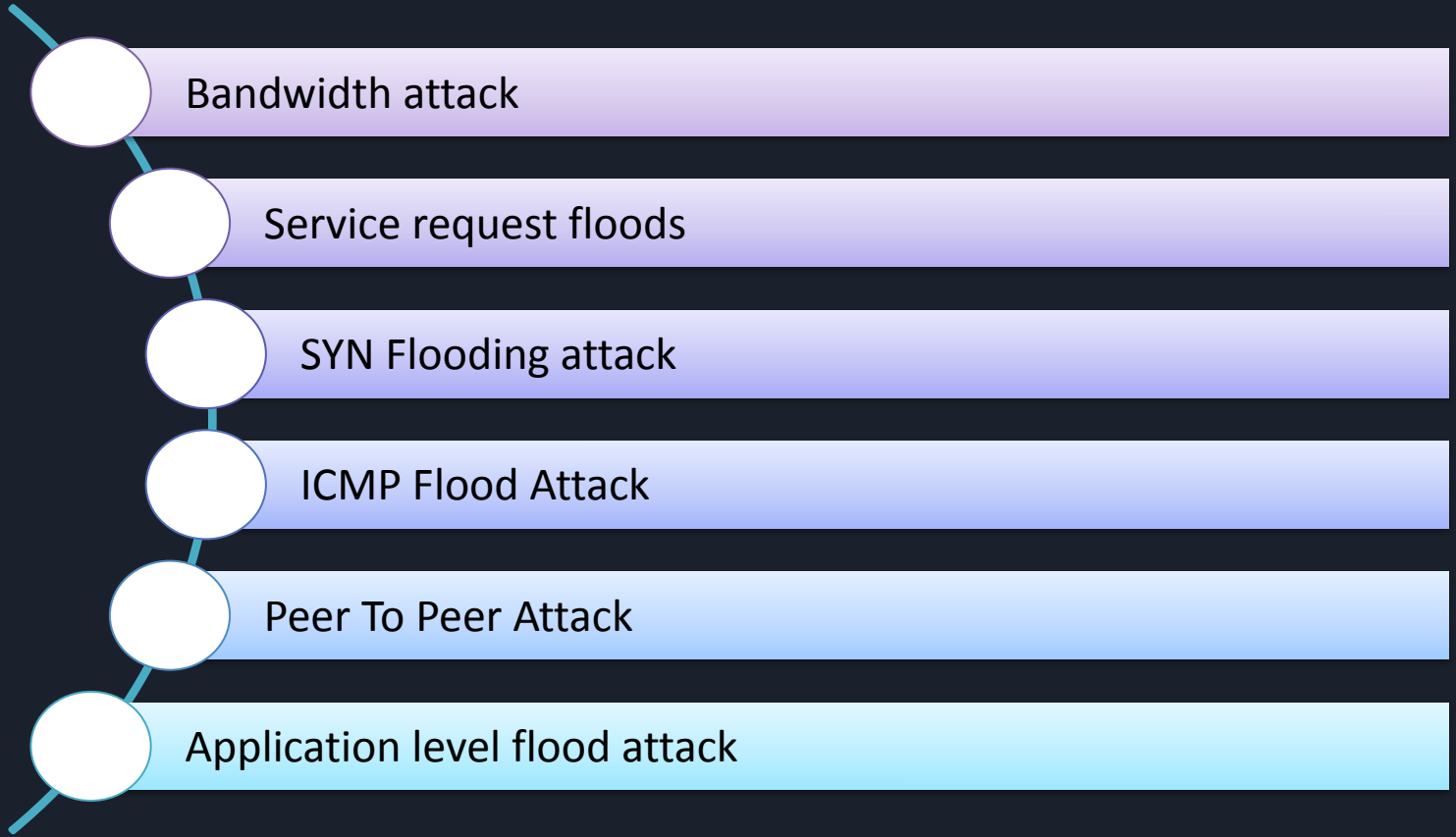
DDOS Attack


Attacker sets a handler system
1
Handler
Handler infects a large number of computers over Internet
2
Compromised PCs (Zombies)
3
Zombie systems are instructed to attack a target server
Attacker
1
Handler
2
Compromised PCs (Zombies)
3
Targeted Server

Symptoms of DOS

- Unusually slow network performance
- Inability to access any website
- Unavailability of a particular website
- Dramatic increase in the amount of spam emails received

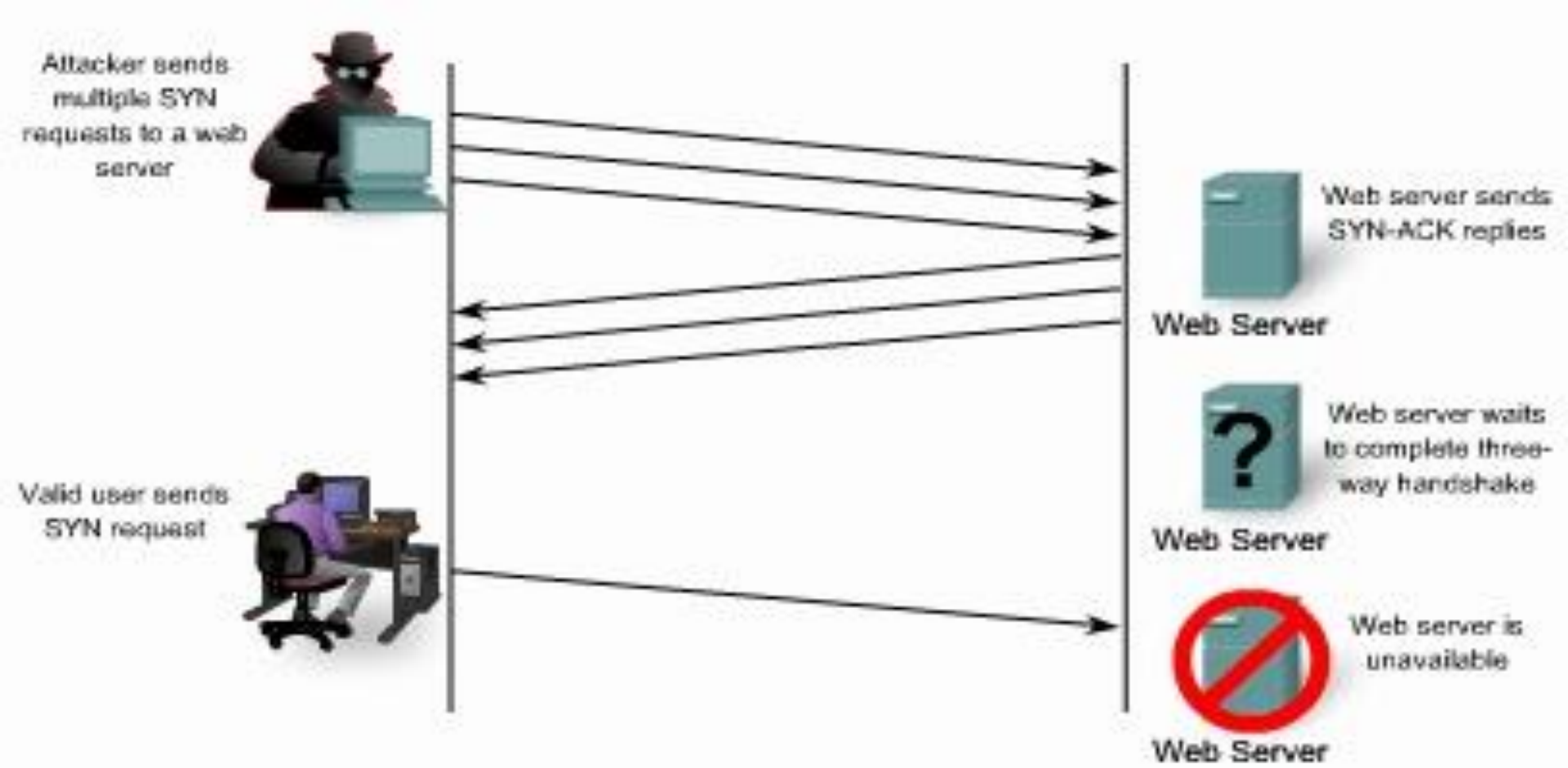
DoS Attack Techniques



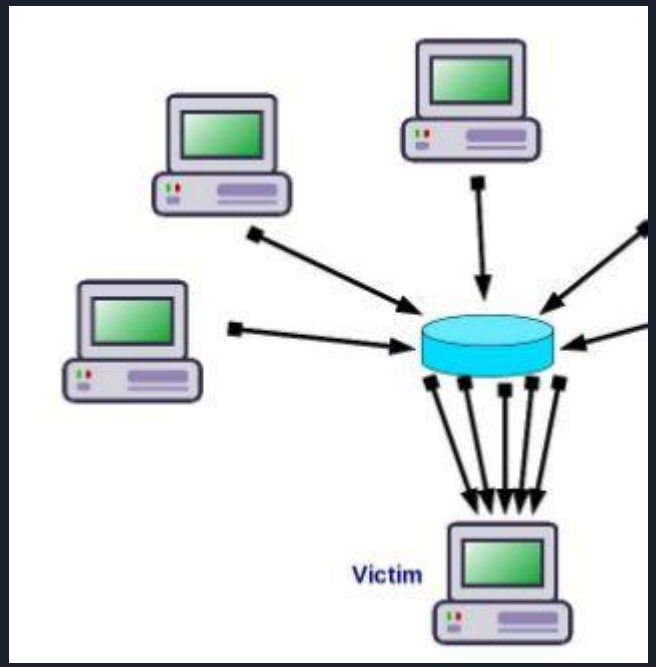
SYN attack/SYN flooding

- A SYN attack affects computers running on the TCP/IP protocol.
- An attacker sends multiple SYN packets to the target computer.
- For each SYN packet received, the target computer allocates resources and sends an acknowledgement (SYN-ACK) to the source IP address. Since the target computer does not receive a response from the attacking computer, it attempts to resend the SYN-ACK.
- This leaves TCP ports in a half-open state. When an attacker sends TCP SYNs repeatedly, the target computer eventually runs out of resources and is unable to handle any more connections, thereby denying services to legitimate users.

SYN Flooding Attack



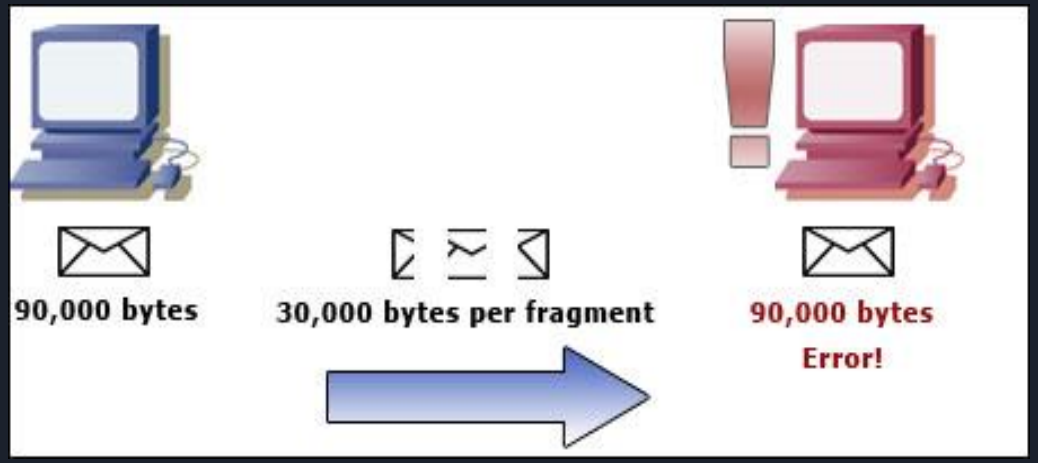
PING flooding



- It relies on the ICMP echo command, more popularly known as ping .
- In legitimate situations the ping command is used by network administrators to test connectivity between two computers.
- In the ping flood attack, it is used to flood large amounts of data packets to the victim's computer in an attempt to overload it.
- Target – Targeted system , Router or blind ping.

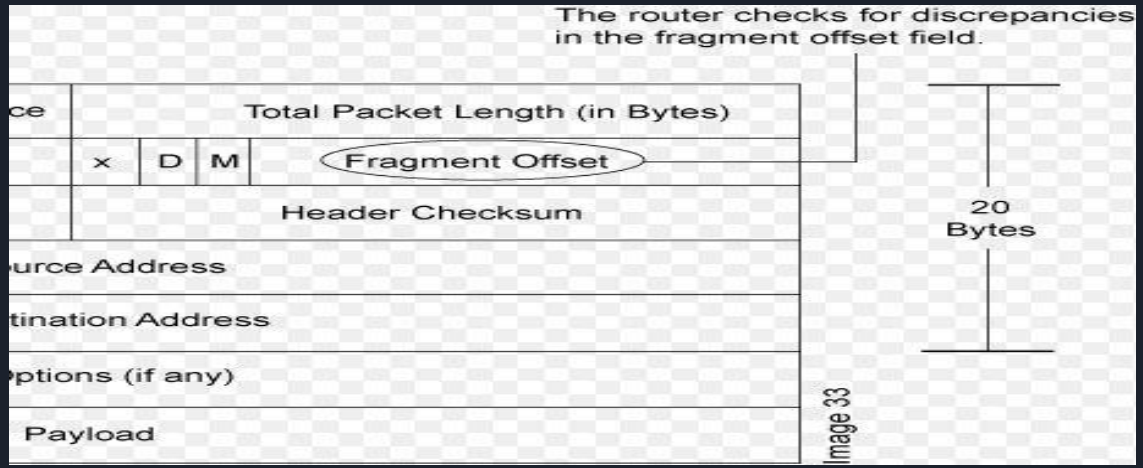
Ping of Death

- The maximum size for a packet is 65,535 bytes. If one were to send a packet larger than that, the receiving computer would ultimately crash from confusion.
- Sending a ping of this size is against the rules of the TCP/IP protocol, but hackers can bypass this by cleverly sending the packets in fragments.



Teardrop Attack

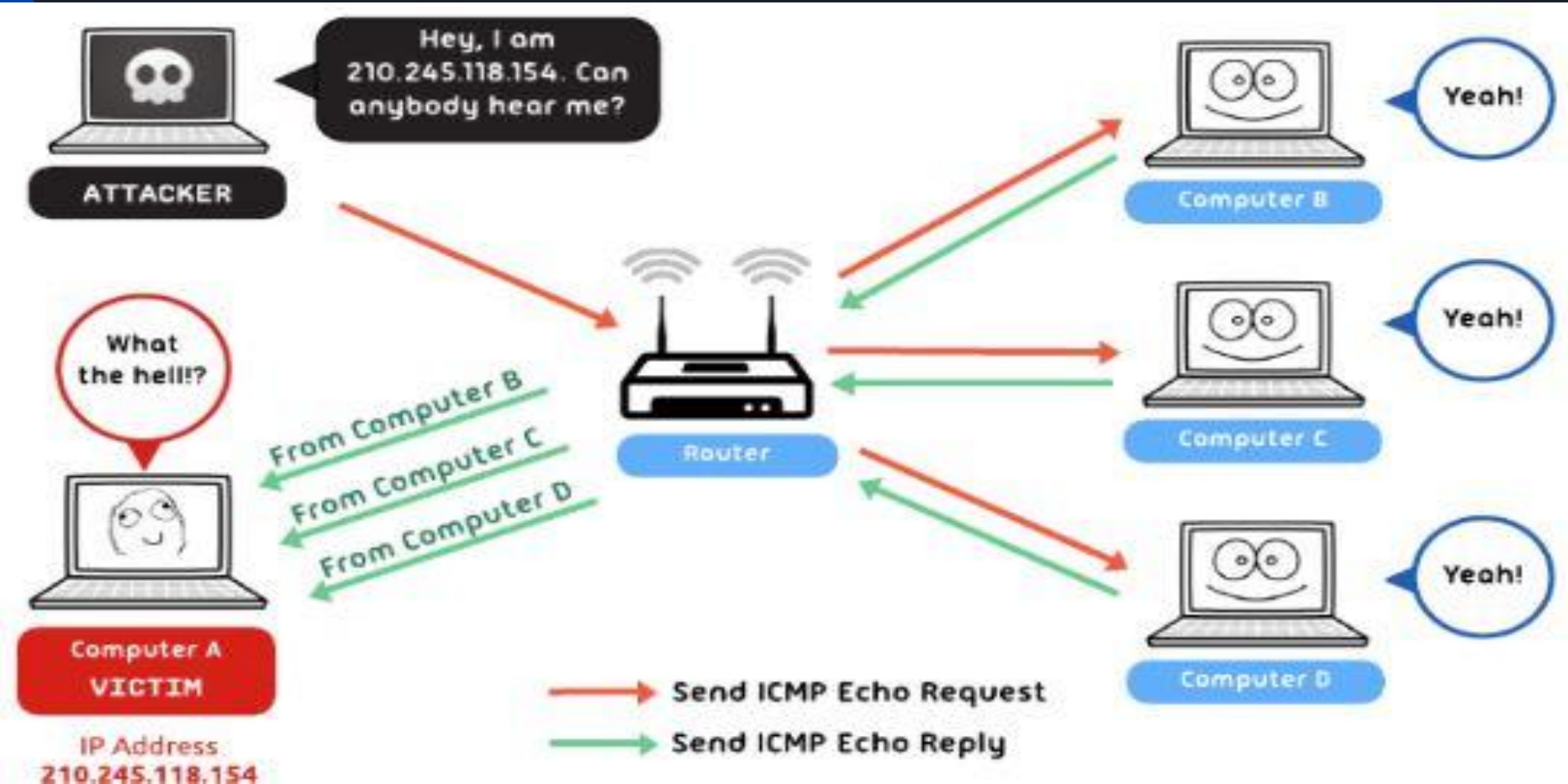
- A teardrop attack is a denial of service (DoS) attack conducted by targeting TCP/IP fragmentation reassembly codes.
- This attack causes fragmented packets to overlap one another on the host receipt; the host attempts to reconstruct them during the process but fails.



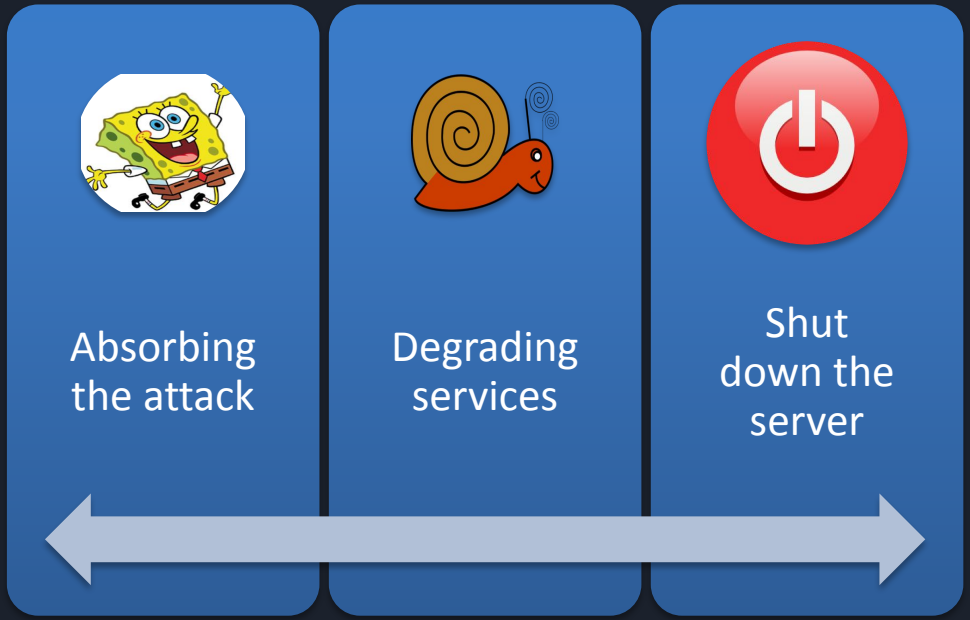
Smurf Attack

- A smurf attack is a type of denial of service attack in which a system is flooded with spoofed ping messages. This creates high computer network traffic on the victim's network, which often renders it unresponsive.
- Smurfing takes certain well-known facts about Internet Protocol and Internet Control Message Protocol (ICMP) into account.
- ICMP is used by network administrators to exchange information about network state, and can also be used to ping other nodes to determine their operational status.
- The smurf program sends a spoofed network packet(broadcasting) that contains an ICMP ping. The resulting echo responses to the ping message are directed toward the victim's IP address.
- Large number of pings and the resulting echoes can make the network unusable for real traffic.

Smurf Attack



DOS/DDOS Countermeasures



- Firewall & Anti virus
- Security awareness
- Disable unnecessary services
- Clean configuration
- Regular Update

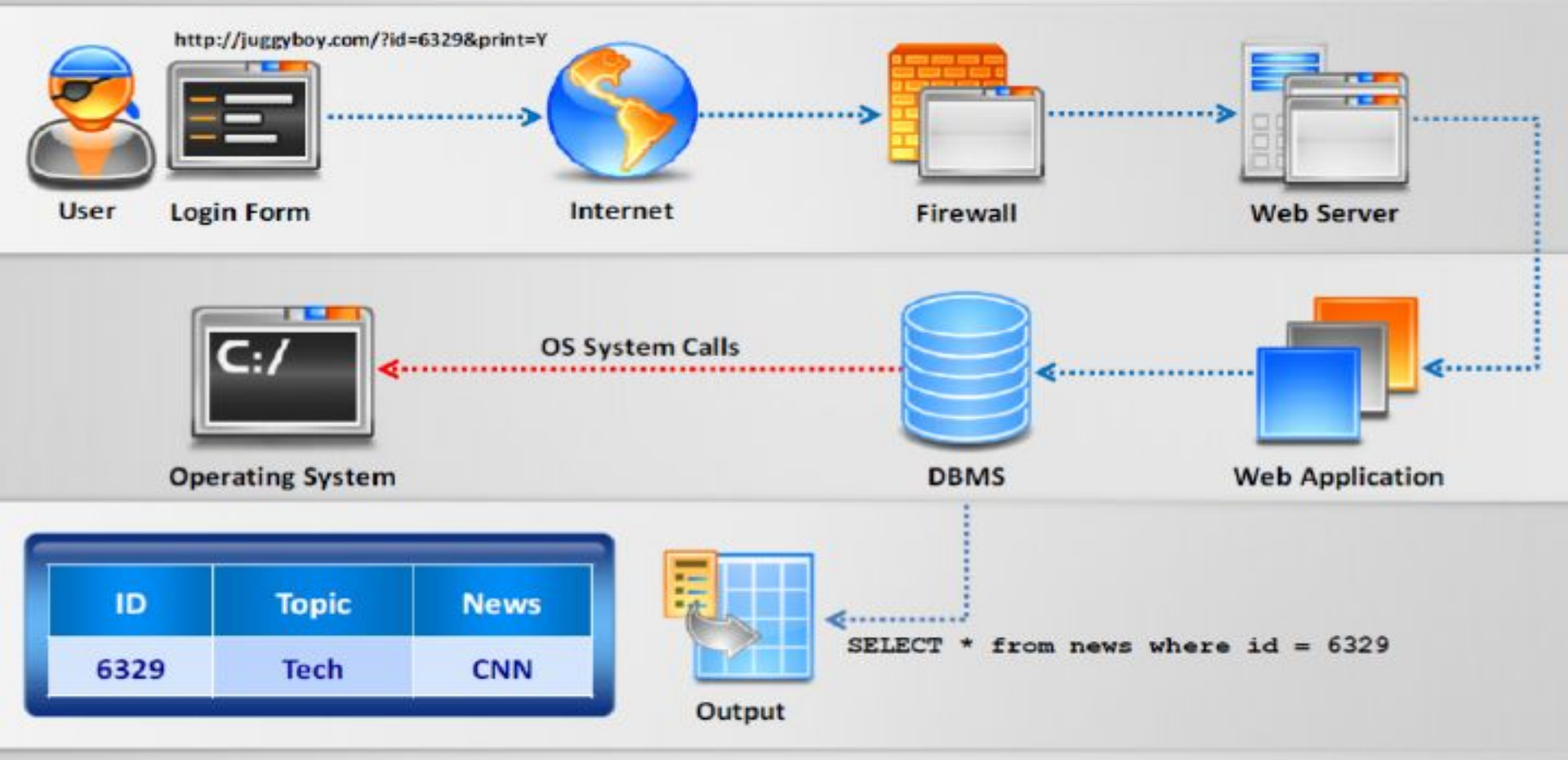
CYBER SECURITY

MODULE - 8

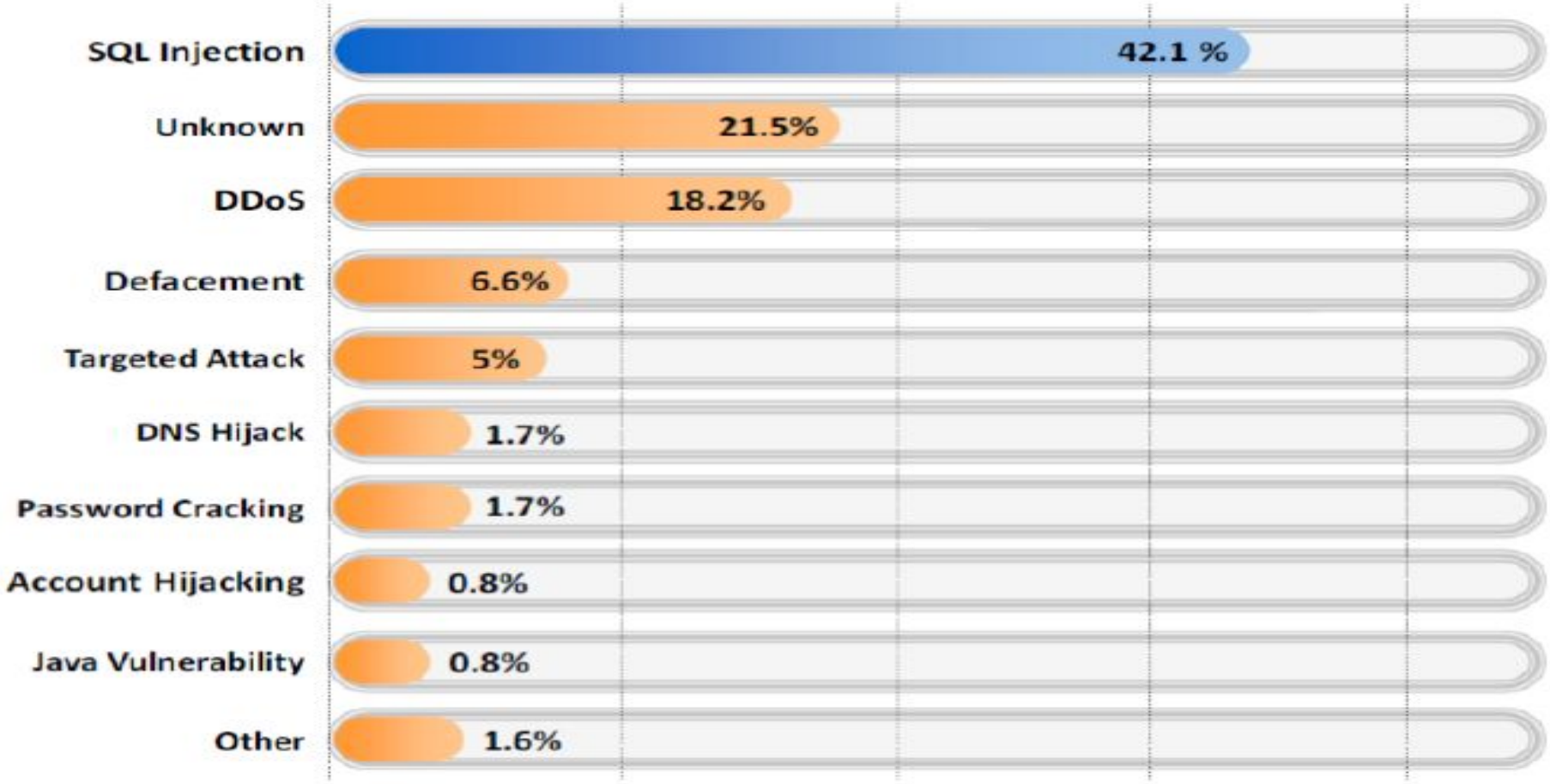
Web & Network Security

Module Duration : 1 hour

How Web Applications Works



Web and Network Attacks



SQL Injection and XSS

- SQL Injection is the most common **website vulnerability** on the Internet

1

- It is a **flaw in Web Applications** and not a database or web server issue

2

- Most programmers are still **not aware** of this threat

3

What is SQL Injection Attack?

- SQL injection is a technique used to take advantage of **non-validated input vulnerabilities** to pass SQL commands through a web application for execution by a **backend database**
- SQL injection is a basic attack used to either **gain unauthorized access** to a database or to **retrieve information** directly from the database

Albert Gonzalez, an indicted hacker stole **130 million credit and debit cards**, the biggest identity theft case ever prosecuted in the United States. He used **SQL injection attacks** to install sniffer software on the companies' servers to **intercept** credit card data as it was being processed.

http://www.theregister.co.uk

SQL Injection Attack Types

Authentication Bypass

Using this attack, an attacker logs onto an application without providing valid user name and password and gains administrative privileges

Remote Code Execution

It assists an attacker to compromise the host OS

Information Disclosure

Using this attack, an attacker obtains sensitive information that is stored in the database

Compromised Availability of Data

Attackers use this attack to delete the database information, delete log, or audit information that is stored in a database

Compromised Data Integrity

An attacker uses this attack to deface a web page, insert malicious content into web pages, or alter the contents of a database

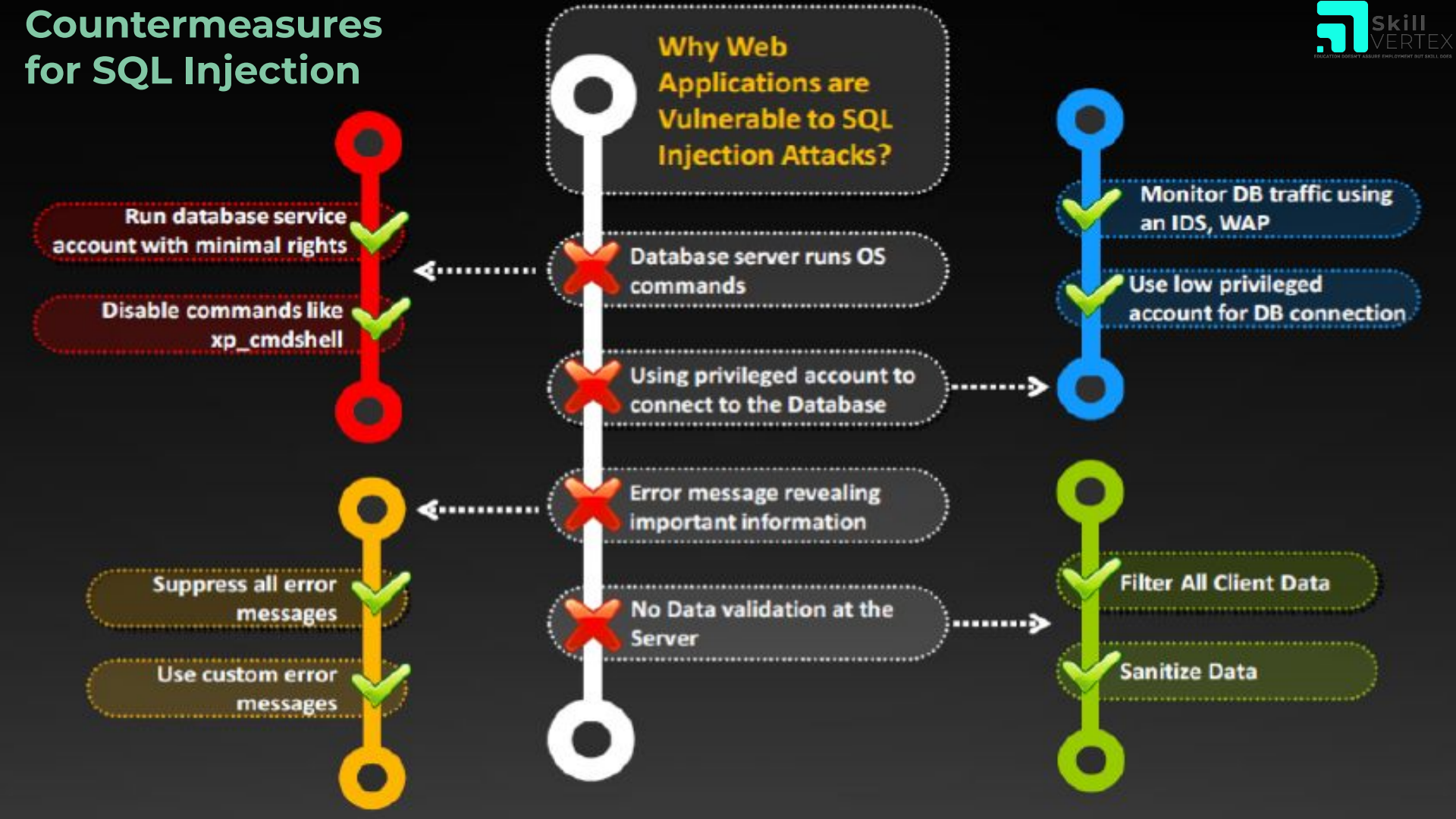
SQL Injection Threats

SQL Injection Methodology

SQL Injection Tools

- BSQL Hacker
- Marathon Tool
- SQL Power Injector
- SQL Map

Countermeasures for SQL Injection



Wireless Networks

- Wi-Fi refers to wireless local area networks (WLAN) based on IEEE 802.11 standard
- It is a widely used technology for wireless communication across a radio channel
- Devices such as a personal computer, video-game console, smartphone, etc. use Wi-Fi to connect to a network resource such as the Internet via a wireless network access point

Advantages

- Installation is fast and easy and eliminates wiring through walls and ceilings
- It is easier to provide connectivity in areas where it is difficult to lay cable
- Access to the network can be from anywhere within range of an access point
- Public places like airports, libraries, schools or even coffee shops offer you constant Internet connections using Wireless LAN

Disadvantages

- Security is a big issue and may not meet expectations
- As the number of computers on the network increases, the bandwidth suffers
- WiFi enhancements can require new wireless cards and/or access points
- Some electronic equipment can interfere with the Wi-Fi networks

Wireless Networks Security using WEP

What Is WEP?

- **Wired Equivalent Privacy** (WEP) is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmissions
- WEP uses a **24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission

64-bit WEP uses a 40-bit key

128-bit WEP uses a 104-bit key size

256-bit WEP uses 232-bit key size

WEP Flaws

It was developed without:

- Academic or public review
- Review from cryptologists

- **It has significant vulnerabilities and design flaws**

Wireless Networks Security using WPA

- Wi-Fi Protected Access (WPA) is a **data encryption method** for WLANs based on 802.11 standards
- A snapshot of 802.11i under development providing **stronger encryption**, and enabling PSK or EAP authentication

TKIP (Temporal Key Integrity Protocol)

- TKIP utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check
- TKIP mitigated vulnerability by **increasing the size of the IV** and using mixing functions

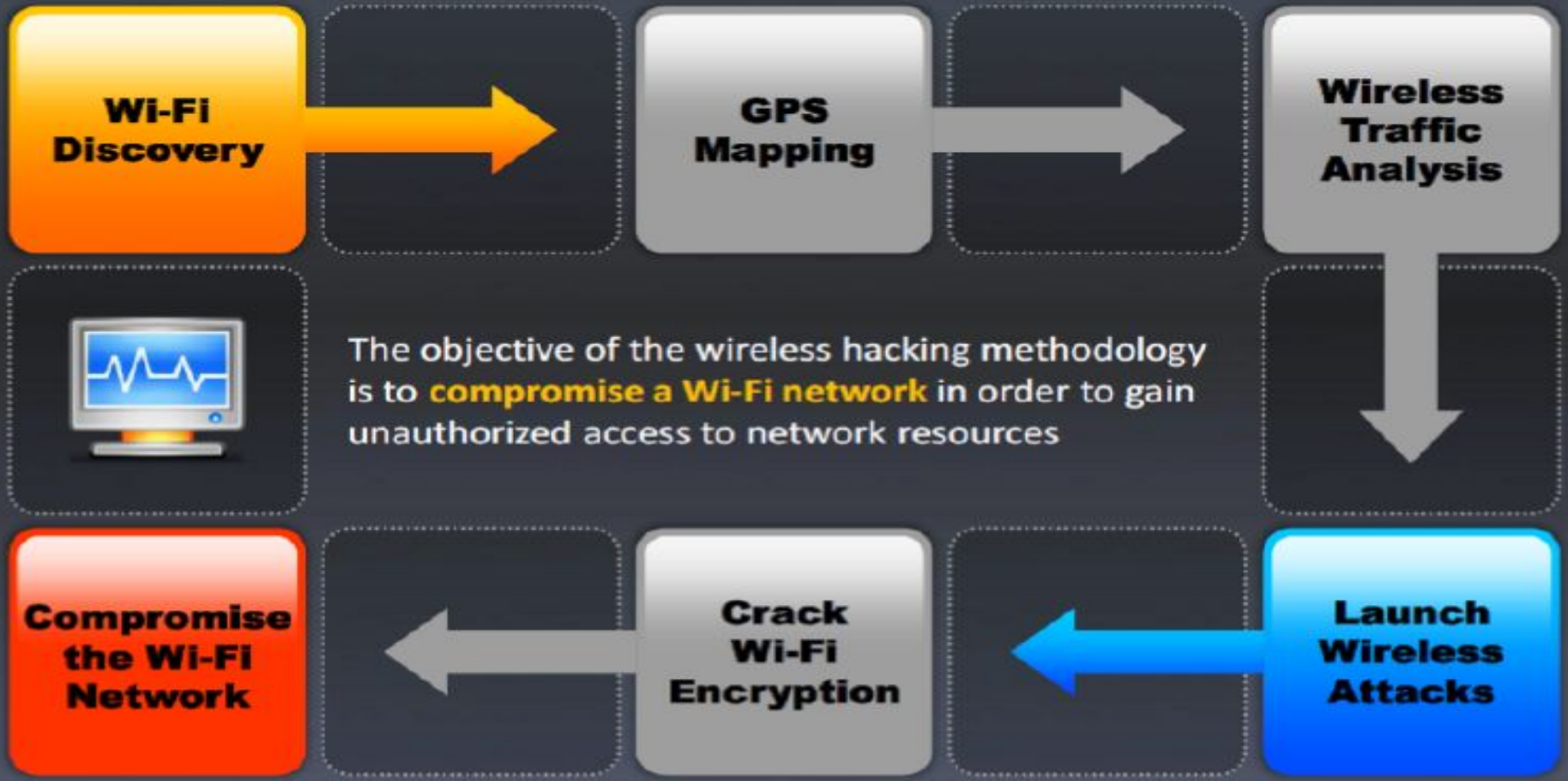
128-bit Temporal Key

- Under TKIP, the client starts with a 128-bit "temporal key" (TK) that is then combined with the client's MAC address and with an IV to create a keystream that is used to encrypt data via the RC4
- It implements a sequence counter to protect against replay attacks

WPA Enhances WEP

- TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys
- Temporal keys are changed for every 10,000 packets. This makes TKIP protected networks more resistant to cryptanalytic attacks involving key reuse

Wireless Hacking Methodology



Wireless Discovery

Steps

1. The first task an attacker will go through when searching for Wi-Fi targets is checking the potential networks that are in range to find the best one to attack
2. Drive around with Wi-Fi enabled laptop installed with a wireless discovery tool and map out active wireless networks

You will need these to discover Wi-Fi networks

- **Laptop with Wi-Fi Card**
- **External Wi-Fi Antenna**
- **Network Discovery Programs**

Tools Used: inSSIDer, NetSurveyor, NetStumbler, Vistumbler etc.

GPS Mapping

- Attackers create map of discovered Wi-Fi networks and **create a database** with statistics collected by Wi-Fi discovery tools such as Netsurveyor, NetStumblers etc.

- GPS is used to **track the location** of the discovered Wi-Fi networks and the **coordinates are uploaded to sites** like WIGLE
- Attackers can **share this information** with the hacking to community or sell it to make money

Attacker

Discovery of Wi-Fi networks

Post the GPS locations to WIGLE

Wireless Traffic Analysis

Identify Vulnerabilities

1. Wireless traffic analysis enables attackers to identify vulnerabilities and susceptible victims in a target wireless network
2. This helps in determining the appropriate strategy for a successful attack
3. Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized which makes easy to sniff and analyze wireless packets

Wi-Fi Reconnaissance

Attackers analyze a wireless network to determine:

- Broadcasted SSID
- Presence of multiple access points
- Possibility of recovering SSIDs
- Authentication method used
- WLAN encryption algorithms

Tools

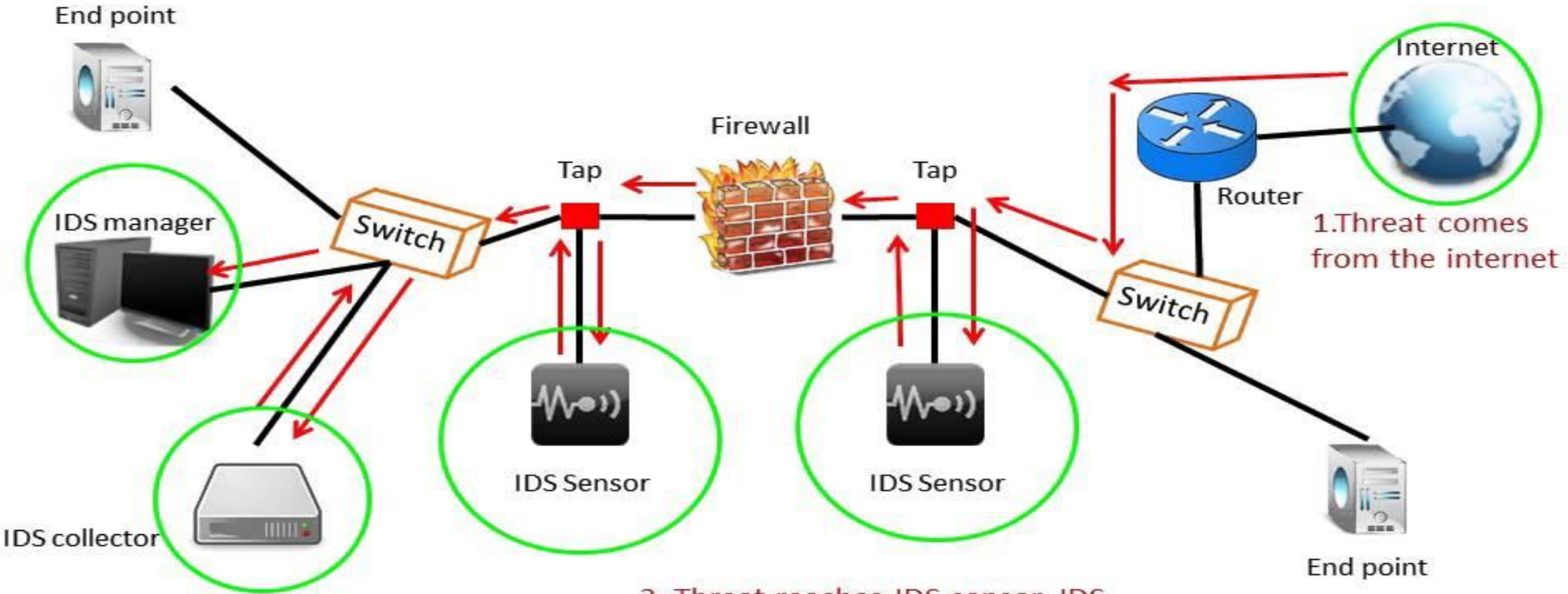
Wi-Fi packet-capture and analysis products come in a number of forms

- Wireshark/Pilot Tool
- OmniPeek Tool
- CommView Tool
- AirMagnet Wi-Fi Analyzer

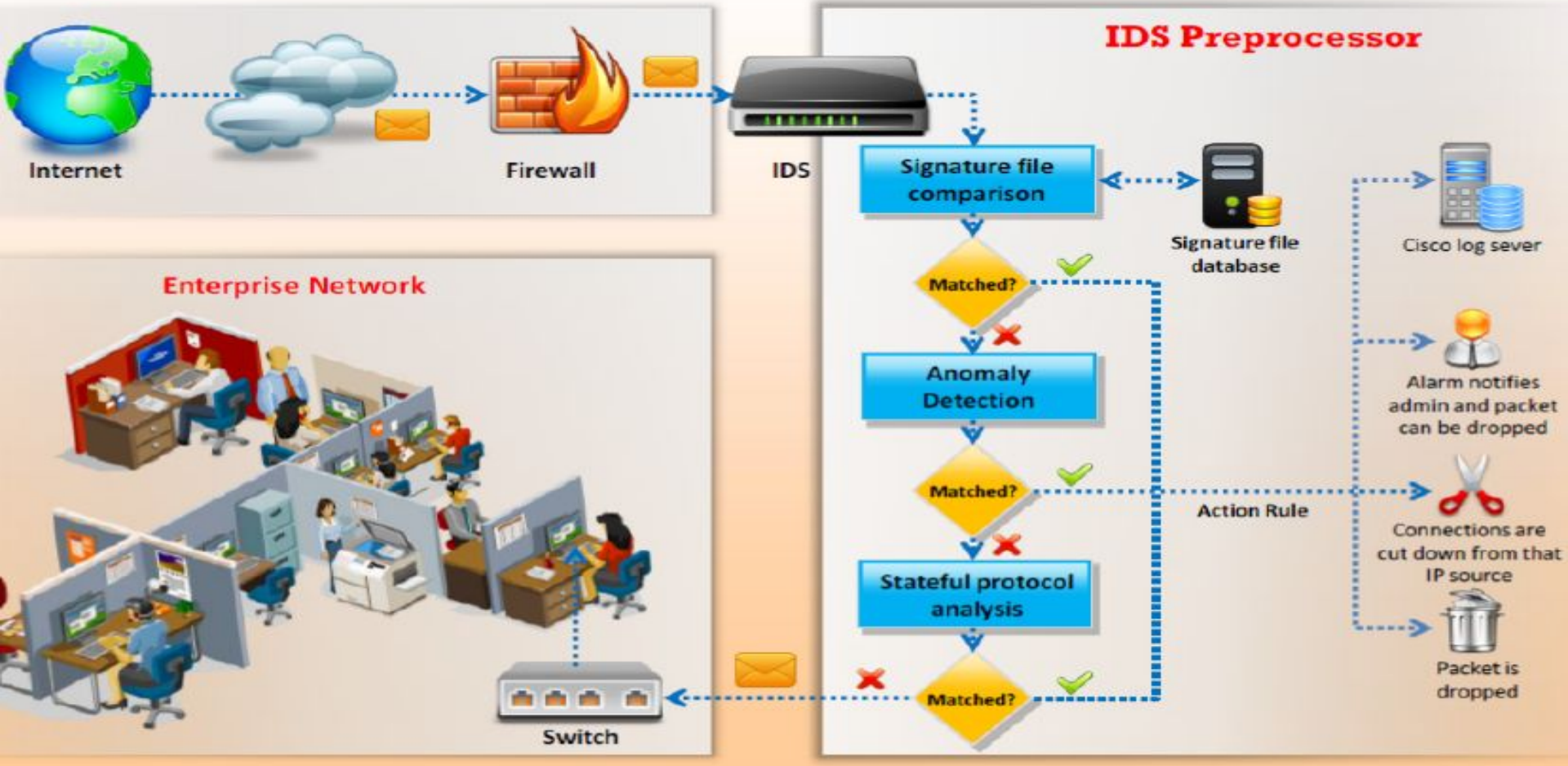
Countermeasures

1. Change the default SSID after WLAN configuration
2. Set the router access password and enable firewall protection
3. Disable SSID broadcasts
4. Disable remote router login and wireless administration
5. Enable MAC Address filtering on your access point or router
6. Enable encryption on access point and change passphrase often

IDS Systems


End point
Internet
Firewall
Tap
Tap
IDS manager
Switch
Router
1.Threat comes from the internet
Switch
IDS Sensor
IDS Sensor
IDS collector
End point
3. The IDS collector analyse the threat and sends report to the IDS manager.
2. Threat reaches IDS sensor. IDS sensor monitors the network. When there is a threat detected, it passes information to the collector.

IDPS Systems



IDS System Detection Mechanism

Signature Recognition

It is also known as misuse detection. Signature recognition tries to **identify events** that misuse a system

Anomaly Detection

It detects the **intrusion based** on the fixed behavioral characteristics of the users and components in a computer system

Protocol Anomaly Detection

In this type of detection, models are built to explore **anomalies** in the way vendors deploy the **TCP/IP specification**

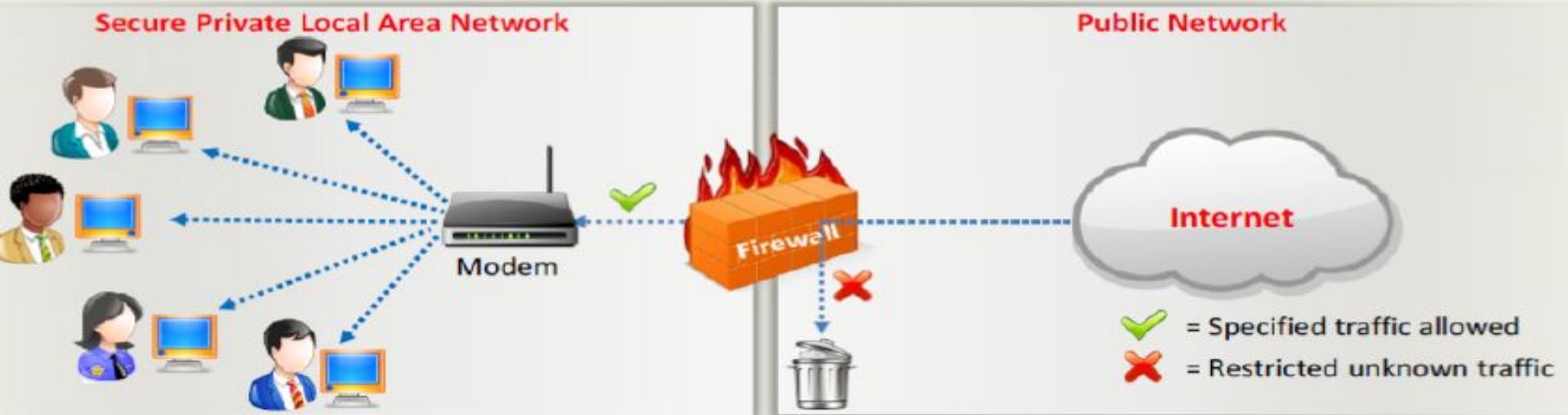
Firewall

Firewalls are hardware and/or software designed to prevent **unauthorized access** to or from a private network

Firewalls **examine all messages entering or leaving the Intranet** and blocks those that do not meet the specified security criteria

They are placed at the junction or **gateway** between the two networks, which is usually a private network and a public network such as the Internet

Firewalls may be concerned with the type of traffic or with the **source** or **destination addresses** and ports



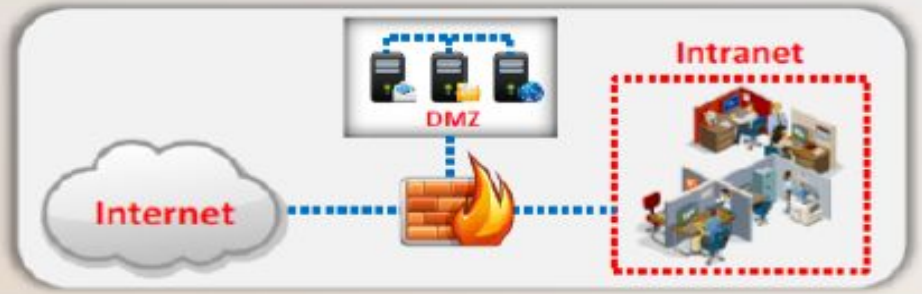
Firewall Architecture

Bastion Host:

- Bastion host is a computer system designed and configured to protect network resources from attack
- Traffic entering or leaving the network passes through the firewall, it has two interfaces:
  - public interface directly connected to the Internet
  - private interface connected to the Intranet

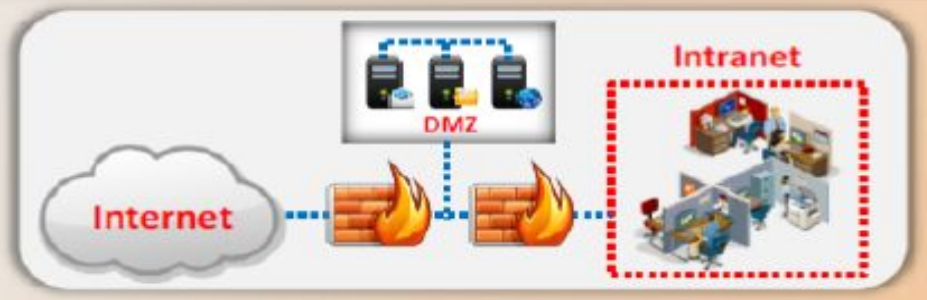
Screened Subnet:

- The screened subnet or DMZ (additional zone) contains hosts that offer public services
- The DMZ zone responds to public requests, and has no hosts accessed by the private network
- Private zone can not be accessed by Internet users

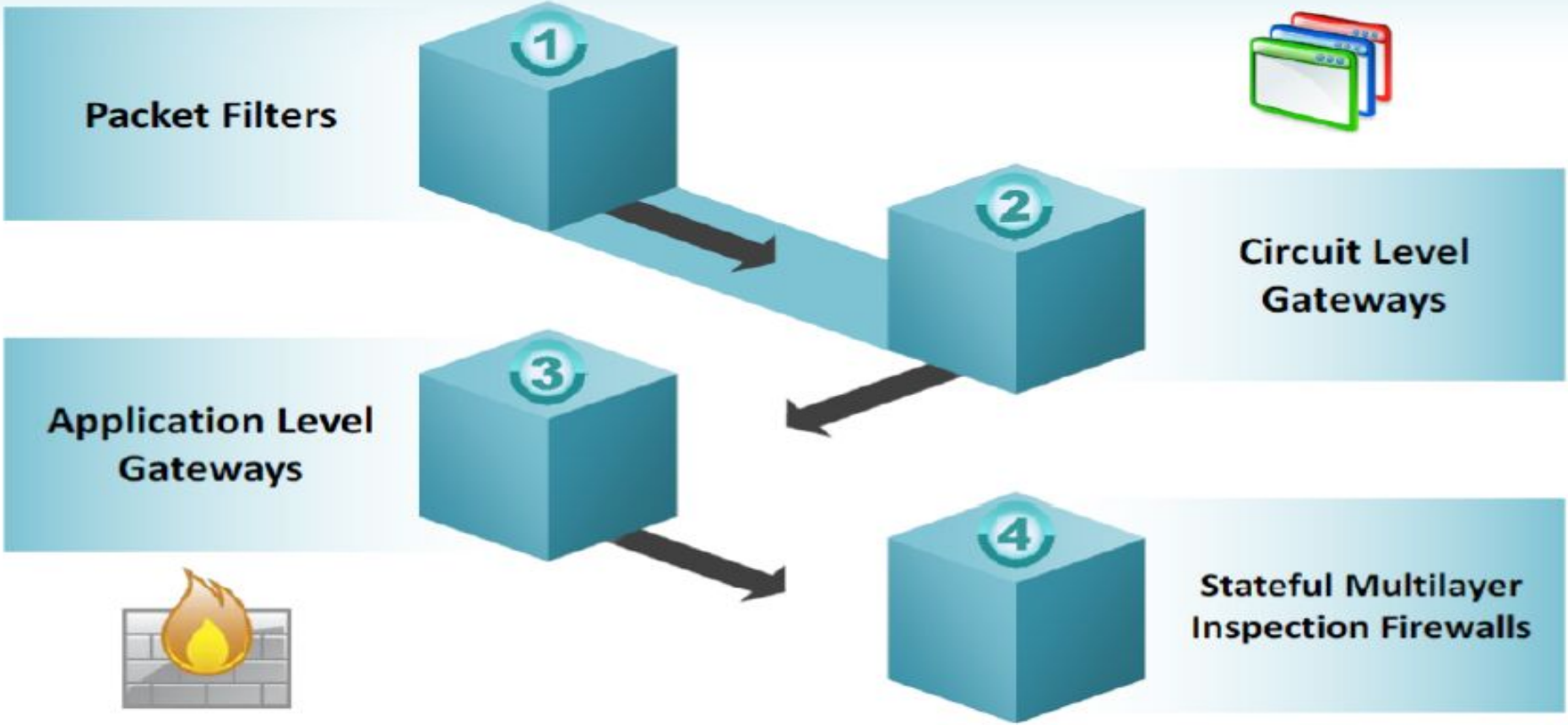


Multi-homed Firewall:

- In this case, a firewall with three or more interfaces is present that allows for further subdividing the systems based on the specific security objectives of the organization



Types of Firewall



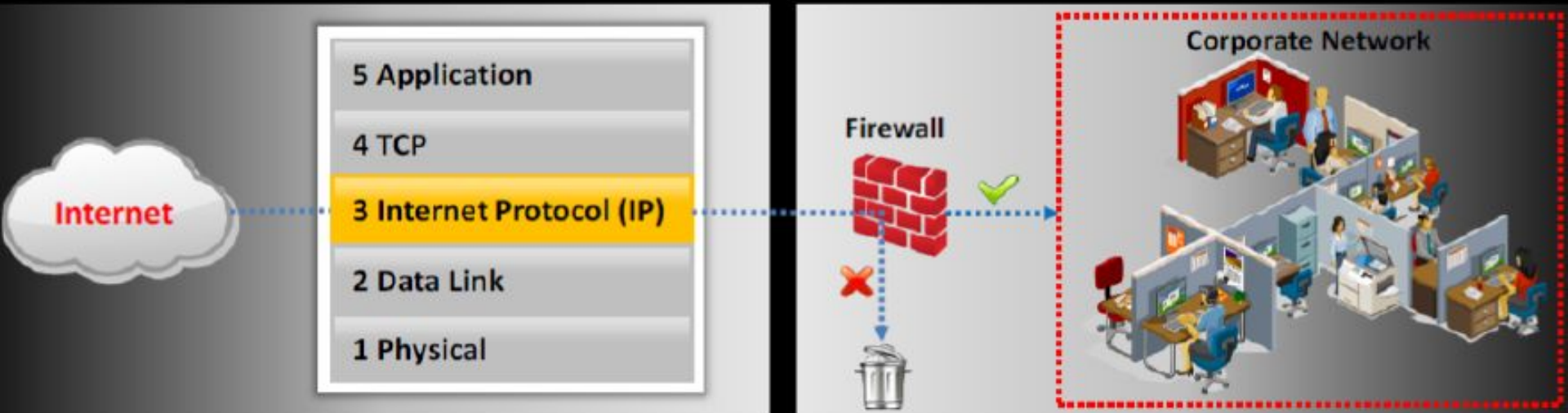
Packet Filtering Firewall

Packet filtering firewalls work at the **network level of the OSI model** (or the IP layer of TCP/IP), they are usually a part of a router

Depending on the **packet and the criteria**, the firewall can drop the packet and forward it, or send a message to the originator

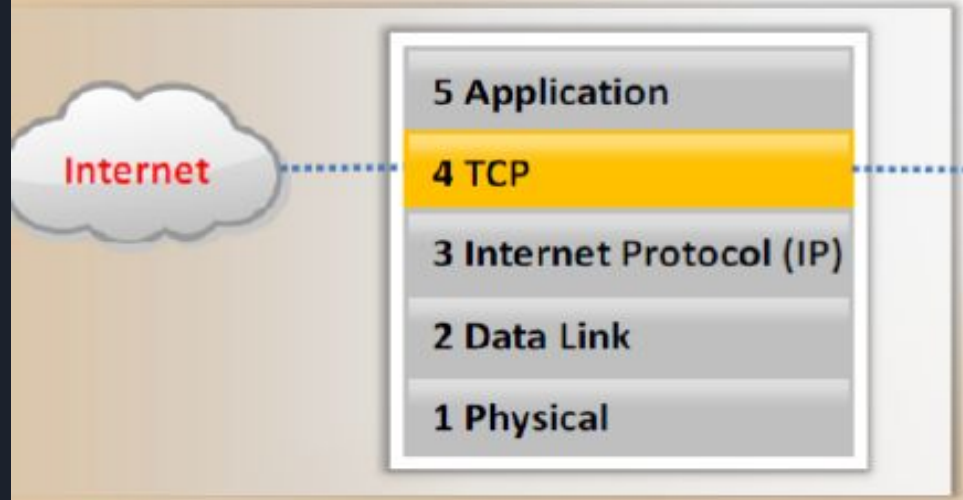
In a packet filtering firewall, **each packet is compared** to a set of criteria before it is forwarded

Rules can include the source and the destination **IP address**, the source and the destination **port number**, and the **protocol** used



Circuit Level Firewall

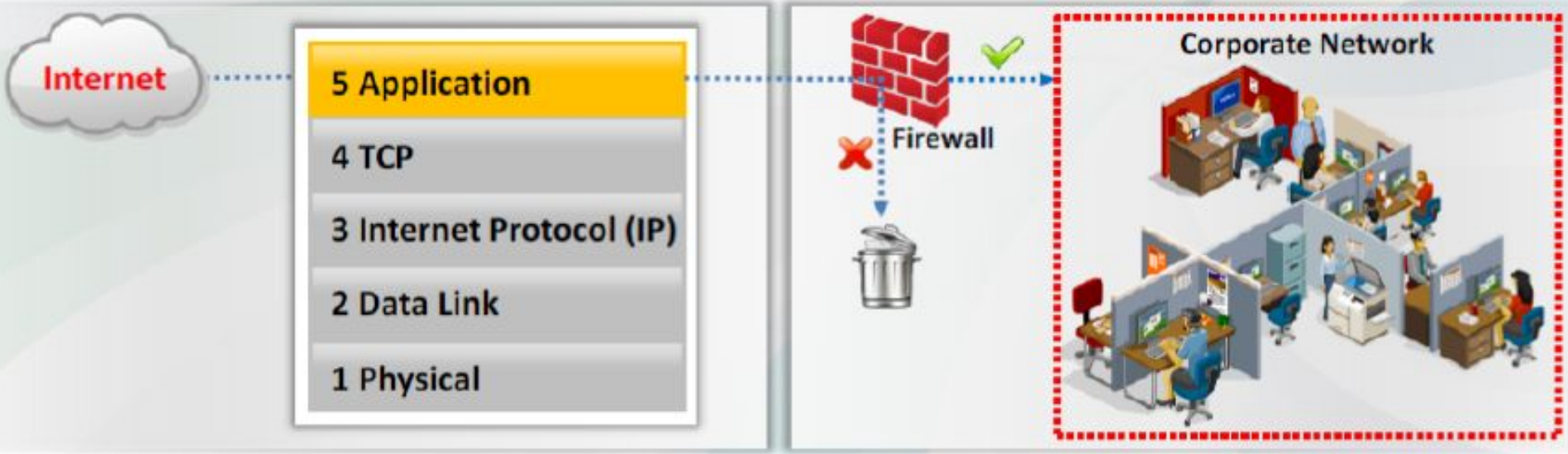
- Circuit-level gateways work at the session layer of the OSI model or the TCP layer of TCP/IP
- Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway
- They monitor requests to create sessions, and determine if those sessions will be allowed
- Circuit proxy firewalls allow or prevent data streams, they do not filter individual packets



Application Level Firewall

- Application-level gateways (proxies) can filter packets at the application layer of the OSI model
- Incoming and outgoing traffic is restricted to services supported by proxy; all other service requests are denied

- Application-level gateways configured as a web proxy prohibit FTP, gopher, telnet, or other traffic
- Application-level gateways examine traffic and filter on application-specific commands such as http:post and get



Stateful Multilayer Inspection Firewall

- Stateful multilayer inspection firewalls **combine the aspects of the other three types** of firewalls
- They **filter packets at the network layer**, to determine whether session packets are legitimate, and they evaluate the contents of packets at the application layer