OSI LAYERS and CyberATTACKS

APPLICATION	EXPLOIT
PRESENTATION	PHISHING
SESSION	HIJACKING
TRANSPORT	RECONNAISSANCE
NETWORK	MITM
DATA LINK	SPOOFING
PHYSICAL	SNIFFING

The concept of OSI LAYERS is the meaningful theorical representation to understand how informations are labeled and processed within an IT network.

On the next slides, let's follow up the most recent cyberattacks on each layer.

APPLICATION LAYER or network process to end users applications and services.
Here information digit are called DATA.

DNS - EMAIL - SMTP - TELNET - HTTP etc.

EXPLOIT ATTACK refers to the malicious code that exploits a weakness of systems to cause accidental conduct or acquire unapproved access.

In example, there are commonly different type of security exploit:

- Denial of Service (DoS) & Remote code execution
- SQL injection & Broken authentication.

PRESENTATION LAYER or data representation, encryption : HTML - MP3 - SOCKET - DOC etc.

There are 5 Most Common type of PHISING ATTACK.

EMAIL PHISHING a fake domain that mimics a genuine organization and sends a thousands of generic requests.

SPEAR PHISING a malicious emails sent to a specific person.

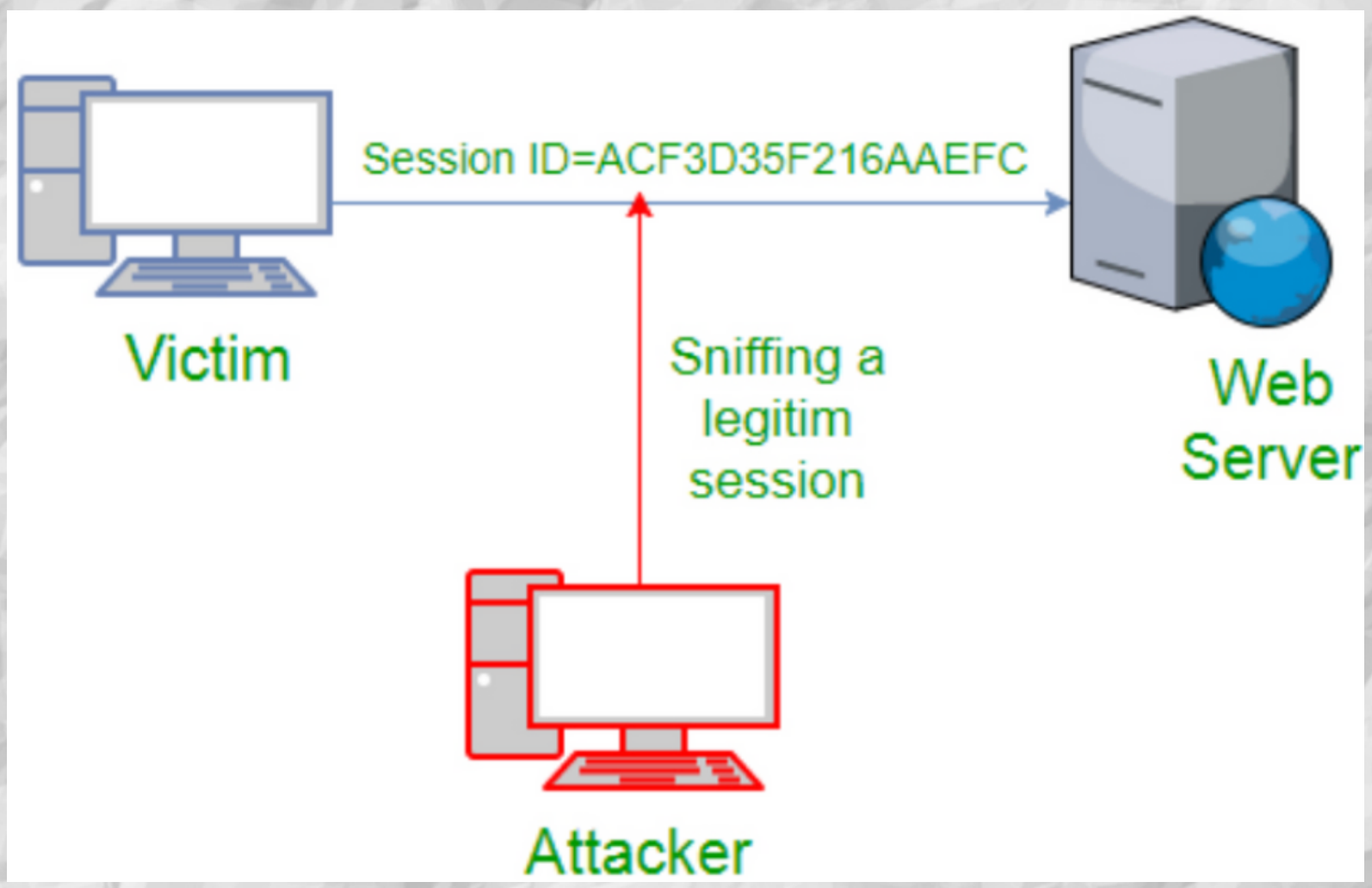
WHALING more targeted taking aim at senior executive.

VISHING the telephones replace emails as the method of communication.

ANGLER PHISING new attack vector is social media

SESSION LAYER or interhost communication RTP - SIP - Session establishment in TCP etc.

Hijacking is a security attack on a user session for a web application.
The most common method of session hijacking is called IP Spoofing.



TRANSPORT LAYER or end to end connections and reliability : TCP - UDP - SSL, TLS etc.

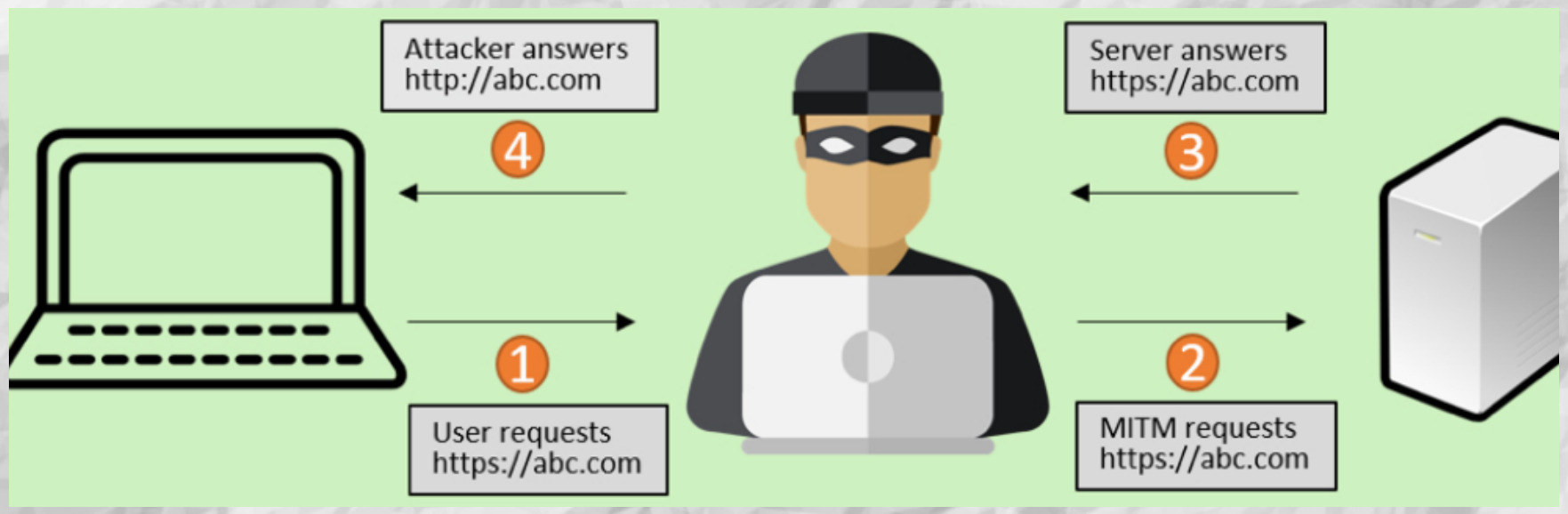
RECONNAISSANCE ATTACK is used by the attacker as a preparation to gather relevant information before launching an actual attack.

There are three types of reconnaissance attacks:

- SOCIAL a social networking site is used to gather informations about the target.
- PUBLIC informations are collected from public domains.
- SOFTWARE a tool is used to gather informations about the target.

NETWORK LAYER : routing and logical addressing occurs here.
IP - OSPF - ARP - ICMP - IPsec etc.

MITM **(Man In The Middle) Attack is a type of cyberattack where attackers intercept an existing conversation or data transfer by pretending to be a legitimate end user.**



DATALINK LAYER :Physical addressing
Ethernet - 802.11 - MAC/LLC - Fiber channels etc.

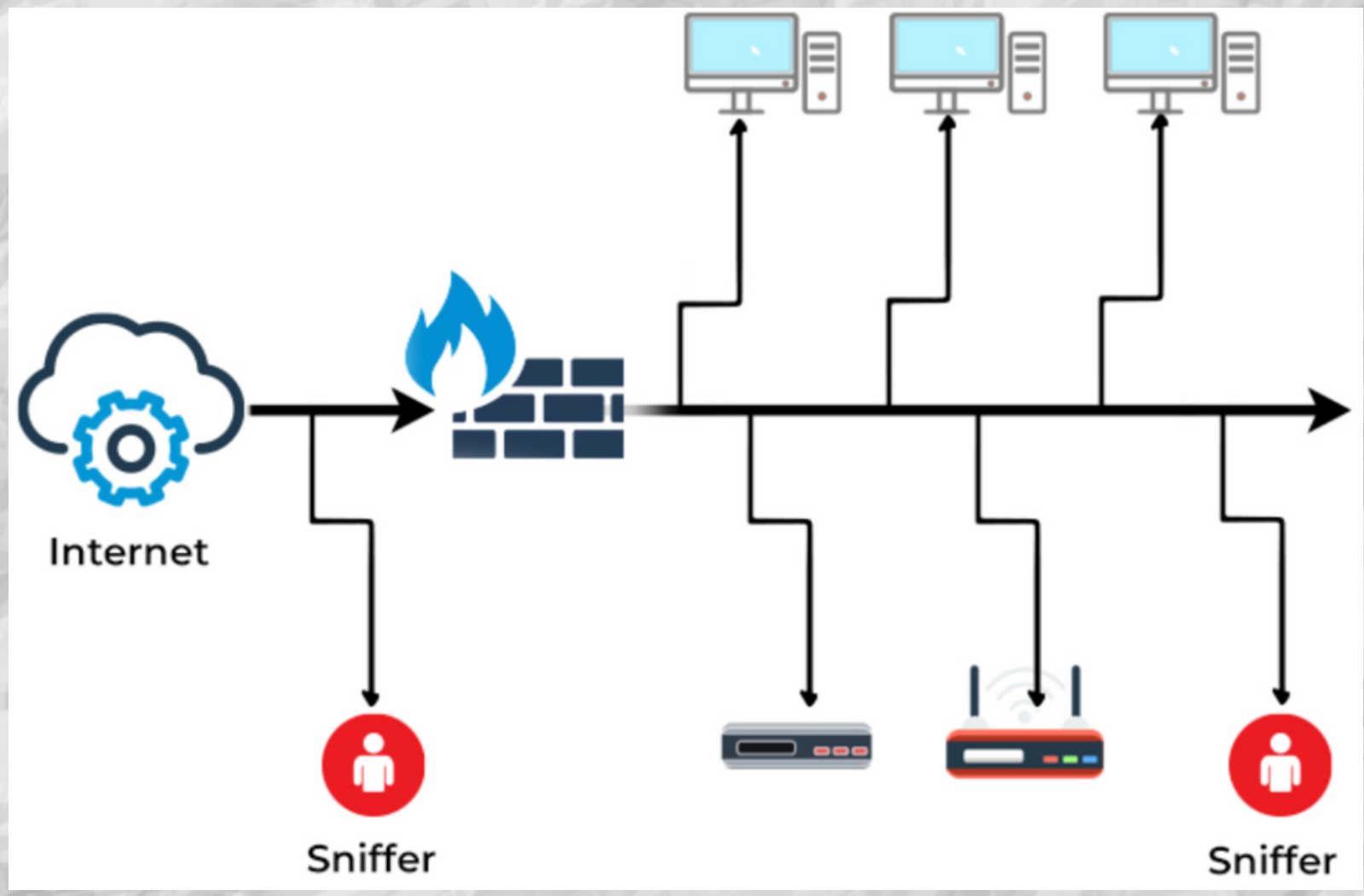
SPOOFING Attack occurs when malicious actors act as trusted human contacts, brands, organization to access systems and infect them with malware, steal data, cause harm and disruption.

The most recurrent spoofing attacks are ***DNS spoofing***, ***email spoofing***, ***IP address spoofing*** etc.

To prevent this kind of attacks, it recommended to always install a malware protection or anti-spam.
Websites with a valid security certificate.
Regularly apply security updates to OS, browsers, network tools, software etc.

PHYSICAL LAYER :Media, signal, and binary transmission intervene in this layer.
Rj45 - DSL - 802.11 - 100BASE-TX etc.

Here is how a packet ***SNIFFING ATTACK*** Works
Hackers capture network packets to intercept or steal data that may be unencrypted
Two types of sniffing : PASSIVE and ACTIVE.



THANKS for READING

IF you find useful,
please share and
leave a comment.

@mbaindiguimedgar