Task 1:

1. Learn network security concepts

Virus:

is a type of malicious software, or malware, that spreads between computers and causes damage to data and software.

Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage. A key thing to know about computer viruses is that they are designed to spread across programs and systems. Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened.

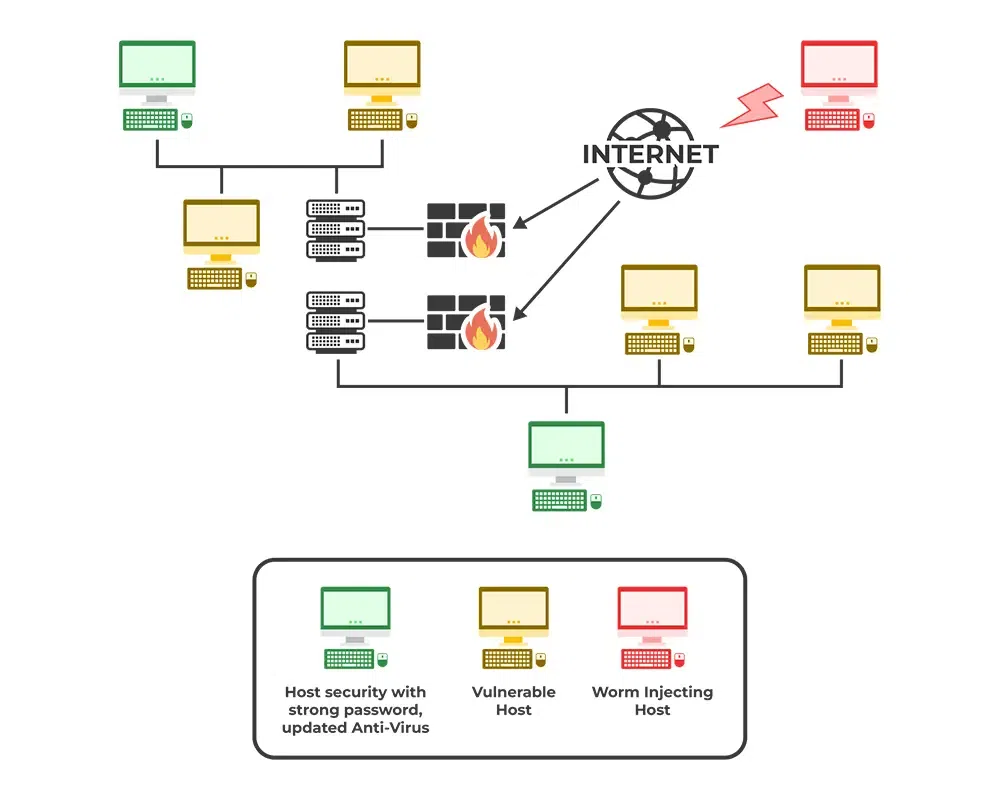
Worm:

is a type of harmful software that copy itself and spread from one computer to another without requiring any user intervention. It’s like a sickness that can move through a network of computers, searching for weaknesses to infect

A computer worm operates by finding vulnerabilities in computer systems and networks. Once it infects one computer, it searches for other computers connected to the same network and spreads to them. If once they enter into the system, worms create copies of themselves and distribute those copies to other vulnerable machines.

**Types of Computer Worms**

1. Email worm
2. Network worm
3. File sharing worm
4. Internet worms



Trojan:

are malicious programs that disguise themselves as legitimate files, which makes them difficult to detect. Learn more about Trojan viruses, how to identify them, and steps to remove them.  Trojan viruses are quite dangerous, and while they may not replicate or spread like traditional [viruses](https://us.norton.com/blog/malware/what-is-a-computer-virus), the potential for causing harm is significant. Trojan malware is particularly harmful because users unknowingly install it, which enables cybercriminals to covertly exploit vulnerabilities and have the malware go unnoticed for a while.

**Viruses:** Viruses are self-replicating and spread from one system to another by attaching themselves to legitimate files or programs. They can infect multiple files and are designed to propagate

**Trojans:** Unlike viruses, Trojans do not replicate on their own. Instead, they rely on deception to be manually installed by unsuspecting users. They often disguise themselves as harmless or even beneficial applications. But once a Trojan is executed, it can perform various nefarious actions without the user's knowledge.

Types of trojan:

1. Backdoor
2. Downloader
3. **Remote Access Trojan (RAT)**
4. **Distributed Denial of Service (DDoS) Attack Trojans**
5. Infostealer Trjan

Phishing attacks:

Phishing got its name from “**phish**” meaning fish. It’s a common phenomenon to put bait for the fish to get trapped. Similarly, phishing works. It is an unethical way to dupe the user or victim to click on harmful sites. The attacker crafts the harmful site in such a way that the victim feels it to be an authentic site, thus falling prey to it. The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim. The main motive of the attacker behind phishing is to gain confidential information like:

* Password
* Credit card details
* Social security numbers
* Date of birth

How is Phishing Carried Out?

1-**Clicking on an unknown file or attachment**

**2-Using an open or free wifi hotspot**

**3-Responding to social media requests**

**4-Clicking on unauthenticated links or ads**

**Types of Phishing Attacks**

1-**Email Phishing**

2-**Spear Phishing**

3-**Whaling**

4-**Smishing**

5-**Vishing**

6-**Clone Phishing**

**Firewall:**

is a security device (hardware, software, or both) that monitors and controls incoming and outgoing network traffic. It establishes a barrier between a trusted internal network and untrusted external networks, such as the internet. Firewalls help prevent unauthorized access to or from a private network.

**Types of firewalls**:

* **Packet-filtering firewall**: Inspects packets and allows or blocks them based on predefined rules.
* **Stateful inspection firewall**: Monitors the state of active connections and makes decisions based on the state and content of traffic.
* **Proxy firewall**: Acts as an intermediary between internal clients and external servers, filtering traffic based on its content.

Encryption:

is the process of converting data into an unreadable format (ciphertext) using algorithms. Only authorized parties can decrypt the data back into readable form (plaintext). It's widely used to protect sensitive information, such as passwords, personal data, and communications.

**Types of encryption**:

* **Symmetric encryption**: Uses the same key for both encryption and decryption (e.g., AES).
* **Asymmetric encryption**: Uses a public key for encryption and a private key for decryption (e.g., RSA).

**Secure Network Configurations**:

implementing measures to protect network infrastructure from threats. Common practices include:

* **Using strong passwords** for all devices and systems.
* **Disabling unused services and ports** to minimize vulnerabilities.
* **Network segmentation**, which divides a network into smaller segments to control access and improve security.
* **Using VPNs (Virtual Private Networks)** for secure remote access.
* **Regular updates and patching** to protect against known vulnerabilities.

2. Implement Basic Security Measures:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

3. **Basic Security Configurations on the Router**

A screenshot of a computer

Description automatically generated

Monitor Network Traffic:

A screenshot of a computer

Description automatically generated

Tcp

A screenshot of a computer

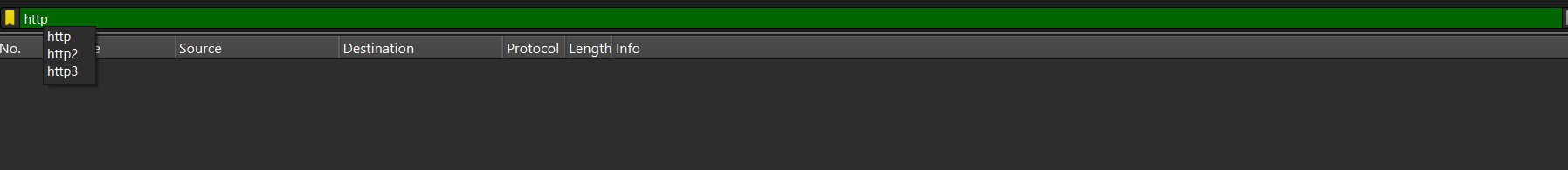
Description automatically generated

Dns

A screen shot of a computer

Description automatically generated

http



**HTTP (HyperText Transfer Protocol)**:

* Used for web traffic, mainly on port 80 (unsecured) or port 443 (HTTPS, encrypted).
* Packets include requests and responses, such as GET, POST, and 200 OK.

**DNS (Domain Name System)**:

* Used for resolving domain names (e.g., google.com) to IP addresses.
* Look for DNS query packets with requests and response packets with resolved IPs.

**TCP (Transmission Control Protocol)**:

* Used for reliable communication. Commonly seen in web traffic and other services that require error-checking (e.g., email).
* TCP traffic shows a **three-way handshake** (SYN, SYN-ACK, ACK).

**UDP (User Datagram Protocol)**:

* Used for faster, connectionless communication (e.g., DNS, streaming).
* Lacks the reliability of TCP but is faster for certain applications.

**a. Suspicious Protocol Usage:**

* **Unencrypted HTTP**: Look for sensitive data, such as passwords or personal information being sent over HTTP (port 80) instead of HTTPS (port 443).
* **Unusual Ports**: Traffic on ports that don’t correspond to the normal usage of a service could indicate malware communication.
* **DNS Exfiltration**: Abnormally large DNS query responses or unusual domain names in DNS traffic can indicate data exfiltration.

**b. Large Numbers of Packets:**

* **Denial-of-Service (DoS) Attack**: High volumes of TCP SYN packets could indicate a SYN flood, a form of DoS attack.
* **Unusual DNS Traffic**: Excessive DNS requests, especially to unknown or sketchy domains, could indicate malware trying to communicate with a command and control server.

**c. Scanning Activity:**

* If you see a lot of **SYN packets** being sent to various ports on a machine, this could be a sign of **port scanning**, often performed by attackers looking for open services to exploit.

**d. Unusual IP Addresses:**

* **External Connections**: Unexpected connections to external IP addresses, especially from countries or regions you don’t typically communicate with, could indicate malware activity or unauthorized access.

**e. Malformed Packets:**

* **TCP retransmissions** and **checksum errors** may indicate network issues, but they could also be a sign of malicious activity, such as attackers attempting to bypass firewalls.

statistical

i/o graphic🡪To spot traffic spikes that may indicate Denial of Service (DoS) attacks or file transfers.

A screenshot of a computer

Description automatically generated

Endpoints🡪To see which devices are most active on your network and whether any unknown devices are present.

A screenshot of a computer

Description automatically generated

Flow chart🡪To troubleshoot failed connections by seeing whether the TCP handshake is successful or where the communication breaks down.

A screenshot of a computer

Description automatically generated

Service Response Time🡪To analyze the performance of DNS queries or measure how quickly a web server responds to HTTP requests.

A screenshot of a computer

Description automatically generated

**Expert Information🡪To troubleshoot network performance issues or detect suspicious anomalies like malformed packets, which can sometimes indicate an attack or configuration error.**

A screenshot of a computer

Description automatically generated

**Larger Networks**

* **Intrusion Detection Systems (IDS)**: IDS monitors network traffic for suspicious activity and potential threats, alerting administrators of any detected anomalies. In larger networks, IDS can provide critical insights into unusual behavior, allowing for early detection of security breaches.
* **Network Segmentation**: This practice divides a network into smaller, isolated segments, limiting access to sensitive areas of the network. By separating different parts of a network (e.g., user devices, servers, and critical systems), segmentation reduces the risk of lateral movement by attackers once they gain access to one part of the network.
* **Multi-Factor Authentication (MFA)**: MFA adds an extra layer of security beyond just a password. Users must provide two or more verification factors (e.g., a password and a temporary code sent to their phone). This prevents attackers from gaining access even if they have stolen a user’s credentials.