Topic 6

Network Security

Slides developed by VIGILANCEHUB

SECURE TODAY, THRIVE TOMORROW

What you will learn in these slides...

Networking fundamentals

- IP and MAC addresses
- OSI Model

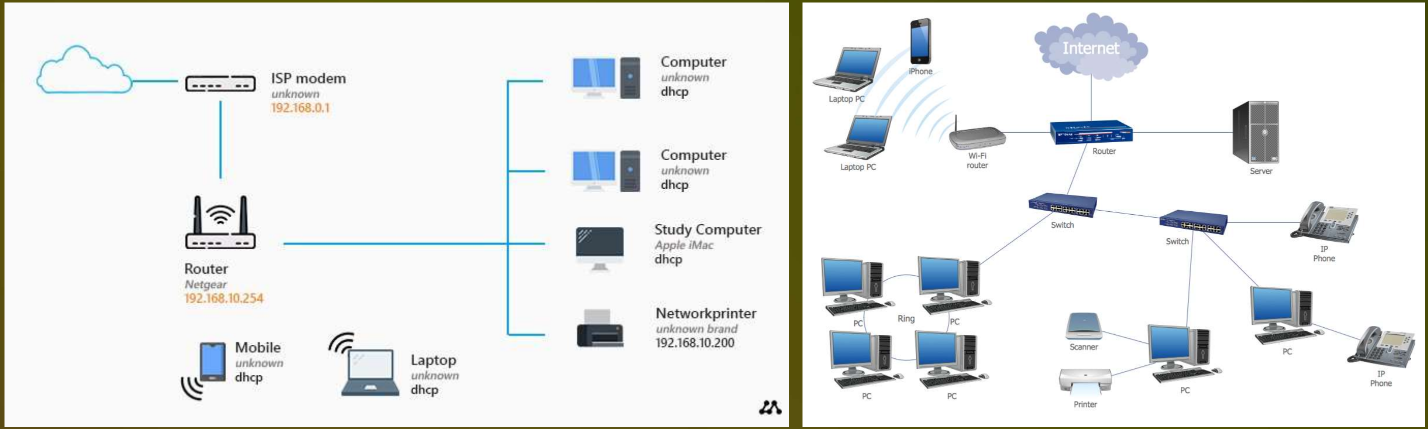
Network components

Network monitoring practices

VIGILANCEHUB
SECURE TODAY, THRIVE TOMORROW

Network Security in everyday life

- Think of your home or office network. What devices are used? How do they communicate with each other? How to ensure messages you send are not intercepted by attackers?
- Network security involves practices and technology designed to protect the CIA of data and resources on a network



Network diagrams of a typical home and office network respectively

Image credits: https://lazyadmin.nl/home-network/home-network-diagram/, https://www.conceptdraw.com/How-To-Guide/lan-diagrams

Networking Fundamentals

- Before we discuss the network devices that make up a functional network, it is good to learn some fundamentals and concepts used in networking!
  - IP addresses
  - MAC addresses
  - OSI Model

does this seem familiar to you

9:29 AM

yeah that's spongebob

Internet Protocol (IP) Address

- A unique numerical label assigned to each device or website
- Allows devices to find and communicate with each other over the Internet or local network
- Can be static (permanently assigned to a device) or dynamic (changes each time you connect to the network)
- Two types of IP addresses: IPv4 and IPv6
  - An example of an IPv4 address is 192.168.1.4 while an example of IPv6 is 2001:0db8:85a3:0000:0000:8a2e:0370:7334
  - IPv6 is a newer version and was designed to accommodate a much larger number of devices/unique IP addresses
- Without an IP address, a device cannot communicate with other devices over the network!

Media Access Control (MAC) Address

- Think of a MAC address like a home address where each house has a unique address
- Every device has a unique MAC address for sending and receiving data
- Consists of six pairs of letters and numbers (hexadecimal), each separated by a colon or hyphen, depending on the operating system
  - An example of a MAC address is 75-3D-12-C2-84-0F
- MAC addresses are built into the device’s hardware and cannot be changed
  - As each MAC address is unique to each device, network administrators can be more certain that the correct device is connecting to the network

Open Systems Interconnection (OSI) Model

- A framework used to understand how different networking protocols interact and communicate over a network
- Consists of seven layers (from top to bottom layer)

Layer		
7	**Application**	Provides network services to user applications (e.g., web browsers, email clients)
6	**Presentation**	Translates data between Application layer and the network (e.g., encryption)
5	**Session**	Manages sessions or connections between applications (e.g., session management, authentication)
4	**Transport**	Ensures data is transferred completely and accurately (e.g., TCP, UDP)
3	**Network**	Determines how data is sent to the receiving device, logical addressing using packets (e.g., IP addresses, routers)
2	**Data Link**	Manages data transfer between two devices on the same network, formats data in frames (e.g., switch, Ethernet)
1	**Physical**	Physical connection between devices (e.g., cables, wires)

Reference: https://casey.is/blogging/osi-model/

Network Components

- Firewall
- Switch
- Router
- Access Point (AP)
- Network Interface Card (NIC)
- Server

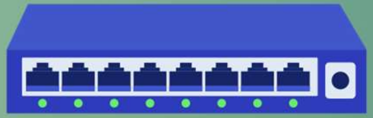
Firewall

- Monitors and filters incoming and outgoing network traffic
- Enforces security policies to block unauthorized access
- Can be hardware or software based
  - The firewall in most operating systems is a good example of a software firewall

Importance in cybersecurity

- Prevents malicious traffic from entering and exiting the network
- Maintains the confidentiality and integrity of data

Switch



- Connects multiple devices over a network
- Most switches have either 24 or 48 Ethernet ports
- Often operates at Layer 2 of the OSI Model (although Layer 3 switches exist too)

Importance in cybersecurity

- Switches perform network segmentation to limit the spread of cyber threats
- Enhances internal network performance and security

Router

- Similar to a typical home router although a few differences exist
  - Network routers in organizations are often designed for large-scale networks with many devices, while a home router is designed for smaller-scale networks with fewer devices
  - Most network routers are wired while home routers are often wireless
- Directs data packets between different networks
- Often includes built-in security features such as firewalls

Importance in cybersecurity

- Ensure data reaches its intended destination securely
- Firewall feature can prioritize traffic to ensure critical-assigned data is properly transmitted while suspicious data packets are blocked (often configured through Access Control Lists (ACLs))
- Facilitates secure connections, reducing the risk of data breaches

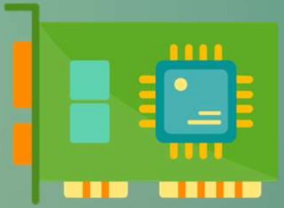
Access Point (AP)

- Provide wireless connectivity to devices within a network
- Its main purpose is to provide Wi-Fi, compared to a home router which has more capabilities (including providing Wi-Fi)
- Supports various Wi-Fi standards and encryption protocols
- Can be managed centrally for consistent security policies (usually through a phone or web application)

Importance in cybersecurity

- Ensure secure wireless access through encryption
- Controls wireless traffic to prevent unauthorized access

Network Interface Card (NIC)



- A small hardware that connects a computer or device to a network
- Often included in a motherboard or added as an expansion card
- Supports both wired and wireless connections

Importance in cybersecurity

- Must support secure network protocols to protect data transmission
- An integral part of maintaining secure network connections

Server

- A computer or program that provides services, resources or data to clients over a network
- Can host applications, databases and/or websites

Importance in cybersecurity

- Central point for securing sensitive data and critical services
- Strong security practices must be in place to prevent unauthorized access
- Must be updated and patched regularly to protect against vulnerabilities and threats

Recap on Topic 2

Common cyber threats

- Malware
- Phishing
- SQL Injection / Cross-site Scripting
- DoS / DDoS Attack
- Insider Threats
- Zero-day Exploit

In this topic, we will also discuss other cyber threats that focus more on exploiting network vulnerabilities!

- Man-in-the-middle Attack
- Port scanning

VIGILANCEHUB

SECURE TODAY, THRIVE TOMORROW

Recap on Denial of Service (DoS)

- Disrupts the availability of a website or server by flooding malicious requests or queries
- Legitimate requests and queries are unable to be processed and the website/server often hangs or crashes

*** A DoS attack can have severe repercussions on a network such as service disruption, loss of revenue, legal/compliance issues, and many more.**

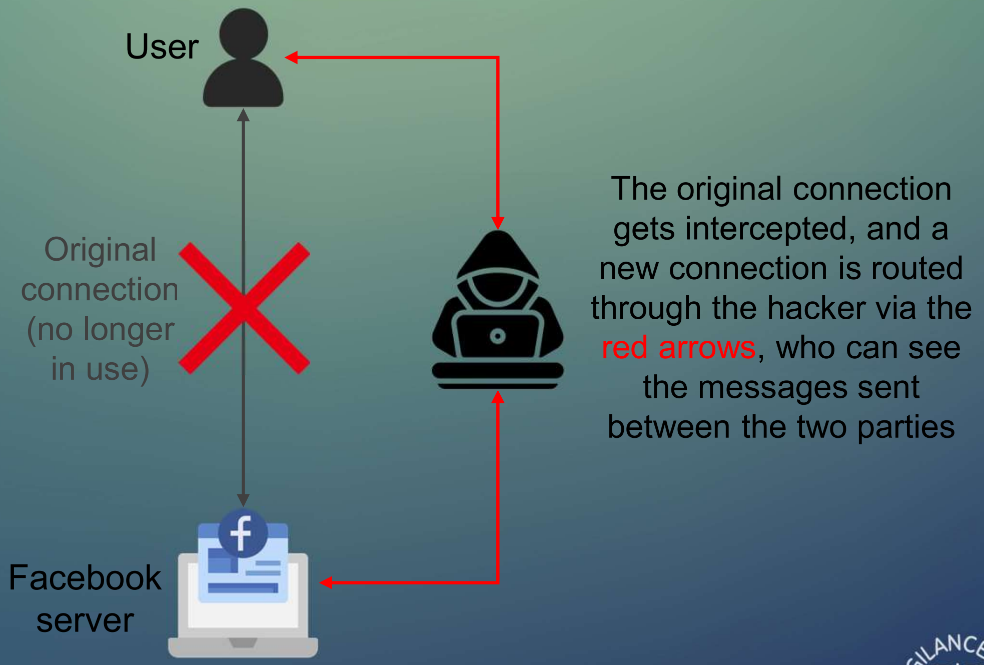
Distributed Denial of Service (DDoS)

- Involves multiple compromised devices sending requests to a website (as compared to one device for DoS)
- Harder to mitigate due to the large number of devices

Man-in-the-middle (MITM) Attack

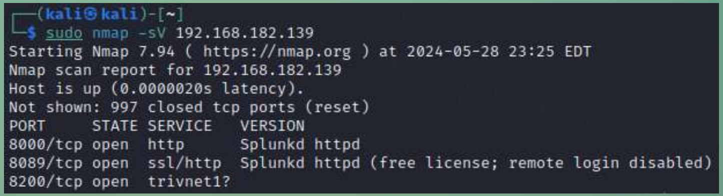
- Occurs when an attacker secretly intercepts a communication between two users/devices on a network
- The attacker can eavesdrop and/or even alter the communication without the two parties knowing
- Sensitive information such as login credentials or credit card details may be compromised

MITM attack example: A user logs in to Facebook, inputting their email and password



The original connection gets intercepted, and a new connection is routed through the hacker via the red arrows, who can see the messages sent between the two parties

Port scanning



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.182.139
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-28 23:25 EDT
Nmap scan report for 192.168.182.139
Host is up (0.0000020s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
8000/tcp open  http     Splunkd httpd
8089/tcp open  ssl/http Splunkd httpd (free license; remote login disabled)
8200/tcp open  trivnet1?
```

- Is a method to look for open ports and services available on a device
- Can be used for **both** malicious and/or non-malicious purposes
  - Malicious: Attackers use it to find potential vulnerabilities that can be exploited from the list of open ports
  - Non-malicious: IT professionals and network administrators use it for the same purpose but to fix and patch these vulnerabilities instead

Intrusion Detection and Prevention

- In addition to network components, intrusion-mitigating devices also play a huge role in organizations

Intrusion Detection System (IDS)	Intrusion Prevention System (IPS)
• Continually monitors traffic and system activities for any malicious behaviour • Upon detection of malicious activity or breach, the IDS alerts users • Can be network-based (monitor network traffic) or host-based (monitor individual devices) • IDS is a passive control system, where a user must take their own action upon being alerted	• In addition to detection, an IPS also takes action to block suspicious activities • Can prevent attacks automatically in real-time • IPS features are often integrated into firewalls or other security features • IPS is an active control system where it cleans up the mess for you, eliminating the need for user actions

- Both IDS and IPS work together to enhance overall security in organizations
- However, if not properly configured, both IDS and IPS may produce false positives
  - For example, if an IPS alerts and prevents an activity which turned out to be harmless, people may be inconvenienced
  - Therefore, IPS should be updated regularly so that it can recognize the latest threats

Reference: https://www.okta.com/identity-101/ids-vs-ips/

Virtual Private Network (VPN)

- A secure an encrypted connection over the Internet or public network between a device and the network being accessed
- IP address is hidden, and internet traffic is encrypted when using a VPN
- Users can access a private network remotely as though they are connected to it

Importance in cybersecurity

- VPNs protect sensitive data from being intercepted by attackers
- Geographic restrictions can be bypassed, allowing users to access resources or content from different locations (e.g., some Netflix shows are only available in certain countries)

Other ways to protect your networks

- Network segmentation
  - Dividing your network into smaller, isolated segments to limit the spread of malware and unauthorized access
  - Often done through VLANs and subnetting (not covered)
- Regular software updates and patches
  - Ensure your software and applications are up to date with the latest security patches
  - Allow auto-updates if possible
- MAC address filtering
  - Network administrators can specify which devices can connect to the network based on their MAC address, since all MAC addresses are unique
  - Often done through Access control lists
  - When a device tries to connect, its MAC address is checked against the list whereby, if its not on the list, connection is denied

Topic 6 Summary

- Networking fundamentals
  - IP and MAC addresses
  - OSI Model
- Network components and monitoring
  - Hardware components that make up a network
  - Network-related cyber attacks
  - How to protect networks

I WILL FIND YOUR NETWORK ENGINEER
AND GET THIS SITE UP AND RUNNING

In the next topic...

Data Protection Fundamentals

- Data Protection legislations
- Documents and terms used in data protection