iiNURTURE
Education Solutions
TOMORROW'S HERE

Chapter 2.1

Sniffers and DoS

Aim

To equip the students with the process of Sniffing and Session hijacking so that it can be procedural approach can be followed while performing sniffing and hijacking

Instructional Objectives

Objectives of this chapter are:

- Describe Sniffing and types of Sniffing
- List various Sniffing tools and how they work
- Explain the methods to prevent Sniffing
- Explain how session hijacking works in a TCP communication process
- List tools used for Session hijacking, with their features
- Explain DoS attacks and their consequences
- Describe categorization of DoS attacks

Learning Outcomes

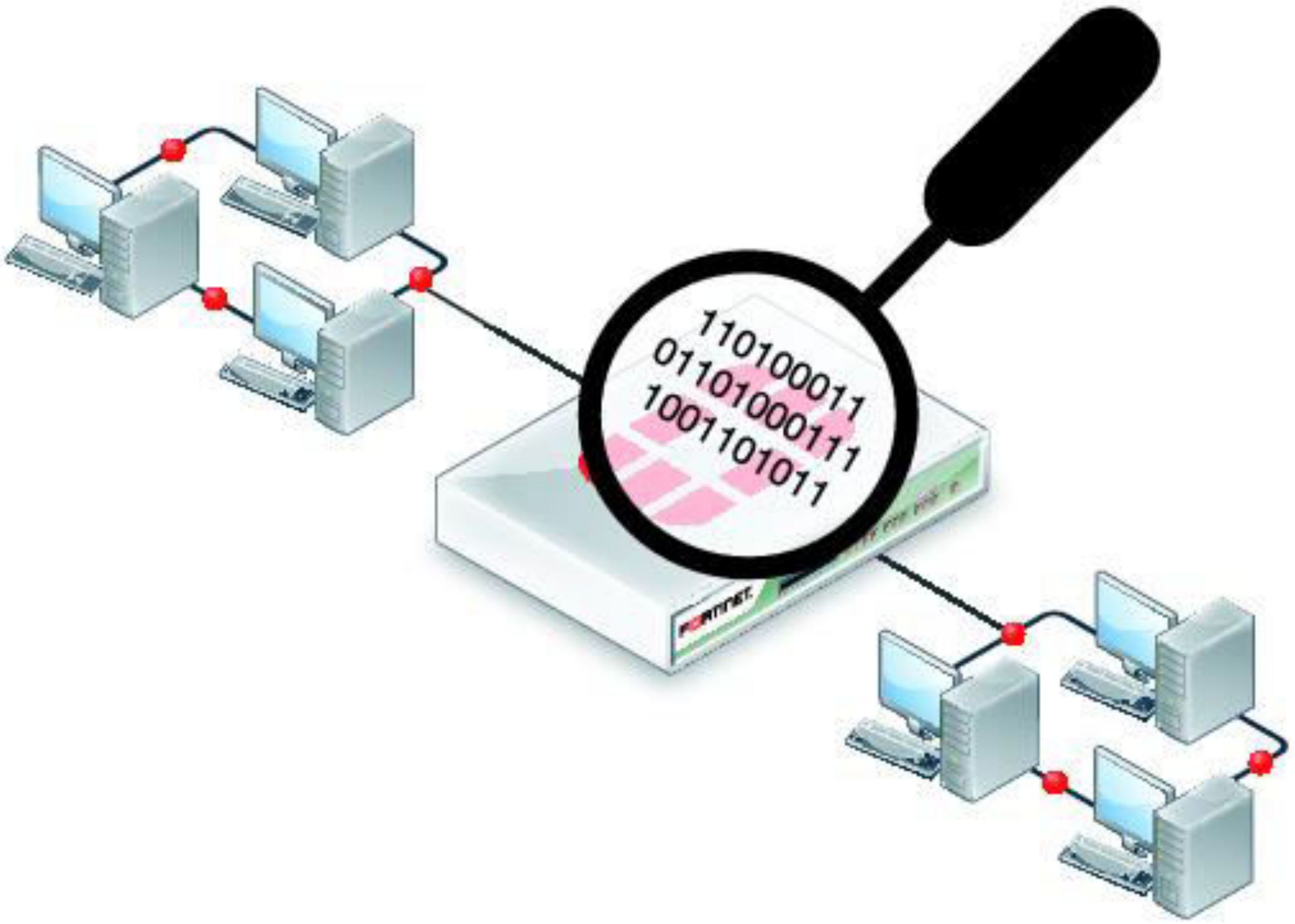
At the end of this chapter, you are expected to:

- Define Sniffing
- Describe the role of Sniffers in hacking
- Identify Sniffing tools and their features
- Summarise the steps in Session hijacking by taking the instance of TCP
- Compare different Session hijacking tools
- Explain how DoS attacks work, with examples

Sniffer and its types

Introduction to Sniffing

Searching for Information in the network

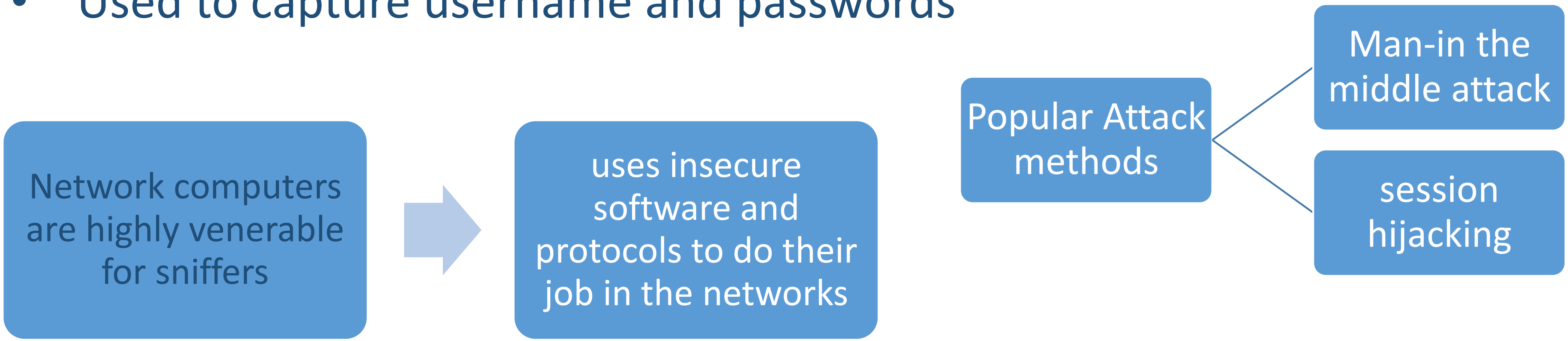


Preventive measure to tackle the network sniffing

Sniffers

Process of gathering traffic from a network by capturing the data as they pass and storing them to analyse later

- It can be a hardware or a software
- Used to capture username and passwords



Network computers are highly venerable for sniffers

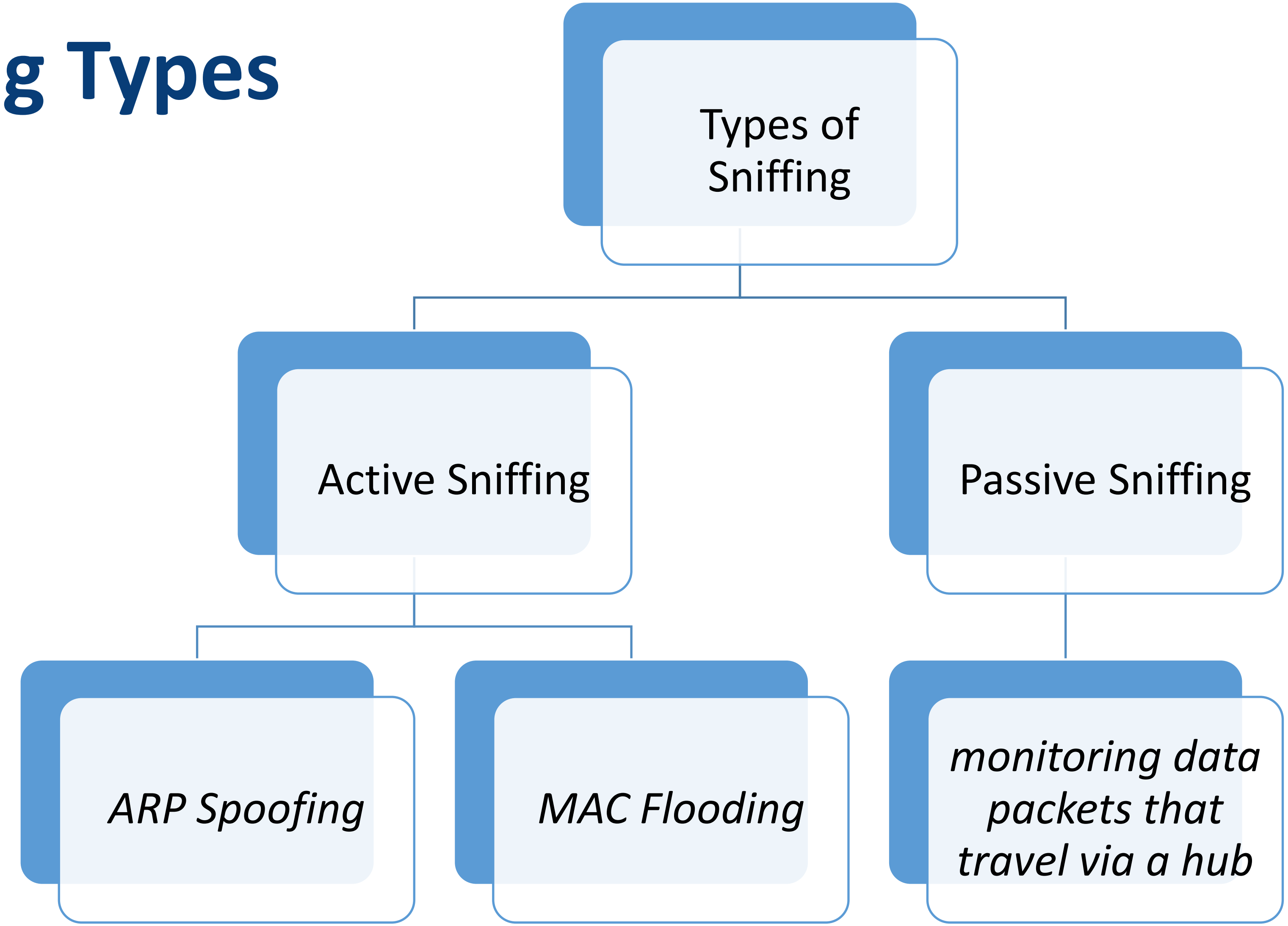
uses insecure software and protocols to do their job in the networks

Popular Attack methods

Man-in the middle attack

session hijacking

Sniffing Types



Types of Sniffing

Active Sniffing

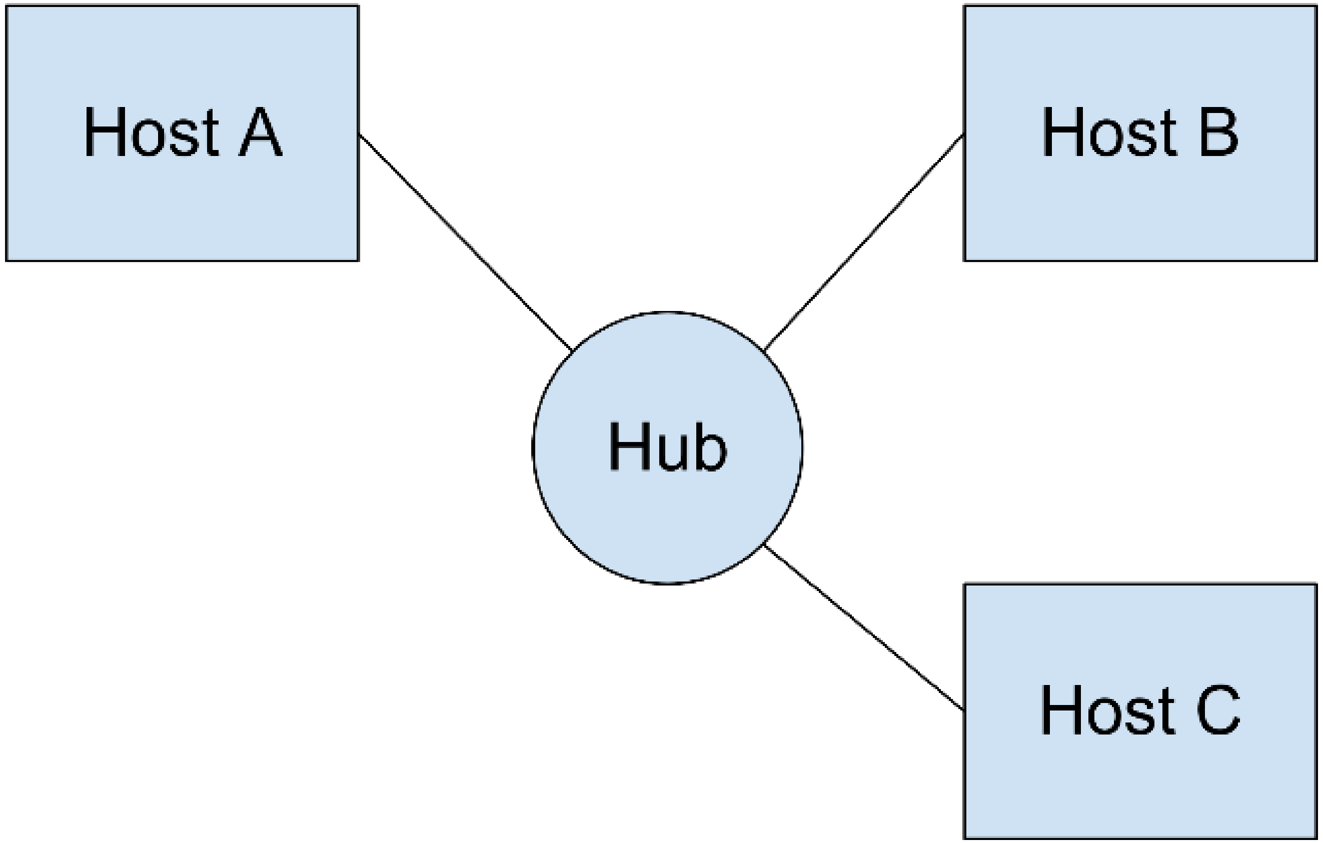
Passive Sniffing

ARP Spoofing

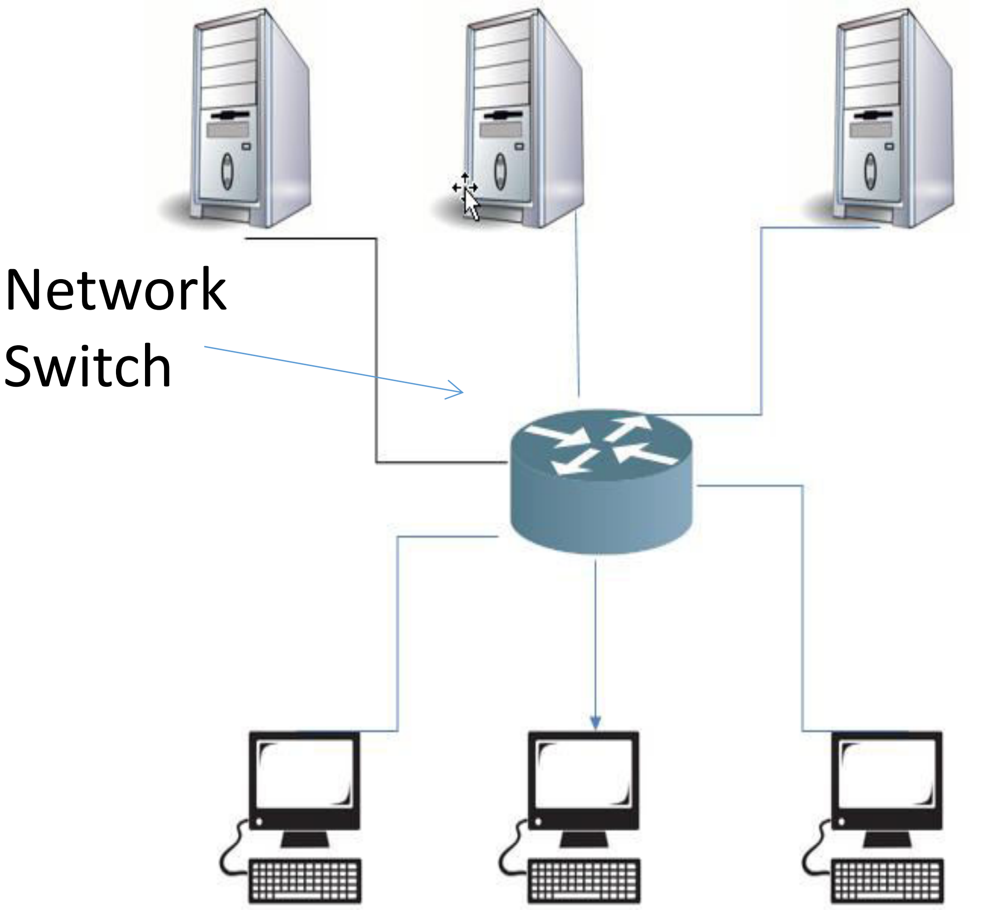
MAC Flooding

monitoring data packets that travel via a hub

Passive Sniffing



Active Sniffing



ARP Spoofing

- Positions himself between target and the intended recipient
- Starts sending fake ARP requests

MAC Flooding

- It occurs when the values in the MAC address overflows
- MAC table also called Content Addressable Memory (CAM) Table

Steps involved in ARP Spoofing

Step 1

- The attacker sets the IP address of any ARP Spoofing tool that he wishes to use (Like Arpspoof, Cain and Abel or Arpoison) to match IP subnet of a target. He also scans for IP and MAC addresses of hosts in target's subnet

Step 2

- From this list of hosts, he chooses his target and starts sending ARP packets across the network. These packets contain attackers MAC address and target's IP address

Step 3

- Other hosts on the LAN cache the spoofed ARP packets and as the MAC address will be that of the attacker, they will start sending the outbound traffic to the attacker.

Step 4

- With the information that he wanted in his possession now, the attacker can launch higher level attack.

Sniffing Tools

Snort

- Open source Utility
- Intrusion detection and sniffing
- Works well on Windows, Unix and Linux
- Behaves like Network packet analyser

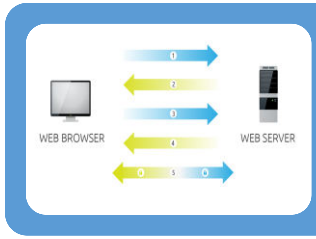
Dsniff

- Collective of tools
- Used in Network Auiditing and penetration testing
- Network monitoring tools: filesnarf, mailsnarf,msgsnarf, urlsnarf, webspy
- Intercept network traffic: Arpspoof, dnsspoof, macof,

Wireshark

- Formerly called Ethereal and is a free-ware
- network analyser that is used for both Windows and Unix platforms
- most preferred network analysing tool

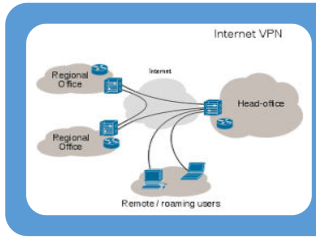
To prevent Sniffing in a network



Secure Socket Layer

IP Security

Pretty Good Privacy (PGP) and Multipurpose Internet Mail Extensions (MIME)



Virtual Private Network or VPN

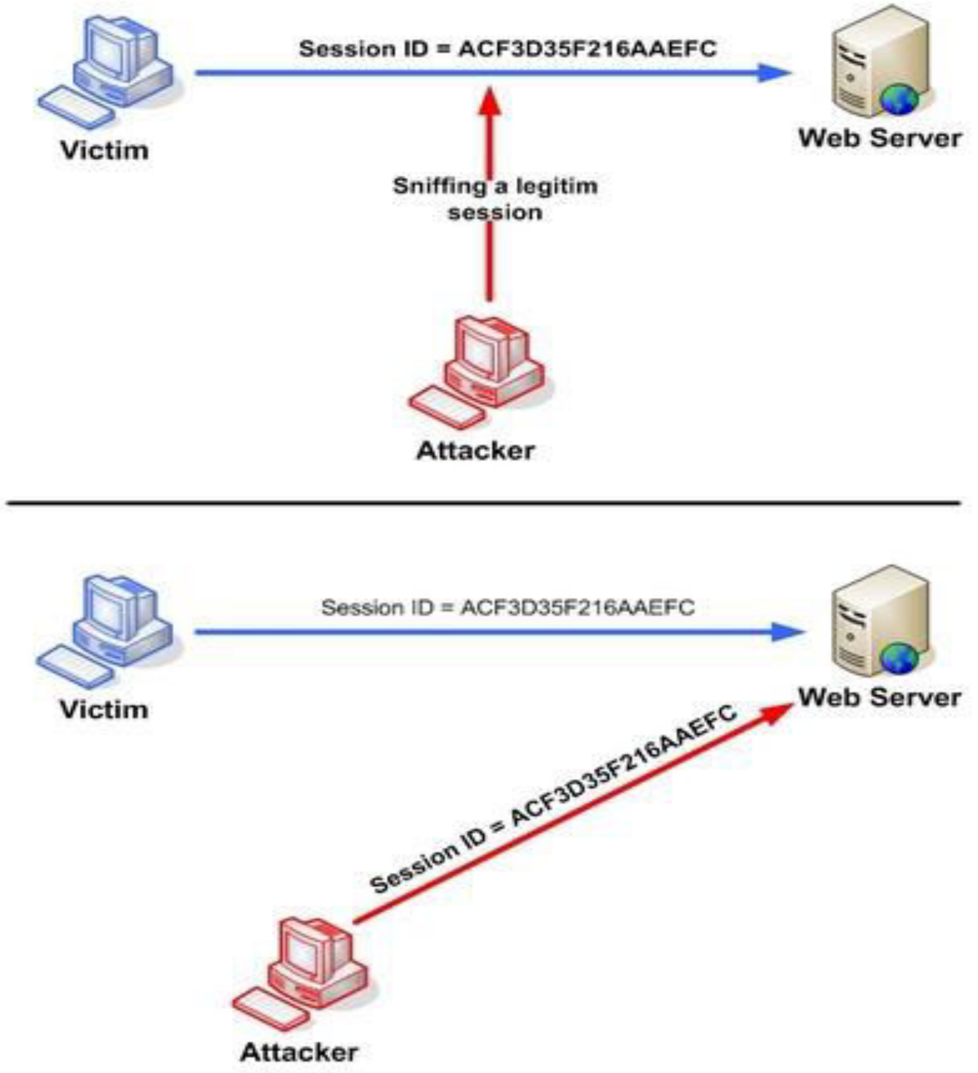
Quiz / Assessment

1) Hubs and Switches operate at the ------------ layer and --------- layer, of the OSI mode, respectively			
a) Physical and Network	b) Physical and Data Link	c) Network and Transport	d) Network and Application
2) Which among the options is an active sniffing method?			
a) ARP Spoofing	b) MAC flooding	c) Both a. and b.	d) Password sniffing

Session Hijacking

"An act of taking control over an active user session by obtaining access to a valid session ID "

A protocol refers to '*rules that define the format in which messages will be exchanged between two layers of communication'*

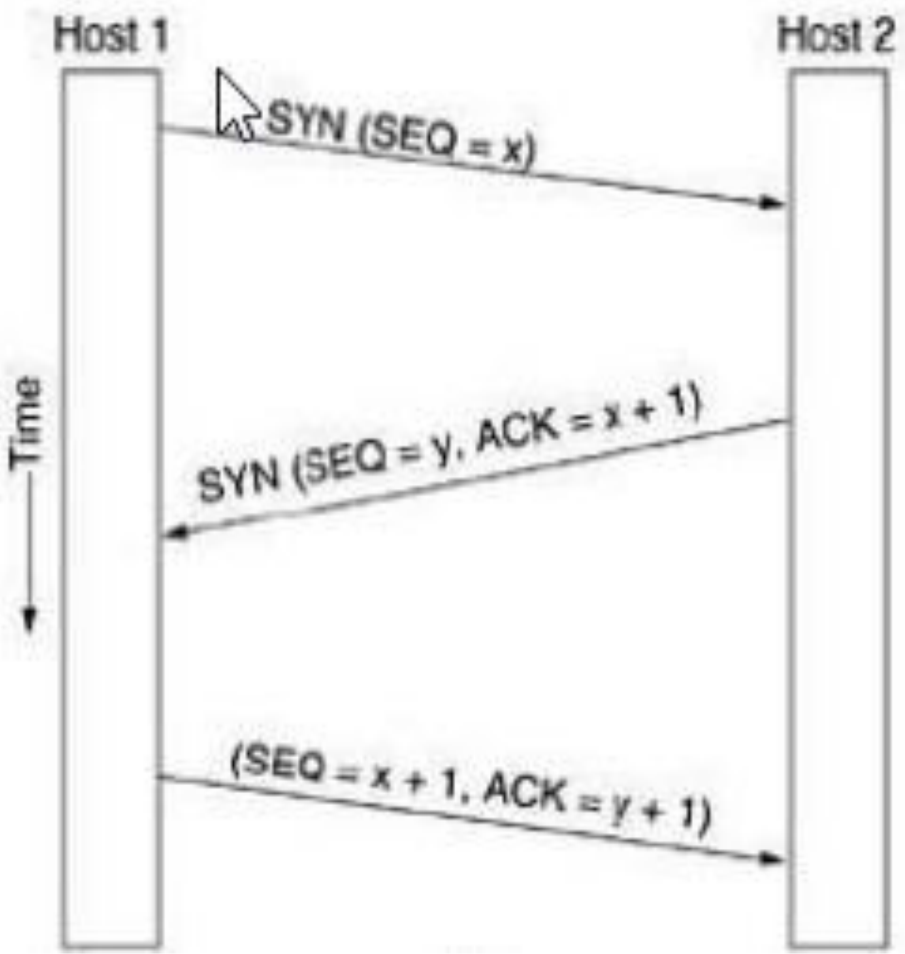

Victim
Session ID = ACF3D35F216AAEFC
Web Server
Sniffing a legitim session
Attacker
Victim
Session ID = ACF3D35F216AAEFC
Web Server
Session ID = ACF3D35F216AAEFC
Attacker

Steps in Session Hijacking

A protocol refers to ‘*rules that define the format in which messages will be exchanged between two layers of communication*’

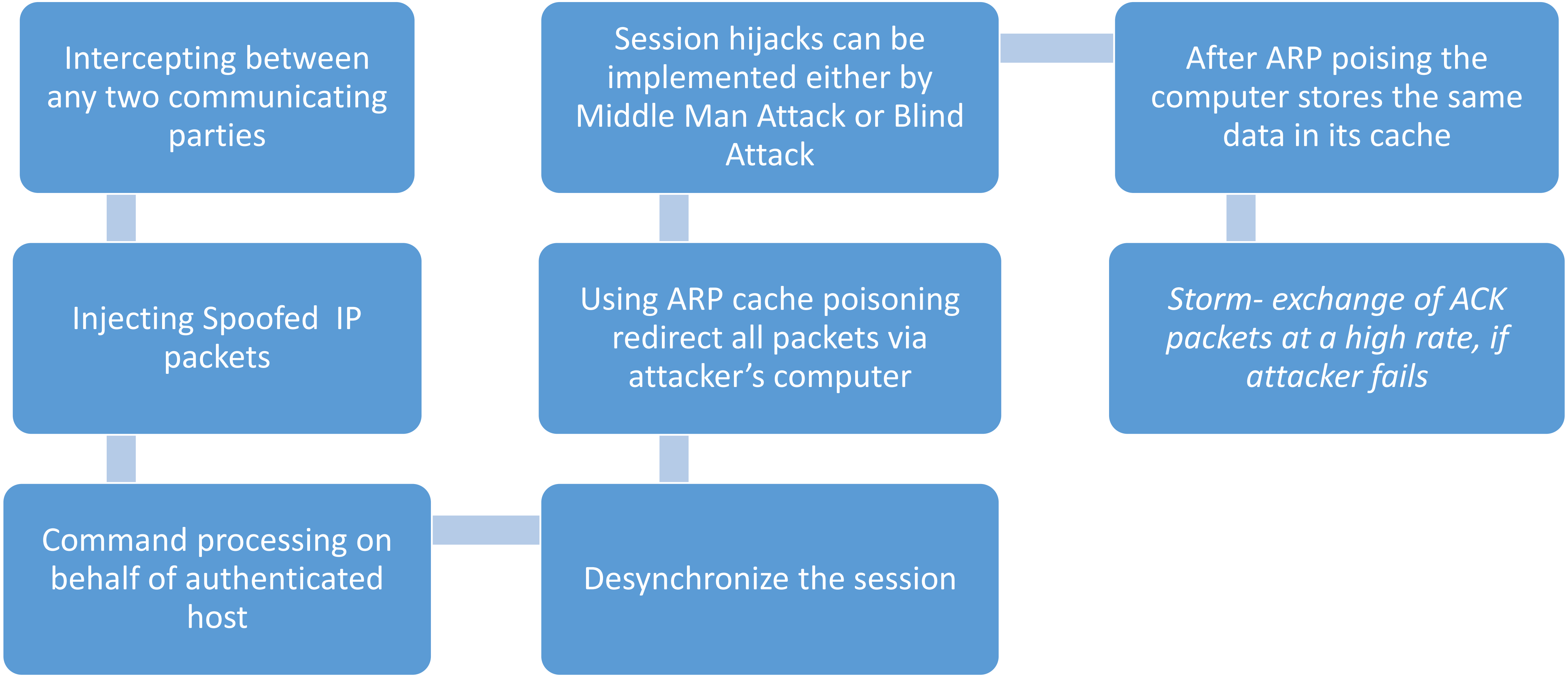
Application Layer	• Enables applications to access the services and defines the protocols applications that must use in order to exchange data • Protocols: HTTP, FTP, SMTP, Telnet, DNS RIP
Host-to-Host Transport	• Provides *session services* and *datagram services*to Application layer • Protocol: TCP, UDP
Internet	• Addressing, Packaging, Routing • Protocols: IP, ARP, ICMP, IGMP
Network Interface (Network Access)	• Placing and removing TCP/ IP packets to connect different network types that consists of Data Link layer and Physical Layer • Protocols: In LAN – Ethernet and Token Ring and In WAN – X.25 and Frame Relay

Method of Session hijacking



three-way handshake
method

TCP /IP Session hijack



Intercepting between any two communicating parties

Injecting Spoofed IP packets

Command processing on behalf of authenticated host

Desynchronize the session

Using ARP cache poisoning redirect all packets via attacker's computer

Session hijacks can be implemented either by Middle Man Attack or Blind Attack

After ARP poising the computer stores the same data in its cache

Storm- exchange of ACK packets at a high rate, if attacker fails

Session hijacking tools

Involves two main processes:

1. The attacker must gain the correct Sequence Number

2. The attacker must perform ARP Spoofing successfully

Examples

Ettercap

- comprehensive tool used for man-in-the-middle attack
- supports many features for network and host analysis

Hunt

- An internal software in UNIX to predict Sequence number and masks the work station

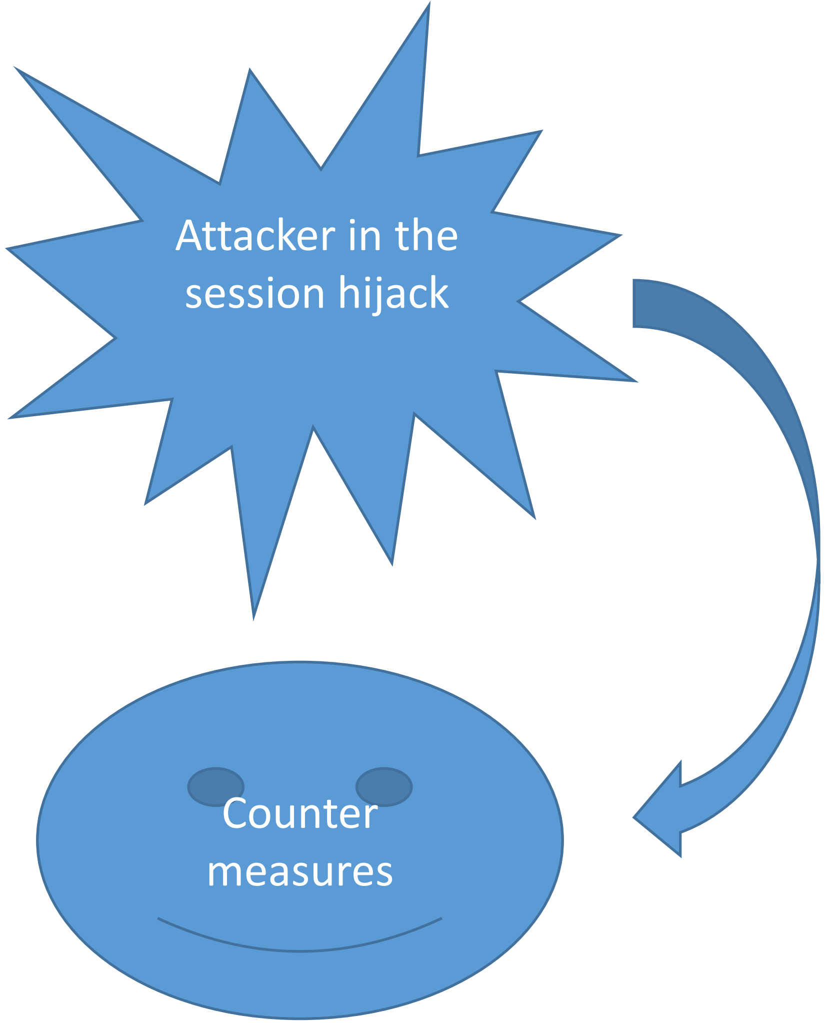
Juggernaut

- Most preferred method that runs only on Linux platform and contains a built-in network sniffer

T-Sight

- Comercially available tool that automatically selects automatically selects open sessions, accurately predicts Sequence Numbers and silence target computers

Methods to prevent Session hijacking



Attacker in the session hijack

Counter measures

Quiz / Assessment

3) The function of Address Resolution Protocol (ARP) is to _______________

a) Provide transmission of data packets

b) Deliver packets

c) Assign source and data addresses to each packet

d) Facilitate transmission and reception of emails

4) Continued state of exchange of ACK packets at high rate, that may suspend the communication on the network, is called as ______________________

a) Denial of Service attack

b) Spoofing

c) ACK Storm

d) blind session hijacking

Categories of DoS Attacks

Basic Types of DOS Attacks

- Consumption of resources
- Protocol attacks
- Logic attacks

Another Category of DOS Attacks

- Application layer Attacks
- Network layer Attacks

Denial of Service

A 'denial-of-service' attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

Denial of Service attempts to

Flood

- Resulting in halting network traffic

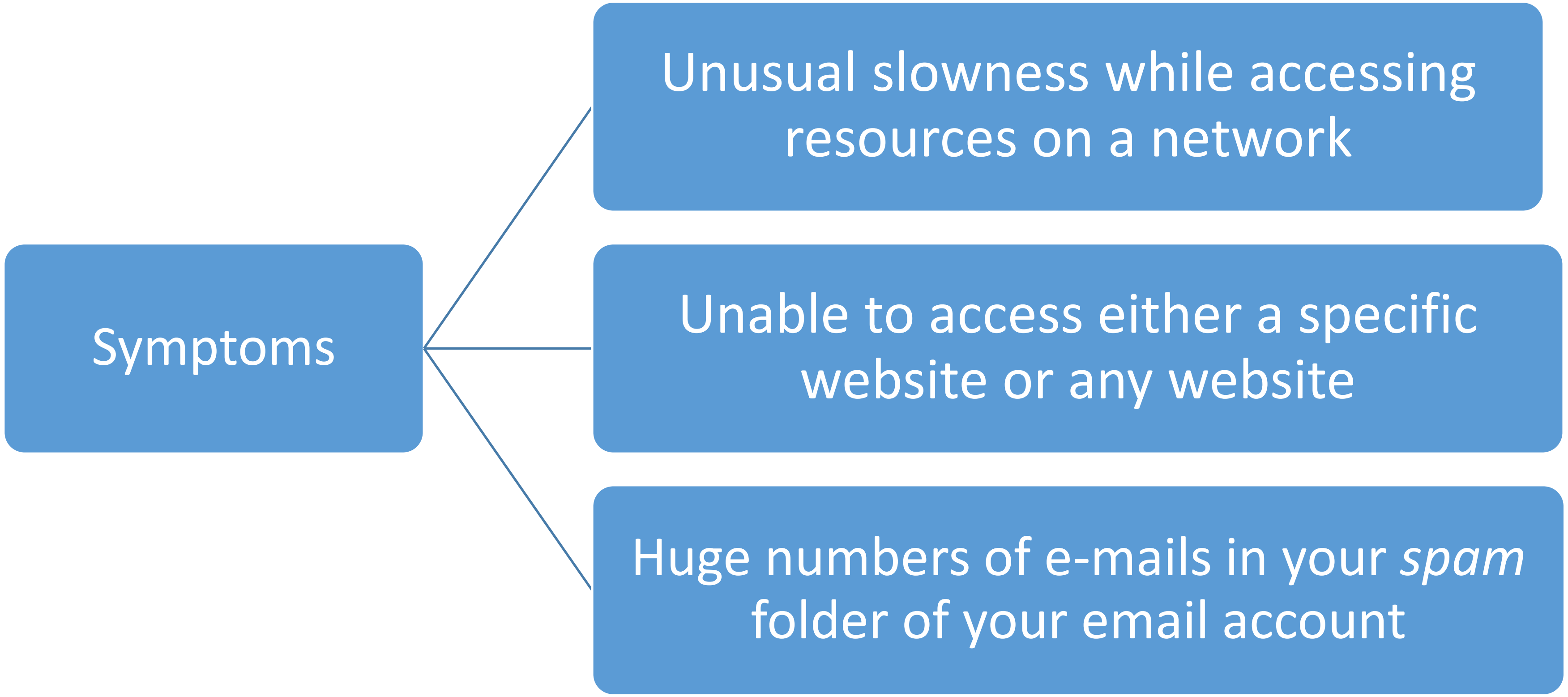
Disturb Connections

- Depriving services between two computers

Limitation for service

- Prevent a person from accessing a service or preventing a service to a system/ person

Symptoms of DoS attacks



Symptoms

Unusual slowness while accessing resources on a network

Unable to access either a specific website or any website

Huge numbers of e-mails in your *spam* folder of your email account

Some DoS attacks

Smuf

- the address is inserted to the target site by the attacker at the source address
- This spoofed packet is sent to broadcast address
- Upon receiving the ICMP Echo requests, all target network will start sending the data
- The target computer will be flooded with these messages

Fraggle

- The method of attack is same as that of Smuf
- Except that it uses Udp echo packets

SYN flood

- Attacker establishes a Connection
- Once acknowledges, marks it into buffer/blockage queue
- Then the message received is not sent by the target

Chargen

- The attacker generates forged UDP packets
- Then chargen port generates set of ASCII characters repeatedly
- high density communication occurs that will consume maximum available bandwidth

Ping flood

- Attacker sends large number of ping (ICMP) packets to the target computer
- If the target starts replying to attacker’s requests causing disruption or suspension in the service

Countermeasures

- Following guidelines while performing network activities
- Implementing security policies at appropriate levels
- Enabling routing filtering
- Disable unused network services
- Restricting bandwidth depending on the usage
- Blocking unwanted IP address
- Having physical security in place
- Maintaining the computers by regularly installing software patches and other security related upgrades
- Implementing protocols that cover the design stage of the information system.

Quiz / Assessment

5) In which of the below DoS attack type, attacker exploits the weakness in UDP, TCP or ICMP?

a) Logic DoS attack	b) Protocol DoS attack	c) Bandwidth consumption	d) compromising physical network components

6) The attacker used *ping- f*commandin _____________ DoS attack in order to flood the target computer with ping packets

a) SYN flood	b) Fraggle	c) Teardrop	d) Ping flood

e-References & External Resources

- *How does ARP Spoofing work? http://www.veracode.com/security/arp-spoofing*
- Read this article from Microsoft's TechNet magazine about 'How to prevent session hijacking?'https://technet.microsoft.com/en-us/magazine/84338f84-9a77-48c7-aeba-75cfa740859f
- *https://www.monkey.org/~dugsong/dsniff/*gives some information about Dsniff
- Read this article on 'Session Hijacking tools in windows' https://www.sans.org/reading-room/whitepapers/windows/session-hijacking-windows-networks-2124
- http://www.sans.edu/research/security-laboratory/article/denial-of-service
- https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html
- The website https://scotthelme.co.uk/advanced-session-hijacking/ contains many useful articles on session hijacking and related topics, with screen shots for clear understanding of the user.

1. The CEH Prep Guide, the comprehensive guide to Certified Ethical Hacking by Ronald L. Krutz and Russell Dean Vines
2. The Basics of Hacking and Penetration Testing, second edition, by PatrickEngebretson
3. Official Certified Ethical Hacker Review Guide by Kimberly Graves
4. Unofficial Guide to Ethical Hacking by Ankit Fadia

Activity

Online Activity
(30min)

Brief description of activity

Description:
Create a power point presentation on ‘Session hijacking using Wireshark’.

Thank You