NAME: DIANA WANJIRU

ADMISSION NUMBER: CS-EH02-24103

LINK (completed module):
https://academy.hackthebox.com/achievement/1242115/34

INTRODUCTION TO NETWOTRKING (HTB)

Introduction

Networking forms a vital foundation in cyber security. Having a clear understanding of networking gives one a better chance to understand concepts in cyber security.

Network Types

I had a look into the different types of networks such as the WAN, LAN, WLAN, WPAN, GAN, MAN and looked at VPN and the different types of VPNs which include site to site VPN, Remote Access VPN and the SSL VPN.

Networking Topologies

A network topology defines how devices such as computers, switches, and routers are physically or logically arranged and connected within a network. Physical topology refers to the actual layout of cables and nodes, while logical topology describes how data flows between devices. Network components are linked through wired (like twisted pair or Fiber optic) or wireless (like Wi-Fi or satellite) connections, with nodes such as routers, switches, and firewalls facilitating communication. Common network topologies include point-to-point, bus, star, ring, mesh, tree, hybrid, and daisy chain—each with unique structures and methods of data transmission. Complex networks often combine these topologies to achieve better scalability, reliability, and efficiency.

Proxies

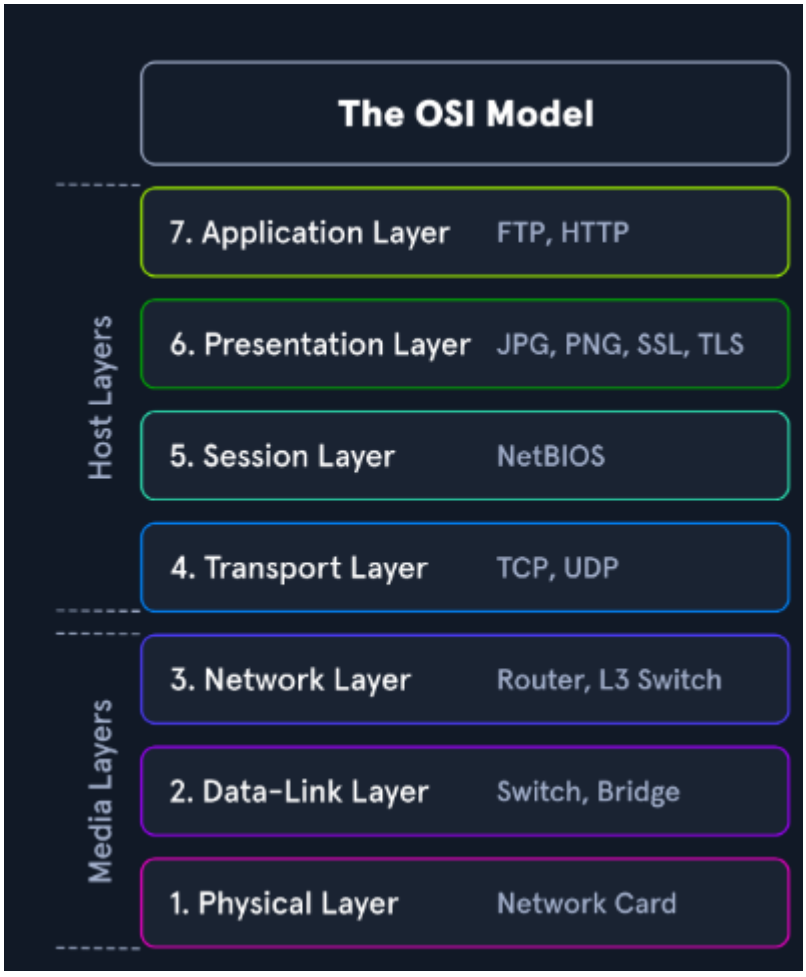
A proxy is a device or service that sits between a client and a destination, acting as a mediator that can inspect and forward traffic, unlike a gateway which simply passes traffic. Common misconceptions include thinking a VPN or changing an IP address is the same as using a proxy, though proxies typically operate at Layer 7 of the OSI model. There are different types of proxies: forward proxies handle outgoing client requests, often used in corporate networks or tools like Burp Suite, while reverse proxies manage incoming requests to protect and filter web servers, with examples including Cloudflare and ModSecurity. Proxies can also be transparent, where the client is unaware of its presence, or non-transparent, requiring explicit configuration for traffic to pass through. Overall, proxies provide security, traffic control, and monitoring capabilities, and are widely used in corporate networks, web security, and penetration testing.

Networking Models

The OSI and TCP/IP models are frameworks that describe how data is communicated between hosts in a network, with OSI having seven layers—Application, Presentation, Session, Transport, Network, Datalink, and Physical—and TCP/IP having four layers—Application, Transport, Internet, and Link. The OSI model is a strict reference framework used to define and analyze network communication, while TCP/IP is a practical protocol suite used for data transmission across the Internet. Data is transferred between layers in the form of Protocol Data Units (PDUs), with each layer adding a header in a process called encapsulation, which ensures proper routing and delivery. During transmission, the data passes through each layer, and the receiving device unpacks the headers layer by layer until the application can use the data. Understanding both models helps network professionals, including penetration testers, analyze, intercept, and troubleshoot network traffic effectively.

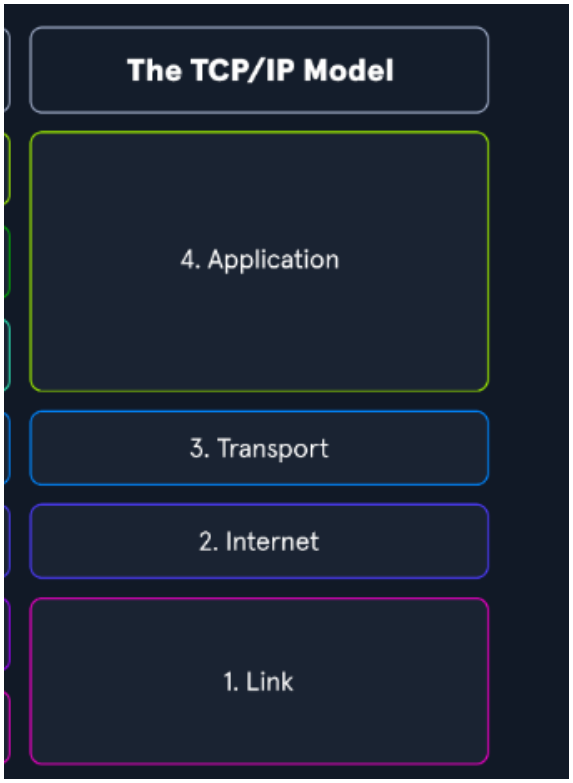
The OSI model

The ISO/OSI model is a reference framework that enables different systems to communicate. It has seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Layers 2–4 handle data transport, while layers 5–7 manage application-level functions. Each layer uses the layer below and provides services to the layer above. Data is sent from layer 7 down to layer 1 and received from layer 1 up to layer 7.



The TCP/IP model

The TCP/IP model, also known as the Internet Protocol Suite, is a four-layer framework consisting of the Link, Internet, Transport, and Application layers. It defines how data is transmitted across networks, with IP handling addressing and routing, while TCP ensures reliable data delivery and connection management. Unlike the seven-layer OSI model, TCP/IP combines certain layers to simplify communication and increase efficiency. Each layer performs specific functions—from placing packets on the network to enabling applications to exchange data seamlessly regardless of location. Core TCP/IP tasks include logical addressing, routing, error control, application support, and name resolution through DNS.



Network Layer

The network layer (Layer 3) of the OSI model manages the routing and delivery of data packets between devices across different networks. It assigns logical addresses, establishes routes, and forwards packets from node to node until they reach their destination. This layer focuses on addressing and routing rather than processing data from higher layers. Common protocols at this layer include IPv4, IPv6, IPsec, ICMP, IGMP, RIP, and OSPF, which handle packet forwarding and path determination. When direct communication between subnets isn't possible, routers forward packets through intermediate nodes until they reach the target network.

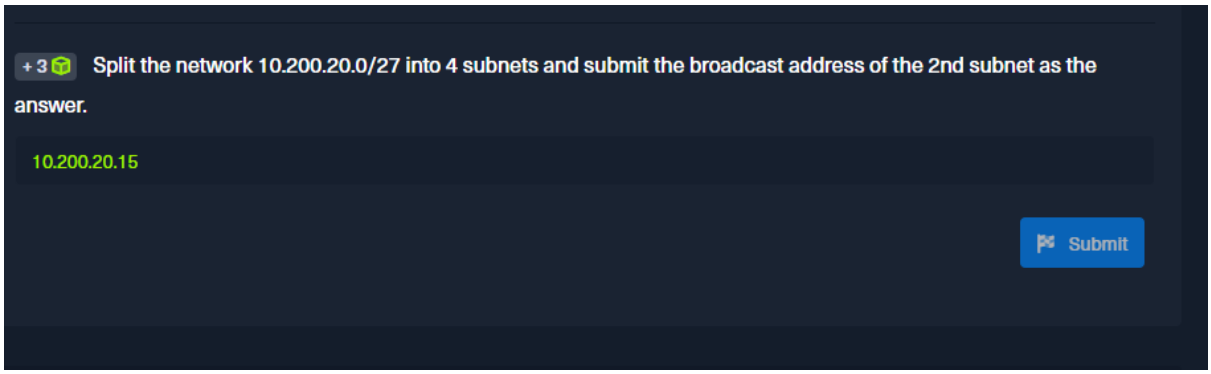
IPv4 Addresses

Each device in a network has a unique MAC address for local communication, while IP addresses (IPv4 or IPv6) enable data transfer between networks. An IPv4 address is a 32-bit number written in dotted-decimal form (e.g., 192.168.10.39) and includes both network and host parts. Formerly divided into classes A–E, IP addresses are now organized using subnetting and CIDR, which allow flexible network segmentation (e.g., /24). Broadcast addresses deliver messages to all devices in a network, and default gateways link local networks to external ones.

Subnetting

Subnetting divides a large IPv4 network into smaller segments called subnets, each with a shared network address. It defines the network, broadcast, and host addresses within each subnet. For instance, 192.168.12.160/26 with a 255.255.255.192 mask provides 62 usable hosts, while further splitting into /28 subnets yields four smaller networks of 16 addresses each. Although it involves binary math, knowing powers of two and which octet changes simplifies subnet calculations.

I also answered the questions that followed. Here are the screenshots.



MAC Addresses

MAC addresses are 48-bit (6-byte) hardware identifiers (hex formats like DE:AD:BE:EF:13:37) with the first 3 bytes as the OUI (manufacturer) and the last 3 as the device NIC; the low-order bits of the first octet indicate unicast vs multicast and global vs locally administered. Ethernet frames use MACs for local delivery, and ARP maps IPv4 addresses to MACs on a LAN. MACs can be spoofed or abused (spoofing, flooding, ARP poisoning) so they shouldn't be trusted for

security—use network segmentation, strong authentication, encrypted protocols (IPsec/SSL/TLS), and IDS/firewalls to mitigate risks.

IPv6 Addresses

IPv6, the 128-bit successor to IPv4, offers a vastly larger address space (~340 undecillion), faster routing, built-in IPsec, and supports multiple addresses per interface via SLAAC or DHCPv6. Managed by IANA, it enables end-to-end connectivity without NAT and replaces broadcasts with multicast. IPv6 addresses use hexadecimal notation (eight 16-bit blocks separated by colons, e.g., fe80::dd80:b1a9:6687:2d3b/64) and follow RFC 5952 rules—lowercase letters, omitted leading zeros, and one :: for consecutive zero blocks. Address types include unicast (single), anycast (one of many), and multicast (all).

Networking Key Terminology

Information technology covers countless terms, but knowing key protocols is essential. Common ones include **WEP, WPA, and TKIP** (wireless security), **SSH, FTP, HTTP, and SMTP** (data and communication), **SNMP, VLAN, and STP** (network management), and **RIP, OSPF, and EIGRP** (routing). Security and encryption are handled by **PGP, IPsec, and VPN**, while **SIP and VOIP** manage voice and video communication. **ARP, NAT, and DHCP** handle addressing, and **IKE, GRE, and PPTP** secure VPN tunnels. Others like **CDP, HSRP, and VRRP** ensure device discovery and redundancy, while **EAP, LEAP, and PEAP** handle authentication. These protocols form the foundation for secure and efficient network communication.

Common Protocols

Internet protocols (RFC-defined) enable device communication using **TCP** (reliable, connection-oriented) and **UDP** (fast, connectionless). **ICMP** handles diagnostics (ping, TTL, errors). **SIP** manages VoIP sessions (TCP/5060–5061) and can be exploited for user enumeration. Understanding key protocols, ports, and security risks ensures reliable, secure networking.

Wireless Networks

Wireless networks use RF signals to connect devices via Wi-Fi (IEEE 802.11) on 2.4 or 5 GHz bands through a WAP. Devices connect using the SSID, password, and protocols like TCP/IP, DHCP, and WPA2/WPA3 for security. Early WEP encryption was weak, while WPA/WPA2/WPA3 improved security with AES and stronger authentication. Extra protection includes MAC filtering, SSID hiding, and firewalls. Attacks like disassociation highlight the need for proper wireless hardening.

Virtual Private Networks

A **VPN** securely connects remote devices to private networks through encrypted tunnels using protocols like **IPsec** (UDP/500, 4500) and **PPTP** (TCP/1723). **IPsec** ensures encryption and authentication via **AH**, **ESP**, and **IKE** for key exchange. **PPTP** is outdated due to weak **MSCHAPv2** encryption, replaced by **L2TP/IPsec**, **IKEv2**, and **OpenVPN**.

Vendor Specific Information

Cisco IOS is the operating system for Cisco routers and switches, offering features like IPv6, QoS, encryption, and virtualization (VPLS, VRF). It's managed via CLI or GUI and supports protocols like OSPF, STP, and DHCP, plus security with ACLs. VLANs logically segment networks to improve performance, organization, and security by isolating broadcast domains. VLANs can be assigned statically or dynamically, with trunk ports carrying multiple VLANs using 802.1Q tagging. Cisco protocols like CDP aid device discovery, while STP prevents network loops in switch-based networks.

Key Exchange Mechanisms

Key exchange methods securely share cryptographic keys between parties to enable encrypted communication. Common methods include **Diffie-Hellman (DH)**, which establishes shared keys but is vulnerable to MITM attacks; **RSA**, which uses prime factorization for encryption and digital signatures; and **Elliptic Curve Diffie-Hellman (ECDH)**, which offers stronger security with less computation. **ECDSA** is used for efficient digital signatures. The **Internet Key Exchange (IKE)** protocol, used in VPNs, combines DH with encryption and authentication to establish secure tunnels, operating in **Main Mode** (more secure) or **Aggressive Mode** (faster). It can also use **Pre-Shared Keys (PSKs)** for authentication, though they must be exchanged securely to prevent compromise.

Authentication Protocols

Authentication protocols verify user and device identities to secure network access and data exchange. Common ones include **Kerberos**, **TLS/SSL**, **OAuth**, **SAML**, **OpenID**, **PKI**, **SSO**, **MFA**, **CHAP**, and **EAP**. For secure communication, **SSH** and **HTTPS** use encryption and certificates to prevent interception. Wireless networks often use **PEAP** or **EAP-TLS** for encrypted authentication, replacing weaker protocols like **LEAP**. Overall, these protocols ensure confidentiality, integrity, and secure access across networked systems.

TCP/UDP Connections

TCP is a connection-oriented, reliable transport (retransmits, sequence/ack numbers) while UDP is connectionless and faster for real-time traffic. IP packets carry headers (version, length, TTL, protocol, src/dst, checksum, ID, options) and a payload (TCP/UDP segment). The IP ID can link flows from the same host; Record-Route and traceroute use ICMP/TTL to reveal intermediate hops. TCP headers include ports, sequence/ACK numbers, flags, window and checksum; UDP has only ports, length and checksum. Blind spoofing fakes IP/TCP fields (e.g., ISN) to hijack or confuse connections.

Cryptography

Encryption secures internet data like payments and emails by converting it into unreadable form using mathematical algorithms and digital keys. **Symmetric encryption** (e.g., AES, DES) uses one shared key for encryption and decryption, while **asymmetric encryption** (e.g., RSA, PGP, ECC) uses a public and private key pair for secure communication and digital signatures. **AES** is faster and stronger than **DES** and **3DES**, supporting 128–256-bit keys. Data can be encrypted in various **cipher modes** (e.g., CBC, CFB, OFB, CTR, GCM), each suited for specific tasks like streaming, disk, or network encryption.

Conclusion

This module has equipped me with the basic knowledge on networking which forms a good foundation in my cyber security journey.