CYBER SECURITY

Networking

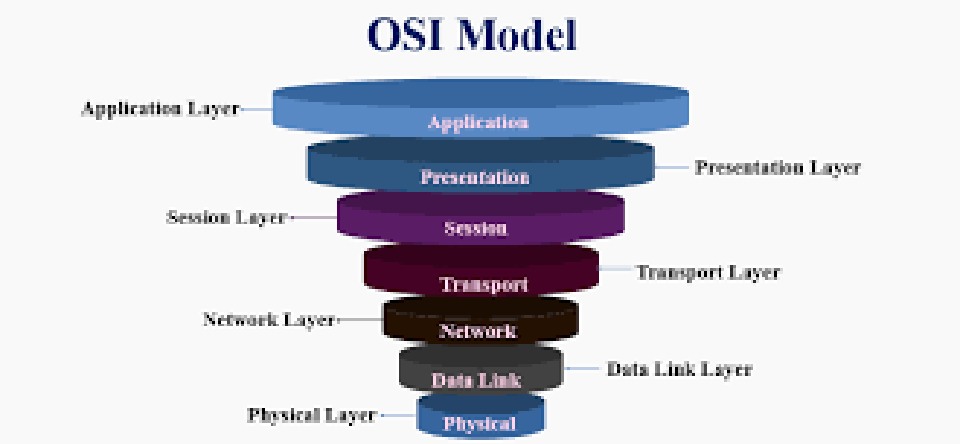
1. Introduction

Cyber Crime
Just like regular crime, it also exists on the Internet. some examples of Cyber Crime:

- Identity Theft
- Online Predators
- BEC ("Business Email Compromise")
- Ransomware
- Stealing of sensitive intellectual property

Cyber crime activities have increased regulary, and cacthing these criminals is a very hard challenge as the internet facilitate the crimes making possible to laundring money, hide identity, targeting thousands of victims and so on.
To be able to understand common cyber attacks and some of the defend operations we need to have a clear understanding of networking principles.

Networking basics – The OSI model
The OSI ("Open Systems Interconnection") model represents an easy and intuitive way to standardize the different parts required to communicate across networks. The model makes it clear what is required to communicate on a network by splitting the requirements into multiple layers.
This is what the OSI model looks like:



source: google.com/osimodel

The first 3 layers: **Application**, **Presentation** and **Session** are implemented in software whitin the Operating System
The bottom 3 layers: **Network**, **Data link** and **Phisycal** are implemented in hardwares whitin devices on the network.

Layer 7 – Application
This is what the users use to interact with services across a network. Most developers create applications on the Application Layer.
Exemples of application layer are: **HTTP**, **FTP** and **SNMP**.

Layer 6 – Presentation
Typically an unseen layer, but is responsible of adapting, transforming and translating data. This is to ensure the application and layers beneath can understand one another.
Exemples of Presentation are: Encoding Schemes used to represent text and data, for example **ASCII**, Encryption for services, for example **SSL** ("Secure Sockets Layer") and **TLS** ("Transport Security Layer"), Compression.

Layer 5 – Session
This layer's responsibility is handling connections between the application and the layers below. It involves establishing, maintaining and terminating connections, otherwise referred to as sessions.
Common protocols which represent the Session Layer well are: **SOCKS** - A protocol for sending packets through a proxy server, **NetBIOS** - An older Windows protocol for establishing sessions and resolving names and **SIP** ("Session Initiation Protocol") - For engaging in VOIP ("Voice Over IP") communications

Layer 4 – Transport
The protocols of this layer provide end-to-end communication services for applications **.**
Some well known applications of this layer are the protocols: **TCP, UDP** and **QUIC**.

Layer 3 – Network
A layer responsible of routing packets between networks via routers.
On this layers reside the protocols: **IPV4**, **IPV6, ICMP** and **IPSEc**.

Layer 2 – Data Link
The Link Layer is responsible for moving data from physical over to logical (to the network layer).
Protocols on this level include: **Ethernet** when connecting the network with a physical cable, **Wi-Fi** for accessing the internet using radio signals and **NDP**.

Layer 1 – Physical

Physical layer represents the signaling which allows bits and bytes to transfer between a physical medium. It can be transferred via radio or signals over a cable, using electrical signals or light, for example fiber.

2. In Depth - Network Layer

The Internet protocol
IP is used to communicate across networks. The addressing scheme in use is either IPv4 or IPv6.
IP networks can be broken into different sections, often called subnets. This is accomplished by adding an extra piece of information, called a *netmask*. The netmask dictates how large a network is and which packet is routed within the network and which should be routed outside of the network.
Each network has a reserved address for broadcasting traffic to every host in the network, this is called the **broadcast address** .

Routers and Switches
In IP networks the traffic is routed by a router. A router is a networking device which understands the IP format and can forward packets between networks. The switch forwards data within a network, while the router forwards between networks.

Headers
Packets on the network has headers which describe many of the important details we already discussed within the IP protocol. Headers are simply pieces of informations attached to the packets. Exemples of headers are: **source, destination, lenght, protocol** and so on..

Nat – Network address translation
Nat is usually implemented in routers and it's a system which alloww to translate a set of Ip addresses to another set of Ip addresses. Nat is responsable for translating private Ip addresses to public Ip addresses. Another implentation is when we have a front Ip address fro multiple internal Ip addresses and the destination port number is used to decide which server the data should be sent to.

ICMP
ICMP is often associated with Ping and Traceroute but it is also used for other things such as **ICMP Timestamp request**.
Tracerouting is a way to determine which routers are involved in sending a packet from system A to B.

DNS – *Domain name system*

The **DNS** resolves *domain names* to *IP addresses.* Computers identifies theirself using numbers. As it would be impossible to remember Ip addresses humans can use **domain name** isntead. When we want to communicate with a Web page instead of typing the Ip address we can simply input the domain name.
If the Ip address is not stored in our compure's cache, it'll send a request to the **Resolver DNS sever**, which is basically our **ISP**.
If the resolver hasn't got stored the IP address for that domain name it will send a request to the **Root Server.** The root server is the top of the Dns Hierarchy (there are 13 root server in the world.
The root server will redirect the *resolver server* to the **TLD Server,** which store informations for **Top level Domain** (.com, .net, .org etc..).
Finally, the TLD Server will redirect the Resolver to the **Authorative Server**, which knows everything about that domain. The answer is sent back to the Resolver which now stores the information in its own cache.

DHCP – Dynamic Host Configuration protocols
The DHCP protocol allows any system on a network to reach out to a server and receive a configuration. Such configuration typically implies receiving IP address and network range, default gateway and DNS servers.

VPN – Virtual Private Network
A VPN is a system which enables two system to establish encrypted forms for communication, enabling network traffic to be encrypted in transit. Some VPN services are designed for user privacy and encryption for data in transit. These services enables users to send network data via the VPN, effectively masquerading the users IP address when navigating the Internet.

3. In Depth - Transport and Data Link

The transport layer allows end to end communication between applications. When data is sent between devices, it follows one of two different protocols.

TCP – Transmission Control Protocol
The TCP protocol allows reliable and guarantee communications. It is a connection oriented protocol which means that it must first aknowledge a session between the two computers that are communicating.

3-Ways-Handshake
The two computers verify a connection before starting the communication. The first computer will send a **SYN** packet. The receiver will reply with a **SYN/AKN** packet and finally the first computer send a final **AKN** packet.

Spoofing
Anyone can create packets with any of the fields of the headers set to whatever value they desire. This is called spoofing, allowing attackers to send traffic on

behalf of others.
TCP has security built into the protocol, but it relies on the strength of the PRNG ("Pseudo Random Number Generator") number generators. If the Sequence numbers of the communicating parties can be guessed, the security of TCP can be compromised in the sense that an attacker can engage in spoofed communications via TCP.

UDP – User Datagram Protocol
UDP is used for traffic which does not need the resilience and security of TCP. Looking at the UDP Header we can see the same Source and Destination ports in use, but no Sequence numbers or Control bits. The protocol has much less overhead, leading to faster transmission of data. ecause UDP does not have features such as the 3-Way-Handshake, UDP can be easily spoofed.

ARP – Address Resolution Protocol
ARP ("Address Resolution Protocol") is the protocol which allows computer systems to know which MAC address belongs to which IP address. If the traffic has to be routed, the computer system will forward traffic to the Default Gateway configured on the system. ARP, like DNS, is a protocol which resolves one address into another. Every time a system tries to communicate to an IP address which is on the LAN it will check its ARP cache to see if has recently been resolved.

4. Firewalls

Firewalls are a central architectural element to any network. They are designed to keep out all network traffic, except traffic which we allow. Firewalls operate on **Layer 4**, typically **controlling TCP** and **UDP access** to internal assets. Next-Generation Firewalls operate on all the layers of the OSI model, including Layer 7 **.**

NGFW – Next generation Firewalls
A modern Firewall has capabilities that range much wider than a a Layer 4 Firewall. These capabilities are typically security features:

- ***Segmentation****:* Firewalls can segment traffic between hosts and systems into segments, sometimes called zones. Each segment holds services which are allowed to communicate between one another.
- ***IPS*** (Intrusion Prevention System) and ***IDS:*** *IPS and IDS systems have signatures, algorithms and heuristics to detect attacks on the network or host. An IDS or IPS deployed on a host is called a HIDS ("Host Intrusion Detection System").*
- ***Content and Application*** *Filtering:* The Firewall can make attempts in understanding which applications and content is traversing the network.

- ***Sandboxing***: In this context, sandboxing means to have a platform execute files, which are may be malicious. The sandbox records and monitors the activity of the file to see if it is malicious or not

Resoucers

1. W3 School
https://www.w3schools.com/cybersecurity/index.php
2. Cyber Security learning platform
https://tryhackme.com/paths
3. Wikipedia
https://en.wikipedia.org/wiki/OSI_model#:~:text=The%20Open%20Systems%20Interconnection%20model,underlying%20internal%20structure%20and%20technology.