Introduction to Networking

Here is the link to show I have completed this module

https://academy.hackthebox.com/achievement/1917469/34

Network Types

(i) WAN(wide area network) commonly referred to as internet. The WAN is the address that is generally accessed by the internet.

The primary way to identify if the network is a WAN is to use a WAN specific routing protocol such as BGP and if the IP schema in use is not within RFC 1918(10.0.0.0/8,172.16.0.0/12,192.168.0.0/16).

(ii) LAN/WLAN

This will typically assign IP addresses designated for local use RFC 1918.

(iii) VPN

There are of three types site to site vpn,remote access vpn and ssl vpn.

Network Topologies

This is a typical arrangement and physical or logical connection of devices in a network. Computer are hosts such as client and server,switches,routers and bridge work together to allow communication between all parts of the network.

There are of two types of topologies:

(i) Physical topology which is the transmission medium layout used to connect devices I.e the actual layout of cables and devices — how they are physically connected.

(ii) Logical topology is how the signals act on the network media or how the data will be transmitted across the network from one device to the devices' physical connection.

There are various network topology such as point to point topology,bus topology eg coaxial cable,star topology usually a router,hub or switch,ring topology has two cables one for incoming and other for outgoing,mesh topology ,tree topology and hybrid topology.

Proxies

A proxy is when a device or service sits in the middle of a connection and acts as a mediator and always operate at layer 7 of the OSI model.

The key types of proxies are:

(a) Dedicated proxy/forward proxy is when a client makes a request to a computer and that computer carries out the request.

(b) Reverse proxy listens on an address and forward it to a closed-off network

(c) (Non) Transparent proxy

With a transparent proxy, the client doesn't know about its existence and intercepts the client's communication requests to the Internet and acts as a substitute instance.

If it is a non-transparent proxy, we must be informed about its existence. For this purpose, we and the software we want to use are given a special proxy configuration that ensures that traffic to the Internet is first addressed to the proxy.

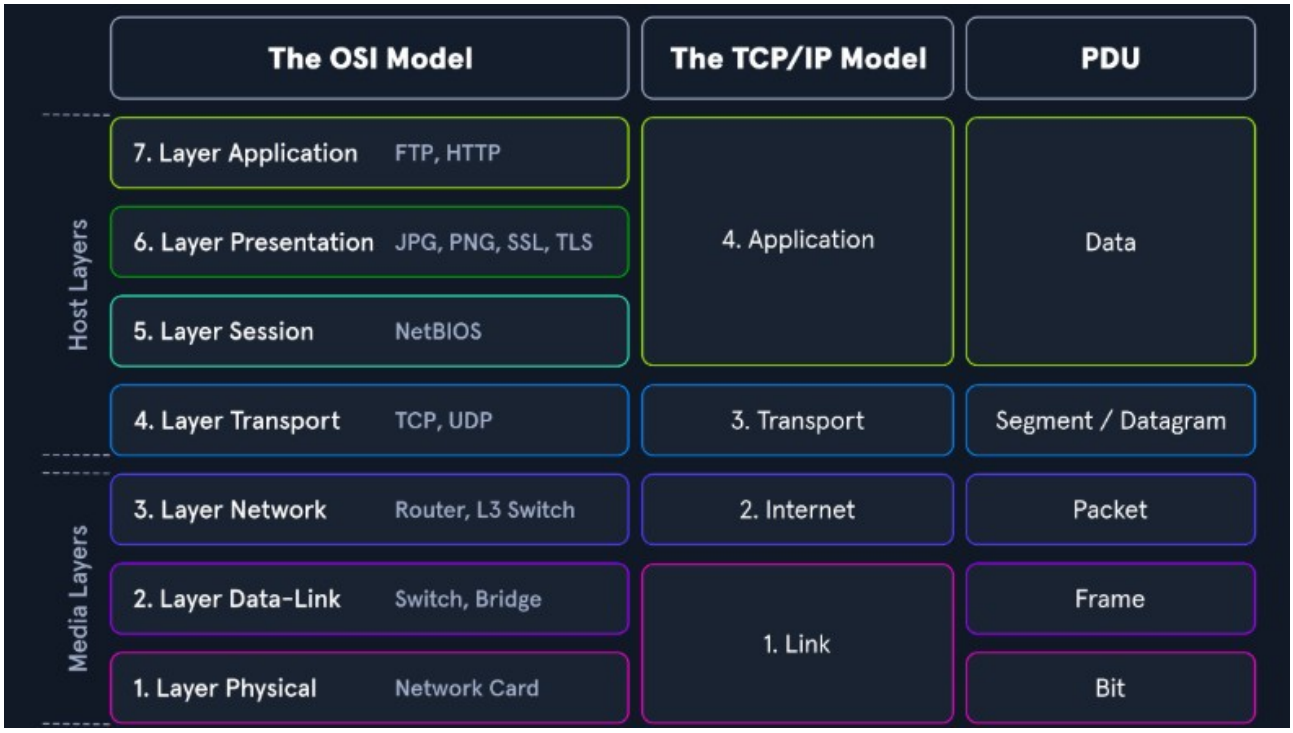
Networking Model

There are of two OSI model and TCP/IP model which describes the communication and transfer of data from one host to another.

TCP/IP is a communication protocol that allow hosts to connect to the internet while OSI is a communication gateway between the network and end users

During the transmission, each layer adds a header to the PDU from the upper layer, which controls and identifies the packet. This process is called encapsulation. The header and the data together form the PDU for the next layer.

The process continues to the Physical Layer or Network Layer, where the data is transmitted to the receiver. The receiver reverses the process and unpacks the data on each layer with the header information. After that, the application finally uses the data. a



The OSI model

The goal in defining the OSI/ISO standard was to create a reference model that enables the communication of different technical systems via various devices and technologies and provide compatibility.

It uses seven different layers,layer 2-4 is transport oriented and layer 5-7 is application oriented.

Layer	Function
7.Application	Among other things, this layer controls the input and output of data and provides the application functions.
6.Presentation	The presentation layer's task is to transfer the system-dependent presentation of data into a form independent of the application.
5.Session	The session layer controls the logical connection between two systems and prevents, for example, connection breakdowns or other problems.
4.Transport	Layer 4 is used for end-to-end control of the transferred data. The Transport Layer can detect and avoid congestion situations and segment data streams.
3.Network	On the networking layer, connections are established in circuit-switched networks, and data packets are forwarded in packet-switched networks. Data is transmitted over the entire network from the sender to the receiver.
2.Data Link	The central task of layer 2 is to enable reliable and error-free transmissions on the respective medium. For this purpose, the bitstreams from layer 1 are divided into blocks or frames.
1.Physical	The transmission techniques used are, for example, electrical signals, optical signals, or electromagnetic waves. Through layer 1, the transmission takes place on wired or wireless transmission lines.

The TCP/IP Model

In this model every application can transfer and exchange data over any network and doesn't matter where the receiver is located.

IP ensures that the data packet reaches its destination, and TCP controls the data transfer and ensures the connection between data stream and application.

Layer	Function
4.Application	The Application Layer allows applications to access the other layers' services and defines the protocols applications use to exchange data.
3.Transport	The Transport Layer is responsible for providing (TCP) session and (UDP) datagram services for the Application Layer.
2.Internet	The Internet Layer is responsible for host addressing, packaging, and routing functions.
1.Link	The Link layer is responsible for placing the TCP/IP packets on the network medium and receiving corresponding packets from the network medium. TCP/IP is designed to work independently of the network access method, frame format, and medium.

The most important tasks for TCP/IP are:

Task	Protocol	Description
Logical Addressing	IP	Due to many hosts in different networks, there is a need to structure the network topology and logical addressing. Within TCP/IP, IP takes over the logical addressing of networks and nodes. Data packets only reach the network where they are supposed to be. The methods to do so are network classes, subnetting, and CIDR.
Routing	IP	For each data packet, the next node is determined in each node on the way from the sender to the receiver. This way, a data packet is routed to its receiver, even if its location is unknown to the sender.
Error & Control Flow	TCP	The sender and receiver are frequently in touch with each other via a virtual connection. Therefore control messages are sent continuously to check if the connection is still established.
Application Support	TCP	TCP and UDP ports form a software abstraction to distinguish specific applications and their communication links.
Name Resolution	DNS	DNS provides name resolution through Fully Qualified Domain Names (FQDN) in IP addresses, enabling us to reach the desired host with the specified name on the internet.

Network Layer

This is the third layer of the OSI model that controls the exchange of data packets as they cannot be directly routed to the receiver and therefore have to be provided with routing nodes.

This layer identifies the individual network nodes,set up and clears connection channels and take care of routing and data flow control. That is it is responsible for logical addressing and routing.

The most common used protocols in this layer are: *Ipv4,Ipv6,ICMP,IGMP,RIP,OSPF.*

IP Addresses

This ensures that the delivery of data to the correct receiver and IPv4 and IPv6 ensures addressing on the internet as it is made up of the network address and host address.

IPv4 consists of a 32-bit binary number combined into 4 bytes consisting of 8-bit groups ranging from 0-255 and is divided into a host part and network apart.

In past the IP network blocks were divided into class A-E and differed in the host and network share's respective length.

A further separation of these classes into small network was done with the help of **subnetting** and was done using the netmasks which is as long as IPv4 addresses.

The two additional IPs added in the IPs column are reserved for the network address and broadcast address.

The default gateway is the name for the IPv4 address of the router that couples networks and systems with different protocols and manages addresses and transmission methods.

The **broadcast IP addre**ss's task is to connect all devices in the network with each other. Broadcast in network is a message that is transmitted to all participants of a network and does not require any responses.

The **last IP address** is the one that is used for broadcast.

Classless Inter-Domain Routing(**CIDR**) is a method of representation and replaces the fixed assignment between IPv4 and network classes.

The division is based on the subnet mask or the so-called CIDR suffix, which allows the bitwise division of the IPv4 address space and thus into subnets of any size. The CIDR suffix indicates how many bits from the beginning of the IPv4 address belong to the network. It is a notation that represents the subnet mask by specifying the number of 1-bits in the subnet mask.

Class	Network Address	First Address	Last Address	Subnetmask	CIDR	Subnets	IPs
A	1.0.0.0	1.0.0.1	127.255.255.255	255.0.0.0	/8	127	16,777,214 + 2
B	128.0.0.0	128.0.0.1	191.255.255.255	255.255.0.0	/16	16,384	65,534 + 2
C	192.0.0.0	192.0.0.1	223.255.255.255	255.255.255.0	/24	2,097,152	254 + 2
D	224.0.0.0	224.0.0.1	239.255.255.255	Multicast	Multicast	Multicast	Multicast
E	240.0.0.0	240.0.0.1	255.255.255.255	reserved	reserved	reserved	reserved

Subnetting

This is the division of an address range of IPv4 addresses into several smaller address range.

In subnetting, subnet mask is used as the template for the IPv4 address and from the 1-bits in the subnet mask we know which bits in the IPv4 address cannot be changed.

These are fixed and therefore determine main network in which subnet is located.

Questions:

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

32 – 27=5

11111111 11111111 11111111 11100000

255 255 255 224

answer is 255.255.255.224

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

lets the last bit change 0 to 1

255.255.255.31

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

27 bits are used for network and 5 bits for host.

2^5=32

32/4=8 and IP ranges from 10.200.20.0 to 10.200.20.31

in each will add 8 to the network address

and answer is 10.200.20.16

Subnet Number	Network Address	IP Range	Broadcast Address
Subnet 1	10.200.20.0	10.200.20.1 – 10.200.20.6	10.200.20.7
Subnet 2	10.200.20.8	10.200.20.9 – 10.200.20.14	10.200.20.15
Subnet 3	10.200.20.16	10.200.20.17 – 10.200.20.22	10.200.20.23
Subnet 4	10.200.20.24	10.200.20.25 – 10.200.20.30	10.200.20.31

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

From the above table answer is 10.200.15

MAC Addresses

This is the physical address for our network and each host in a network has its own 48-bit (6 octets) Media Access Control (MAC) address, represented in hexadecimal format.

The first half (3 bytes / 24 bit) is the so-called Organization Unique Identifier (OUI) defined by the Institute of Electrical and Electronics Engineers (IEEE) for the respective manufacturers.

The last half of the MAC address is called the Individual Address Part or Network Interface Controller (NIC), which the manufacturers assign.

The standard for MAC addresses are :

Ethernet (IEEE 802.3)

WIFI(IEEE 802.15)

Bluetooth (IEEE 802.11)

When a packet is delivered it must be addressed on Layer 2 to the destination host's physical address/ router/NAT which is responsible for routing and each packet has sender and destination address.

MAC address should not be relied upon as sole means of security or identification as they can be changed or spoofed so additional security measures such as network segmentation and strong authentication protocols should be implemented.

Several attacks that can be exploited through use of MAC address are MAC flooding,MAC spoofing and MAC address filtering.

ARP is a network protocol used to resolve a network layer IP address to a link layer MAC address.

When a device on a LAN wants to communicate with another device, it sends a broadcast message containing the destination IP address and its own MAC address. The device with the matching IP address responds with its own MAC address, and the two devices can then communicate directly using their MAC addresses. This process is known as **ARP resolution.**

ARP is an important part of the network communication process because it allows devices to send and receive data using MAC addresses rather than IP addresses, which can be more efficient.

Two type of request message that can be used are ARP requests and ARP reply.

ARP spoofing, also known as ARP cache poisoning or ARP poison routing, is an attack that can be done using tools like Ettercap or Cain & Abel in which we send falsified ARP messages over a LAN and the goal is to associate our MAC address with the IP address of a legitimate device on the company's network, effectively allowing us to intercept traffic intended for the legitimate device.

IPv6 Addresses

It is 128 bit long and follows the end to end principle and provides publically accessible IP addresses for any devices without the need for NAT and are of three different types.

Type	Description
Unicast	Addresses for a single interface.
Anycast	Addresses for multiple interfaces, where only one of them receives the packet.
Multicast	Addresses for multiple interfaces, where all receive the same packet.

The hexadecimal system used is as the following:

Decimal	Hex	Binary
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011

12	C	1100
13	D	1101
14	E	1110
15	F	1111

Lets look at this IPv4 address(192.168.12.160)will look in hexadecimal representation

Representation	1st Octet	2nd Octet	3rd Octet	4th Octet
Binary	1100 0000	1010 1000	0000 1100	1010 0000
Hex	C0	A8	0C	A0
Decimal	192	168	12	160

Common Protocols

The main ones are TCP and UDP. TCP is connection oriented,reliable as it ensures data arrives intact and in order,slower due to handshake and acknowledgment and used in HTTP,HTTPS,FTP,SSH.

UDP is connection-less,faster but less reliable as it does not guarantee delivery and used in VoIP,DNS,TFTP and streaming.

ICMP is used for diagnostics like ping, error reporting and TTL management.

The requests types of ICMP are echo requests(ping),timestamp requests and address mask request.

The message types are echo reply,destination unreachable,time exceeded,redirect,source quench and parameter problem.

TTL as used in ICMP prevents infinite packet looping,helps estimate hop count and can hint at the device OS as windows ttl is 128,Linux/macOS=>64 and Solaris is =>255.

VoIP enables voice/multimedia communication over internet.

The most common VoIP ports are TCP/5060 and TCP/5061, which are used for the Session Initiation Protocol (SIP).

However, the port TCP/1720 may also be used by some VoIP systems for the H.323 protocol, a set of standards for multimedia communication over packet-based networks

Nevertheless, SIP is a signaling protocol for initiating, maintaining, modifying, and terminating real-time sessions involving video, voice, messaging, and other communications applications and services between two or more endpoints on the Internet.

The most common SIP requests and methods are:

Method	Description
INVITE	Initiates a session or invites another endpoint to participate.
ACK	Confirms the receipt of an INVITE request.
BYE	Terminate a session.
CANCEL	Cancels a pending INVITE request.
REGISTER	Registers a SIP user agent (UA) with a SIP server.
OPTIONS	Requests information about the capabilities of a SIP server or user agent, such as the types of media it supports.

The most common network protocol and their key functions are as follows:

Protocol	**Port**	**Description**
HTTP / HTTPS	80 / 443	Transfer web pages (secure/insecure)
FTP / TFTP	20-21 / 69	File transfer protocols
DNS	53	Resolve domain names
SSH / Telnet	22 / 23	Secure and insecure remote login
SMTP / POP3 / IMAP	25 / 110 / 143	Email transfer and retrieval
DHCP / BOOTP	67-68	Dynamic/static IP configuration
SNMP	161-162	Network device monitoring
RDP	3389	Remote desktop access
SMB / NFS	445 / 2049	File sharing and remote system mounting
ICMP / IGMP	0-255	Network diagnostics and multicasting
SIP / H.323	5060-5061 / 1720	VoIP protocols
SQL Services	1433 (MSSQL), 3306 (MySQL), 5432 (PostgreSQL)	Database communication
ISAKMP / IPsec	500	Secure VPN setup
LDAP / Kerberos	389 / 88	Directory and authentication services

Wireless Networks

Wireless networks are computer networks that utilize wireless data connections between network nodes. Devices such as laptops, smartphones, and tablets can communicate with each other and the Internet without requiring physical cables.

These networks use radio frequency (RF) technology to transmit data. Each device contains a wireless adapter that converts data into RF signals and transmits them. Other devices receive and convert these signals back into data.

To connect, a device must be within range and configured with the correct Service Set Identifier (SSID) and password.

The Wireless Access Point (WAP) acts as the central hub, connecting the wireless devices to the wired network.

For a connection to happen,a device sends a **connection request frame** (association request) to the WAP using the IEEE 802.11 protocol.

The request include MAC address,SSID,supported data rates,supported channels and supported security protocols eg WPA2/3.

If the SSID broadcast is disabled, it will not appear in public scans, but it can still be discovered through authentication packets.

The **WEP challenge-response handshake** is a process to establish a secure connection between a WAP and a client device in a wireless network that uses the WEP security protocol. This involves exchanging packets between the WAP and the client device to authenticate the device and establish a secure connection.

Cyclic Redundancy Check (**CRC**) is an error-detection mechanism used in the WEP protocol to protect against data corruption in wireless communications.

The security features implemented in wireless networks are encryption,access control and firewalls.

The table below shows comparisons between encryption protocols:

Protocol	**IV**	**Secret Key**	**Notes**
WEP-40	24-bit	40-bit	Vulnerable to brute-force attacks
WEP-104	24-bit	104-bit	Also vulnerable, outdated
WPA	Dynamic	128-bit+	More secure; uses AES

Lightweight Extensible Authentication Protocol (**LEAP**) and Protected Extensible Authentication Protocol (**PEAP**) are authentication protocols used to secure wireless networks to provide a secure method for authenticating devices on a wireless network and are often used in conjunction with WEP or WPA to provide an additional layer of security.

The difference between them is that; **LEAP** uses a shared key for authentication, which means that the same key is used for encryption and authentication which can be susceptible to dictionary attacks while **PEAP** uses a more secure authentication method called tunneled Transport Layer Security (TLS) and this method establishes a secure connection between the device and the WAP using a digital certificate, and an encrypted tunnel protects the authentication process.

Terminal Access Controller Access-Control System Plus (**TACACS+**)is a protocol used to authenticate and authorize users accessing network devices, such as routers and switches.

When a WAP sends an authentication request to a TACACS+ server, the request typically includes the user's credentials and other information about the session and authentication requests is encrypted.

A Disassociation Attack is a type of all wireless network attack that aims to disrupt the communication between a WAP and its clients by sending disassociation frames to one or more clients.

The WAP uses disassociation frames to disconnect a client from the network. When a WAP sends a disassociation frame to a client, the client will disconnect from the network and have to reconnect to continue using the network.

There are different ways to harden wireless network and are disabling SSID broadcast to make it difficult to discover and connect,WiFi protected access(WPA) as it provides strong authentication and encryption,MAC Filtering to only allow known devices to connect and lastly deploy EAP-TLS as it uses digital certificates for strong mutual authentication.

Virtual Private Network

A **Virtual Private Network (VPN)** enables secure and encrypted communication between a remote device and a private network. It allows remote users to access internal network resources as if they were physically present within the local network.

The benefits of using VPN are:

(i) **Data Encryption:** VPNs encrypt all traffic, protecting sensitive information from interception and tampering.

(ii) **Remote Access:** Employees can securely access internal resources (e.g., file servers, emails) from anywhere with internet access.

(iii) **Cost Efficiency:** VPNs are more affordable than leased lines or dedicated remote access systems, leveraging the public Internet.

(iv)**Site-to-Site Connectivity:** VPNs can connect branch offices into a unified private network, simplifying management and improving resource sharing.

There are several components and requirements that are necessary for VPN to work:

Requirement	Description
VPN Client	This is installed on the remote device and is used to establish and maintain a VPN connection with the VPN server. For example, this could be an OpenVPN client.
VPN Server	This is a computer or network device responsible for accepting VPN connections from VPN clients and routing traffic between the VPN clients and the private network.
Encryption	VPN connections are encrypted using a variety of encryption algorithms and protocols, such as AES and IPsec, to secure the connection and protect the transmitted data.
Authentication	The VPN server and client must authenticate each other using a shared secret, certificate, or another authentication method to establish a secure connection.

At the **TCP/IP layer**, VPNs commonly use the **Encapsulating Security Payload (ESP)** protocol to encrypt and authenticate traffic, ensuring secure data exchange over public networks.

IPsec is a suite of protocols designed to secure IP communications by authenticating and encrypting each IP packet.

Ipsec uses two protocols to provide encryption and authentication:

Protocol	Function
AH (Authentication Header)	Provides integrity and authenticity, but **no encryption**. Adds a cryptographic checksum to each packet.
ESP (Encapsulating Security Payload)	Provides **encryption** and optional authentication. Encrypts the payload and may include an authentication header.

Ipsec can be used in two modes:transport and tunnel modes.

Mode	Description
Transport Mode	In this mode, IPsec encrypts and authenticates the data payload of each IP packet but does not encrypt the IP header. This is typically used to secure end-to-end communication between two hosts.
Tunnel Mode	With this mode, IPsec encrypts and authenticates the entire IP packet, including the IP header. This is typically used to create a VPN tunnel between two networks.

For example, an administrator could place a firewall in between. In order to facilitate IPsec VPN traffic from a VPN client outside a firewall to a VPN server inside, the firewall would need to allow the following protocols:

Protocol	Port	Description
Internet Protocol (IP)	UDP/50-51	This is the primary protocol that provides the foundation for all internet communication. It is used to route packets of data between the VPN client and the VPN server.
Internet Key Exchange (IKE)	UDP/500	IKE is a protocol that is used to establish and maintain secure communication between the VPN client and the VPN server. It is based on the Diffie-Hellman key exchange algorithm, and it is used to negotiate and establish shared secret keys that can be used to encrypt and decrypt the VPN traffic.
Encapsulating Security Payload (ESP)	UDP/4500	ESP is also a protocol that provides encryption and authentication for IP datagrams. It is used to encrypt the VPN traffic between the VPN client and the VPN server, using the keys that were negotiated with IKE.

Point-to-Point Tunneling Protocol (**PPTP**) is a network protocol that enables the creation of VPNs by establishing a secure tunnel between the VPN client and server, encapsulating the data transmitted within this tunnel.

Due to its vulnerabilities, PPTP is no longer recommended for secure VPN implementations.

Vendor specific Information

Cisco IOS is the operating system used in Cisco network devices like routers and switches. It provides essential features for managing and operating networks, including IPv6 support, Quality of Service (QoS), security (encryption and authentication), and virtualization (VPLS, VRF).

It also supports various network protocols and services required for network operations and are:

Protocol Type	Description
Routing protocols	Such as OSPF and BGP are used to route data packets on a network.
Switching protocols	Such as VLAN Trunking Protocol (VTP) and Spanning Tree Protocol (STP) is used to configure and manage switches on a network.
Network services	Such as Dynamic Host Configuration Protocol (DHCP) are used to automatically provide clients on the network with IP addresses and other network configurations.
Security features	Such as Access Control Lists (ACLs), which are used to control access to network resources and prevent security threats.

A VLAN is a logical grouping of network endpoints connected to defined ports on a switch allowing the segmentation of networks by creating logical broadcast domains that can span multiple physical LAN segments.

With VLANs, network administrators can segment networks based on factors such as team, function, department, or application, without worrying about the physical location of endpoints and users. A broadcast packet sent over one VLAN does not reach any other endpoint that is a member of another VLAN. Because each VLAN is regarded as a broadcast domain, it needs to have its own subnet.

Network administrators can assign the ports of a switch to VLANs either statically or dynamically. **Static VLAN** assignment involves assigning each port to a VLAN manually using the switch's network operating system; this must be done for all switches separately (it is essential to keep in mind that endpoints connecting to these ports are unaware of the existence of VLANs). In contrast, **dynamic VLAN** assignment automatically determines an endpoint's VLAN membership based on MAC addresses or protocols.

Security-wise, static VLANs are the more secure option because a port will forever be tied to a specific VLAN ID, unless changed manually afterward.

For dynamic VLANs, an attacker could potentially utilize tools such as **macchanger** to spoof the MAC address of legitimate endpoints and attain membership of their VLANs, therefore sniffing all network traffic sent through them.

VLAN tagging is the process of inserting VLAN information into an 802.1Q Ethernet header, while VLAN untagging is the process of removing the VLAN information from an 802.1Q-tagged Ethernet frame and forwarding the packet to the destined ports.

Lets assign NICs a VLAN in Linux

This will be done by creating an interface on top of another called a parent interface and will be using tools such as ip,nmcli and vconfig.

First we need to ensure 8021q was loaded successfully:

```
$ sudo modprobe 8021q
```

```
lsmod | grep 8021
```

Next find the name of the ethernet interface that will create the VLAN interface on top of which is eth0 by using command ip a

Then use ip to create a new interface that is the member of the desired VLAN 20 like this:

```
sudo ip link add link eth0 name eth0.20 type vlan id 20
```

Then based on the subnet assigned to the address with VLAN 20 within local network we assign the interface an ip address and then start it.

```
sudo ip addr add 192.168.1.1/24 dev eth0.20
sudo ip link set up eth0.20
```

lastly we can check whether the interface has changed.

```
$ ip a | grep eth0.20
```

Key Exchange Mechanisms

This methods are used to exchange cryptographic keys between two parties securely and involves mathematical operations.

(i)Diffie-Hellman is one method of key exchange which allows two parties to agree on a shared key without any prior communication or shared private information and protocol used in this is TLS that is used to protect web traffic. This method is vulnerable to MITM attacks and requires large amount of CPU power.

(ii)RSA uses the properties of large prime numbers to generate a shared secret key. This method relies on the fact that it is easy to multiply large prime numbers together but challenging to factor the resulting number back into prime factor.

(iii) Elliptic curve Diffie-Hellman is a variant of Diffie-Hellman key exchange and uses elliptic curve cryptography to generate shared secret key and is more efficient and secure than it.

To compare all this:

Algorithm	Acronym	Security
Diffie-Hellman	DH	Relatively secure and computationally efficient
Rivest-Shamir-Adleman	RSA	Widely used and considered secure, but computationally intensive
Elliptic Curve Diffie-Hellman	ECDH	Provides enhanced security compared to traditional Diffie-Hellman
Elliptic Curve Digital Signature Algorithm	ECDSA	Provides enhanced security and efficiency for digital signature generation

TCP/UDP connection

TCP packets also known as segment are divided into several sections called header and payloads.

The header contains source and destination port,sequence number,confirmation number,control flags,window size and checksum.

The payload is the actual payload of the packet and contains the data that is being transmitted.

UDP transfers datagrams between two hosts and data is sent directly to the target host without any prior connection.

Blind spoofing is a method of data manipulation attack in which an attacker sends false information on a network without seeing actual responses sent back by the target devices.

This involves manipulating the IP header field to indicate false source and destination mac address.

Cryptography

Techniques used here are encryption of digital keys in symmetric and asymmetric encryption.

DES is an example of symmetric encryption and consits of 64 bits,8 bits used as checksum.

3DES which is an extension of DES was considered more secure than the original DES because it provides security using three rounds of encryption but AES the sucessor is more secure as it provides higher security because uses longer key length.

A cipher mode refers to how a block cipher algorithm encrypts a plaintext message. A block cipher algorithm encrypts data, each using fixed-size blocks of data (usually 64 or 128 bits). A cipher mode defines how these blocks are processed and combined to encrypt a message of any length. There are several common cipher modes, including:

Cipher Mode	Description
Electronic Code Book (ECB) mode	ECB mode is generally not recommended for use due to its susceptibility to certain types of attacks. Furthermore, it does not hide data patterns efficiently. As a result, statistical analysis can reveal elements of clear-text messages, for example, in web applications.
Cipher Block Chaining (CBC) mode	CBC mode is generally used to encrypt messages like disk encryption and e-mail communication. This is the default mode for AES and is also used in software like TrueCrypt, VeraCrypt, TLS, and SSL.
Cipher Feedback (CFB) mode	CFB mode is well suited for real-time encryption of a data stream, e.g., network communication encryption or encryption/decryption of files in transit like Public-Key Cryptography Standards (PKCS) and Microsoft's BitLocker.
Output Feedback (OFB) mode	OFB mode is also used to encrypt a data stream, e.g., to encrypt real-time communication. However, this mode is considered better for the data stream because of how the key stream is generated. We can find this mode in PKCS but also in the SSH protocol.
Counter (CTR) mode	CTR mode encrypts real-time data streams AES uses, e.g., network communication, disk encryption, and other real-time scenarios where data is processed. An example of this would be IPsec or Microsoft's BitLocker.
Galois/Counter (GCM) mode	GCM is used in cases where confidentiality and integrity need to be protected together, such as wireless communications, VPNs, and other secure communication protocols.

Conclusion

Through the Introduction to Networking module on Hack The Box, I gained a strong understanding of how computer networks operate. I learned about key concepts such as the OSI and TCP/IP models, IP addressing, and common protocols like TCP, UDP, and ICMP. The module also helped me become familiar with essential networking tools and how data flows through networks. This knowledge has strengthened my foundation in cybersecurity and prepared me to handle more advanced topics in ethical hacking and network security.