**Network Security**

## **Types of Networks**

*LAN (Local Area Network)*- A small local network

*VLAN (Virtual Local Area Network)*- A virtual LAN

*WAN (Wide Area Network)* - Provides long-distance connections with multiple LANs

## **Devices**

|  |  |
| --- | --- |
| **Device** | **Summary** |
| Hub | Simple network device that receives data from one device and transmits it to all other devices |
| Switch | Device that connects multiple network devices and forwards data only to the intended destination |
| Router | Device that connects different networks, forwarding data between them |
| Firewall | Monitors and controls network traffic to protect against threats |
| Server | Provide services to other devices on the network |
| Endpoint | Final device in a network, such as a laptop or smartphone, that communicates with other devices |

About ingress and egress monitoring traffic, we have some keywords.

Inbound traffic / ingress monitoring: Firewalls, Gateways, Remote authentication Servers, IDS/IPS tools, SIEM solutions, Anti-malware solutions.

Outbound traffic / egress monitoring: Data Loss Prevention (DLP) solutions or Data Leak Protection

# **OSI model & TCP/IP model**

Here we have a example of network models

|  |  |  |
| --- | --- | --- |
| **OSI Model** | **TCP/IP Model** | **Packets** |
| 7 - Application | 4 - Application | HTTP, FTP, SMTP, DNS |
| 6 - Presentation |  | JPEG, MPEG |
| 5 - Session |  | NFS, SQL, PAP |

|  |  |  |
| --- | --- | --- |
| **OSI Model** | **TCP/IP Model** | **Packets** |
| 4 - Transport | 3 - Transport | TCP, UDP |
| 3 - Network | 2 - Internet | IPv4, IPv6 |
| 2 - Data Link | 1 - Network Access | IP, ICMP, ARP |
| 1 - Physical |  | Ethernet, Wi-Fi |

A short summary of each layer

|  |  |
| --- | --- |
| **Layer** | **Provides** |
| Application | Provides network services to end-users, such as email, web browsing, and file transfer |
| Presentation | Translates data received from the application layer into a common format that can be understood by the network, and performs functions such as data encryption and compression |
| Session | Responsible for establishing, managing, and terminating communication connections between two devices on the network |
| Transport | Ensures reliable delivery of data between the end devices, segmenting information into smaller packets and providing flow control and error correction |
| Network | Responsible for routing packets in the network, selecting the most efficient path between end devices and ensuring packets arrive at the correct destination |
| Data Link | Responsible for ensuring the transfer of data between two directly connected devices over a physical medium, such as a network cable or wireless network |
| Physical | Responsible for the transmission of raw bits from one device to another over a physical medium, such as fiber optic or copper cable |

# **Insecure Ports || Secure Ports**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Insecure port** | **Protocol name** | **Description** | **Secure alternative port** | **Protocol name** |
| 21 FTP | File Transfer Protocol (FTP) | Does not encrypt data during transfer, making it vulnerable to sniffing and interception attacks. | 22 SFTP (SSH  File Transfer Protocol) | Secure File Transfer Protocol |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Insecure port** | **Protocol name** | **Description** | **Secure alternative port** | **Protocol name** |
| 23  TELNET | Telnet | Does not encrypt data, including passwords, allowing interception of information. | 22 SSH  (Secure Shell) | Secure Shell Protocol |
| 25 SMTP | Simple Mail Transfer Protocol (SMTP) | Does not encrypt emails in transit, allowing them to be read by third parties. | 587 SMTPS (SMTP  Secure) | SMTP with TLS |
| 37 TIME | Time Protocol | Unexpected errors | 123 - NTP | Network Time Protocol |
| 53 DNS | Domain Name System (DNS) | Does not encrypt DNS queries and responses, allowing interception and manipulation of information. | 853 DNS  over TLS (DoT) | Domain Name System |
| 80 HTTP | Hypertext Transfer Protocol (HTTP) | Information sent via HTTP is not encrypted and is susceptible to sniffing attacks | 443 HTTPS (HTTP  Secure) | Secure Hypertext Transfer Protocol |
| 143  IMAP | Internet Message Access Protocol (IMAP) | Does not encrypt emails in transit, allowing them to be read by third parties. | 993 IMAPS (IMAP  Secure) | IMAP for SSL/TLS |
| 161/162  - SNMP | Simple Network Management Protocol (SNMP) | Does not encrypt transmitted information, including SNMP community passwords, allowing them to be read by third parties. | 161/162  SNMP over TLS | SNMPv3 |
| 445 SMB | Server Message Block (SMB) | Does not encrypt SMB traffic, allowing interception of information. | 2049 NFS | Network File System |
| 389  LDAP | Lightweight Directory Access | Does not encrypt transmitted information, | 636 LDAPS (LDAP | Secure Lightweight |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Insecure port** | **Protocol name** | **Description** | **Secure alternative port** | **Protocol name** |
|  | Protocol (LDAP) | including credentials, allowing them to be read by third parties. | Secure) | Directory Access Protocol |

**How it works: SYN, SYN-ACK, ACK Handshake**

1. TCP Client sends a synchronization (SYN) packet to the web server’s port 80 or 443. This is a request to establish a connection.
2. The web server replies to the SYN packet with an acknowledgement known as a SYN/ACK. 3-Finally, the client acknowledges the connection with an acknowledgement (ACK).

# **Network Infrastructure**

## **Concepts about Data Centers**

|  |  |
| --- | --- |
| **Data Centers** | **Description** |
| Heating, Ventilation and Air Conditioning (HVAC) /  Environmental | The HVAC system is responsible for maintaining the proper temperature, humidity, and air quality in a data center to ensure that servers and other equipment operate reliably. The environmental controls include monitoring and regulating temperature, humidity, and air quality to prevent damage to equipment. |
| Data Center/Closets | A data center is a centralized facility used to store, manage, and disseminate data and information. It typically contains redundant power supplies, backup generators, and backup systems to ensure data availability and continuity in the event of a power outage or other disruption. A data closet is a small room or enclosed space used to house networking and telecommunications equipment. |

**Cloud**

NIST resolution: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

## **Cloud service models**

|  |  |  |
| --- | --- | --- |
| **Service Model** | **Definition** | **Example** |
| SaaS (Software as a Service) | Software provided as a service over the internet. | Imagine you need to create a presentation for a client but you don't have the PowerPoint software installed on your computer. With SaaS, you can access the PowerPoint software over the internet, create your presentation, and save it to the cloud without installing  the software locally on your computer. This is an example of SaaS. |
| PaaS (Platform as a Service) | Platform provided as a | Imagine you want to build a house but you don't want to worry about building the foundation and walls. With PaaS, you can use a construction platform that provides |

|  |  |  |
| --- | --- | --- |
| **Service Model** | **Definition** | **Example** |
|  | service over the internet. | the basic infrastructure, such as the foundation, walls, and roof, and you can build the house on top of this platform, adding the finishes and customizations you want. This is an example of PaaS. |
| IaaS (Infrastructure as a Service) | IT infrastructure provided as a service over the internet. | Imagine you want to create a garden in your backyard but you don't have the tools or materials you need, such as soil, plants, shovels, and watering cans. With IaaS, you can rent the necessary tools and materials to create the garden without having to buy or maintain them after the garden is finished. The service provider provides the  basic infrastructure, such as gardening tools and soil, and you are responsible for taking care of the garden. This is an example of IaaS. |

**Deployment Models**

|  |  |  |
| --- | --- | --- |
| **Model** | **Description** | **Examples** |
| Private Cloud | Cloud infrastructure dedicated to a single organization, managed by the organization or a third-party vendor, offers complete control over data and applications | A private island that is owned by a single person or organization. The owner has complete control over who can access the island and what activities can be performed on it. |
| Public Cloud | Cloud infrastructure shared among multiple users over the internet, owned and managed by a third-party provider, offers cost-effective and scalable solution for businesses of all sizes | A public park that is open to anyone. People can come and go  as they please, and use the park for a variety of activities such as picnics, sports, and events. |
| Community Cloud | Cloud infrastructure shared among several organizations with similar requirements, owned and managed by one of the participating organizations or a third- party provider, allows organizations to share resources and reduce costs while maintaining a higher level of control over their data and applications | A co-op or community garden where several individuals or organizations share resources to grow and maintain a garden. The members work together to maintain the garden and share the benefits of the harvest. |
| Hybrid Cloud | Cloud infrastructure that combines two or more deployment models, such as private | A house with both a private backyard and a public front yard. |

|  |  |  |
| --- | --- | --- |
| **Model** | **Description** | **Examples** |
|  | and public clouds, to meet specific business requirements, provides greater flexibility and scalability compared to a single deployment model | The owner has complete control over the private backyard, but can also use the public front yard for activities such as hosting a garage sale or having a BBQ with neighbors. |

**Some fundamental Terminologies**

|  |  |
| --- | --- |
| **Terminology** | **Definition** |
| Managed Service Provider (MSP) | A company that remotely manages a customer's IT infrastructure and end- user systems, providing services such as monitoring, patch management, and help desk support. MSPs operate under a subscription model and can help businesses reduce IT costs and improve system performance. |
| Service-Level Agreement (SLA) | A contract between a service provider and a customer that defines the level of service expected, including metrics such as uptime, response time, and resolution time. SLAs help establish accountability and ensure that service providers meet the customer's expectations. |
| Network Segmentation | The process of dividing a network into smaller, isolated segments, each with its own security controls and policies. Network segmentation helps reduce the attack surface and contain the impact of security incidents. |
| Demilitarized Zone (DMZ) | A network segment that sits between an internal network and an external network, typically the internet. The DMZ contains servers that provide services to external users, such as email, web, and FTP. The DMZ is heavily secured and is designed to prevent external threats from reaching the internal network. |
| Virtual Local Area Network (VLAN) | A logical network segment that allows devices to communicate as if they were on the same physical network, even if they are located on different switches or subnets. VLANs help improve network performance, simplify network management, and enhance security by isolating traffic. |
| Virtual Private Network (VPN) | A secure and encrypted connection that allows remote users to access a private network over the internet. VPNs provide secure remote access to corporate resources and allow users to bypass geographic restrictions. |
| Defense in Depth | A security strategy that employs multiple layers of defense to protect against threats. Defense in depth includes a combination of technical and procedural controls, such as firewalls, intrusion detection systems, access controls, and employee training. |

|  |  |
| --- | --- |
| **Terminology** | **Definition** |
| Network Access Control (NAC) | A security solution that controls access to a network based on user identity and device status. NAC solutions enforce policies that ensure only authorized users and devices can access the network, and that these devices meet certain security requirements. |

**Threats & Attacks**

**Types of Threats**

|  |  |
| --- | --- |
| **Vulnerability** | **Summary** |
| Spoofing | An attack where a malicious actor disguises their identity to gain unauthorized access to a network or system. This can include IP spoofing, ARP spoofing, and email spoofing. |
| Phishing | An attack where a malicious actor sends a fraudulent message, often through email or social media, with the goal of tricking the recipient into giving up sensitive information or installing malware. |
| DOS/DDOS | Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks involve overwhelming a server or network with traffic, making it unable to handle legitimate requests. |
| Virus | A type of malware that infects a system. Viruses can damage or destroy data, and can spread to other systems through infected files. |
| Worm | Similar to a virus, a worm is a self-replicating malware that can spread across a network without the need for a host file or program. |
| Trojan | A type of malware that disguises itself as a legitimate program in order to trick users into installing it. Trojans can be used to steal data, install additional malware, or take control of a system. |
| On-path attack | An attack where a malicious actor intercepts and modifies network traffic between two systems. This can include Man-in-the-Middle (MitM) attacks or Session Hijacking. |
| Side-channel | An attack where a malicious actor exploits weaknesses in a system's physical properties, such as power consumption or electromagnetic radiation, to extract sensitive information. |
| Advanced Persistent Threat (APT) | A targeted attack where a malicious actor gains persistent access to a network or system, often through spear-phishing or other social engineering tactics. APTs can be used for espionage, data theft, or sabotage. |
| Insider | An attack where a trusted individual with access to a system or network abuses that access for personal gain or to cause harm. |

|  |  |
| --- | --- |
| **Vulnerability** | **Summary** |
| Malware | A broad term for any type of malicious software, including viruses, worms, trojans, and other types of malicious code. |
| Ransomware | A type of malware that encrypts a user's files and demands payment in exchange for the decryption key. Ransomware can be distributed through email, malicious websites, or other means. |

**Tools used to identify and prevent threats**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Description** | **Identifies Threats** | **Prevents Threats** |
| IDS (Intrusion Detection System) | Real-time intrusion detection system that monitors and analyzes network traffic for suspicious activity. | ✔ |  |
| HIDS (Host-based Intrusion Detection System) | Host-based intrusion detection system that monitors activity on a specific operating system for suspicious activity. | ✔ |  |
| NIDS (Network-based Intrusion Detection System) | Network-based intrusion detection system that monitors network traffic for suspicious activity. | ✔ |  |
| SIEM (Security Information and Event Management) | Security information and event management system that collects and analyzes information from various sources to identify security threats. | ✔ |  |
| Anti-malware/Antivirus | Software tool designed to detect, prevent, and remove malicious software such as viruses, worms, and trojans. | ✔ | ✔ |
| Scans | Software tool that scans and analyzes a system for security vulnerabilities. | ✔ |  |
| Firewalls | Security system that monitors and controls network traffic based on a | ✔ | ✔ |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Description** | **Identifies Threats** | **Prevents Threats** |
|  | set of predefined rules. |  |  |
| IPS/NIPS/HIPS (Intrusion Prevention System/Network- based IPS/Host-based IPS) | Intrusion prevention system that identifies and blocks malicious activity in real-time. | ✔ | ✔ |

**Anki Cards**

|  |  |
| --- | --- |
| **Description** | **Terminology** |
| A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or web tool. | API |
| The most essential representation of data (zero or one) at Layer 1 of the Open Systems Interconnection (OSI) model. | Bit |
| transmission is a one-to-many (one-to-everyone) form of sending internet traffic. | Broadcast |
| is a unit of digital information that most commonly consists of eight bits. | Byte |
| A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. | Cloud Computing |
| A system in which the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and  operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. | Community Cloud |
| The opposite process of encapsulation, in which bundles of data are unpacked or revealed | De-encapsulation |
| The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) | Denial Of Service |
| This acronym can be applied to three interrelated elements: a service, a physical server and a network protocol. | DNS |
| Enforcement of data hiding and code hiding during all phases of software development and operational use. Bundling together data and methods is the process of encapsulation; its opposite process may be called unpacking, revealing, or using other terms. Also used to refer to taking any set of data and packaging it or hiding it in | Encapsulation |

|  |  |
| --- | --- |
| **Description** | **Terminology** |
| another data structure, as is common in network protocols and encryption. |  |
| The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings | Encryption |
| The internet protocol (and program) used to transfer files between hosts. | FTP |
| An attacker fragments traffic in such a way that a system is unable to put data packets back together. | fragment attack |
| The physical parts of a computer and related devices. | Hardware |
| A combination of public cloud storage and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider. | Hybrid Cloud |
| The provider of the core computing, storage and network hardware and software that is the foundation upon which organizations can build and then deploy applications | IaaS |
| An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available. | ICMP |
| Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. | IPV4 |
| An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them. | Man-in-the-middle |
| Part of a zero-trust strategy that breaks LANs into very small, highly localized zones using firewalls or similar technologies. At the limit, this places firewall at every connection point. | Microsegmentation |
| Purposely sending a network packet that is larger than expected or larger than can be handled by the receiving system, causing the receiving system to fail unexpectedly. | Oversized Packt Attack |
| The primary action of a malicious code attack. | Payload |

|  |  |
| --- | --- |
| **Description** | **Terminology** |
| An information security standard administered by the Payment Card Industry Security Standards Council that applies to merchants and service providers who process credit or debit card transactions. | PCI DSS |
| The web-authoring or application development middleware environment that allows applications to be built in the cloud before they're deployed as SaaS assets. | PaaS |
| The phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of cloud systems, but removes a number of objections  to the cloud computing model, including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance. | private cloud |
| A set of rules (formats and procedures) to implement and control some type of association (that is, communication) between systems. | Protocols |
| Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model. | Packet |
| The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. | Public Cloud |
| The standard communication protocol for sending and receiving emails between senders and receivers. | SMTP |
| Computer programs and associated data that may be dynamically written or modified during execution. | Software |
| The cloud customer uses the cloud provider's applications running within a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. | SaaS |
| Faking the sending address of a transmission to gain illegal entry into a secure system. | Spoofing |
| Internetworking protocol model created by the IETF, which specifies four layers of functionality: Link layer (physical communications), Internet Layer (network-to-network communication), Transport Layer (basic channels for connections and connectionless exchange of data | Transport Control Protocol/Internet Protocol (TCP/IP) Model |

|  |  |
| --- | --- |
| **Description** | **Terminology** |
| between hosts), and Application Layer, where other protocols and user applications programs make use of network services. |  |
| A virtual local area network (VLAN) is a logical group of workstations, servers, and network devices that appear to be on the same LAN despite their geographical distribution | VLAN |
| A virtual private network (VPN), built on top of existing networks, that can provide a secure communications mechanism for transmission between networks. | VPN |
| A wireless area network (WLAN) is a group of computers and devices that are located in the same vicinity, forming a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN. | WLAN |
| The graphical user interface (GUI) for the Nmap Security Scanner, an open-source application that scans networks to determine everything that is connected as well as other information. | Zenmap |
| Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Microsegmentation of workloads is a tool of the model. | Zero Trust |