# INTRODUCTION

Networking facilitates communication between computers through various topologies, mediums, and protocols. Security professionals should understand networking to detect failures and implement defense layers. Subdividing networks and controlling activities enhance security. Misconfigurations and oversight can compromise network security.

# NETWORKING STRUCTURE

### Network Types

In networking, various types and topologies exist to categorize networks based on their structure. Common terms include Wide Area Network (WAN), Local Area Network (LAN), Wireless Local Area Network (WLAN), and Virtual Private Network (VPN). WAN refers to the internet and encompasses interconnected LANs. LAN and WLAN assign IP addresses for local use, with WLAN providing wireless transmission. VPNs have three main types: Site-to-Site VPN connects multiple networks, Remote Access VPN creates a virtual interface for clients, and SSL VPN operates within web browsers.

### Networking Topologies

In network topology, devices are arranged and connected physically or logically. This includes hosts like computers, switches, bridges, and routers that facilitate connections. The physical topology refers to the layout of transmission media, while the logical topology describes how data is transmitted. Network topologies can be divided into three areas: connections (wired and wireless), nodes (network interface controllers), and classifications (physical or logical). The eight basic types of network topologies are point-to-point, bus, star, ring, mesh, tree, hybrid, and daisy chain. Each has its own characteristics and suitability for different network setups.

### Proxies

A proxy is a device or service that acts as a mediator between two connections, inspecting the contents of the traffic. It is distinct from a gateway, as it operates as a mediator and can inspect traffic. There are different types of proxy services, including dedicated proxies or forward proxies, reverse proxies, and transparent proxies. Forward proxies handle client requests, such as accessing websites through a corporate network. Reverse proxies filter incoming requests, often used for security purposes like DDOS protection or web application firewalls. Proxy services can operate at Layer 7 of the OSI Model and can be transparent or non-transparent depending on whether the client is aware of their existence.

# NETWORKING WORKFLOW

### Networking Models

OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are two networking models that describe the communication and transfer of data between hosts. The OSI model, published by the ITU and ISO, consists of seven layers with clearly defined tasks. It serves as a reference model for system communication. On the other hand, TCP/IP is a generic term for a protocol family that includes various network protocols responsible for data packet switching and transport on the Internet. While TCP/IP is the protocol used for connecting hosts to the Internet, OSI acts as a communication gateway between networks and end-users. The OSI model is often referred to as the reference model and is known for its strict protocols and limitations. TCP/IP, on the other hand, allows for some flexibility as long as general guidelines are followed.

### OSI Model

The ISO/OSI model is a reference model that enables communication between different systems. It consists of seven hierarchical layers, each with specific tasks. The layers include the physical layer for transmission, data link for reliable transmission, network for connections and packet forwarding, transport for end-to-end control, session for maintaining logical connections, presentation for data transformation, and application for input/output and application functions. Both sender and receiver go through all layers when communicating. The model ensures secure, reliable, and efficient communication.

### TCP/IP Model

The TCP/IP model, also known as the Internet Protocol Suite, is a layered reference model consisting of four layers: the Application Layer, Transport Layer, Internet Layer, and Link Layer. Each layer has specific functions in facilitating data exchange and communication. TCP/IP allows applications to access network services, provides session and datagram services, handles logical addressing and routing through IP, ensures error control and flow, supports application-specific ports, and enables name resolution through DNS. TCP/IP differs from the OSI model by combining certain layers and offering flexibility for data transfer across different networks.

# ADDRESSING,

### NETWORK LAYER

The network layer (Layer 3) in the OSI model is responsible for controlling the exchange of data packets by providing routing and data flow control. It handles logical addressing, routing, and the establishment and termination of connection channels. The network layer identifies network nodes, routes data packets from node to node based on addresses, and constructs routing tables. Protocols at this layer, such as IPv4, IPv6, IPsec, ICMP, IGMP, RIP, and OSPF, facilitate packet routing and ensure the transmission of data across different subnets with incompatible addressing schemes. The network layer plays a crucial role in forwarding packets to their destinations and enabling communication within and between networks.

### IPV4

The Media Access Control (MAC) address is used for local network communication, while the Internet relies on IPv4 and IPv6 addresses. IPv4 addresses are 32-bit numbers divided into four octets, represented in decimal form, and consist of a network and host part. Subnetting allows for further division of IP addresses into smaller networks using subnet masks. The subnet mask determines the network and host portions of an IP address. CIDR notation replaces the traditional class-based addressing and represents the subnet mask by indicating the number of 1-bits in the mask. Understanding these address types and structures is essential for establishing accurate communication within networks and across the Internet.

### SUBNETTING

Subnetting is the process of dividing an address range of IPv4 addresses into smaller subnets. A subnet represents a logical segment of a network with IP addresses sharing the same network address. Subnetting allows for creating specific subnets and determining important details such as network address, broadcast address, first and last host addresses, and the number of available hosts. By using subnet masks, the network and host parts of an IP address can be separated, enabling routing between different subnets. Subnetting also allows for further division of subnets into smaller networks based on binary calculations. Understanding the concept of subnetting involves recognizing octets where IP addresses can change, determining subnet sizes using modulo operations, and calculating IP address ranges for each subnet based on network and broadcast addresses.

QUESTIONS

Submit the decimal representation of the subnet mask from the following CIDR: 10.200.20.0/27

255.255.255.224

Submit the broadcast address of the following CIDR: 10.200.20.0/27

10.200.20.31

Split the network 10.200.20.0/27 into 4 subnets and submit the network address of the 3rd subnet as the answer.

10.200.20.16

Split the network 10.200.20.0/27 into 4 subnets and submit the broadcast address of the 2nd subnet as the answer.

### MAC

MAC addresses are unique identifiers assigned to network interfaces and are used to address data packets on layer 2 of the network protocol stack. They consist of 6 bytes, with the first half representing the manufacturer's identifier and the second half being the individual address. MAC addresses can be represented in hexadecimal or binary format. Address Resolution Protocol (ARP) is used to map IP addresses to MAC addresses, facilitating communication on local networks. However, MAC addresses can be manipulated or spoofed, posing security risks. Attack vectors include MAC spoofing, MAC flooding, and ARP spoofing. Implementing additional security measures and protocols is essential to protect against these threats.

### IPV6

IPv6 is the successor to IPv4 and offers a 128-bit address space, compared to the 32-bit address space of IPv4. The Internet Assigned Numbers Authority (IANA) is responsible for assigning IPv6 addresses. IPv6 addresses can coexist with IPv4 through Dual Stack, allowing both protocols to be used simultaneously. IPv6 eliminates the need for NAT and provides publicly accessible IP addresses to devices. It has numerous advantages over IPv4, including larger address space, address self-configuration, multiple addresses per interface, faster routing, end-to-end encryption, and support for larger data packages. IPv6 addresses are represented in hexadecimal notation, and they consist of a network prefix and an interface identifier.

# PROTOCOLS & TERMINOLOGY,

### Networking Key Terminology

The field of information technology encompasses a vast array of terms and concepts, and while it is impossible to cover them all, understanding the essential ones is crucial. The breadth of information technology is comparable to the medical sector, with numerous programming languages, protocols, functions, and potential errors. Specializing in one or two areas is common due to the vastness of the subject. To establish a foundational understanding, a list of commonly used protocols has been compiled, including Wired Equivalent Privacy (WEP), Secure Shell (SSH), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and many more. However, this list is incomplete, and further exploration of protocols will be undertaken in subsequent modules. Familiarity with these protocols will be beneficial, and continual expansion of knowledge is recommended.

### Common protocols

Internet protocols are standardized rules that govern how devices communicate on a network. Two important protocols are TCP and UDP. TCP is a connection-oriented protocol that establishes a virtual connection between devices before transmitting data, ensuring reliability but at a slower speed. UDP, on the other hand, is a connectionless protocol that sends data packets without establishing a connection, making it faster but less reliable. There are numerous protocols used for various purposes, such as Telnet for remote login, HTTP/HTTPS for webpage transfer, DNS for domain name lookup, FTP for file transfer, and many more. ICMP is a protocol used for device communication, including error reporting and status information. It supports various messages and requests, such as echo requests and replies. VoIP is a method of transmitting voice and multimedia communications over the internet, primarily using the SIP protocol. However, SIP can also be used for information disclosure and user enumeration. Understanding these protocols is crucial for effective network communication and security.

### Wireless Networks

Wireless networks revolutionize communication by enabling devices to connect and exchange data without the constraints of physical cables. Utilizing radio frequency technology, devices equipped with wireless adapters can transmit and receive data over the airwaves. WiFi, a popular wireless technology, enables local area networks with a range of a few hundred feet, facilitating seamless connectivity for devices such as laptops, smartphones, and tablets. On a larger scale, wireless wide area networks, powered by cellular data technology, can cover expansive areas like cities or regions.

### VPN

A Virtual Private Network (VPN) is a technology that allows a secure and encrypted connection between a private network and a remote device. This enables remote users to access the network's resources and services in a secure manner. VPNs are commonly used by companies to provide secure remote access for employees, allowing them to connect to the private network from anywhere with an internet connection. VPNs encrypt the connection, making it difficult for attackers to intercept sensitive information. They also offer cost-effective solutions compared to other remote access methods. However, it's important to choose secure VPN protocols like IPsec or OpenVPN, as older protocols like PPTP are no longer considered secure due to vulnerabilities.

### Vendor Specific Information.

Cisco IOS is the operating system used in Cisco network devices such as routers and switches. It offers a wide range of features and services necessary for network device management and operation. With support for IPv6, quality of service (QoS), security features, and virtualization capabilities like VPLS and VRF, Cisco IOS provides the functionality required for modern networks. It can be managed through the command line interface (CLI) or graphical user interface (GUI), and supports various network protocols and services such as routing protocols (OSPF, BGP), switching protocols (VTP, STP), and network services like DHCP.

# CONNECTION ESTABLISHMENT

### Key Exchange Mechanisms

key exchange methods are crucial for securely exchanging cryptographic keys between two parties. Diffie-Hellman is a widely used method that allows two parties to agree on a shared secret key without prior communication. RSA utilizes prime number properties for key generation and is widely used in various applications. Elliptic curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) provide enhanced security and efficiency using elliptic curve cryptography. Internet Key Exchange (IKE) is a protocol used for establishing and maintaining secure communication sessions, such as in VPNs, and can operate in main mode or aggressive mode. Pre-Shared Keys (PSK) can be used for authentication and establishing shared secrets, adding an extra layer of security but requiring secure key exchange.

### Authentication Protocols

Authentication protocols play a vital role in securing networks by verifying the identities of users and devices. They provide standardized and secure methods for exchanging information and protecting sensitive data. Protocols like Kerberos, SRP, SSL/TLS, OAuth, OpenID, SAML, 2FA, FIDO, PKI, SSO, MFA, PAP, CHAP, EAP, SSH, and HTTPS offer different authentication mechanisms and encryption techniques to ensure the confidentiality, integrity, and authenticity of communication

### TCP/UDP Connections

Blind spoofing is a data manipulation attack where an attacker sends false information on a network without being able to see the actual responses from the target devices. It involves manipulating the IP header fields, such as the source and destination addresses, to deceive the recipient. In the context of TCP, blind spoofing can be used by sending TCP packets with falsified source and destination port numbers, as well as a false Initial Sequence Number (ISN).

### Cryptography.

Encryption is a critical tool used on the internet to protect sensitive data during transmission. It can be categorized into symmetric and asymmetric encryption techniques. Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption involves a pair of keys: a public key for encryption and a private key for decryption. Advanced Encryption Standard (AES) is widely regarded as the most secure symmetric encryption algorithm, while asymmetric encryption methods like RSA and ECC offer enhanced security and enable authentication through digital signatures.

# CONCLUSION

A solid understanding of networking foundations and relevant components is required in order to function as an information security specialist. To advance in any area of information security, one needs a solid networking foundation. We can fully comprehend the complete network structure, its network traffic, and how various communication standards are handled by understanding how a network is organized and how the communication between the various hosts and servers occurs utilizing the various protocols. To build our tools and interface with the protocols, this understanding is crucial. [**LINK**](https://academy.hackthebox.com/achievement/643478/34)