**Summary of Network Threats (Completed)**

**Malware** is any code that can be used to steal data, bypass access controls, cause harm to, or compromise a system.

* **Virus:** A type of computer program that, when executed, replicates and attaches itself to other files by inserting its own code into them.
* **Worm:** A malicious software program that replicates by independently exploiting vulnerabilities in networks.
* **Trojan Horse:** A malware that carries out malicious operations by masking its true intent.
* **Logical Bomb:** A malicious program that waits for a trigger (e.g., a specific date, time, or user action) to set off the malicious code.
* **Ransomware:** Designed to hold a computer system or the data it contains captive until a payment is made.

**Social Engineering**

* **Phishing:** Occurs when a user is contacted by email or instant message by someone masquerading as a legitimate person or organization in order to trick the recipient into installing malware on their devices or sharing personal information such as login credentials or financial information.

**Denial of Service (DoS) Attacks**

* **DoS Attacks:** Work by creating an overwhelming quantity of traffic or by sending maliciously formatted packets that cannot be identified by an application, causing the receiving device to run slowly or crash.
* **DDoS Attacks (Distributed DoS):** Similar to DoS but originate from multiple coordinated sources, making them much harder to block.

**Network-Based Attacks**

* **DNS Attacks:** Includes spoofing and hijacking.
  + **DNS Spoofing:** An attacker injects false DNS information into a DNS resolver's cache, causing it to return an incorrect IP address and redirecting users to a malicious website.
  + **DNS Hijacking:** An attacker takes control of a domain name's registration or manipulates DNS queries to resolve the domain to their own IP address.
* **IP Spoofing:** The creation of Internet Protocol (IP) packets with a false source IP address, often used to conceal the attacker's identity or impersonate another system.
* **Man-in-the-Middle (MITM) Attack:** An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. This is typically achieved by intercepting traffic and relaying it after decryption/re-encryption.
* **Session Hijacking:** Exploiting a valid computer session (e.g., a browser session) to gain unauthorized access to information or services in the target system.

| **Security Measure Implemented** | **Implementation Detail** | **Rationale (Why Implemented)** | **Source** |
| --- | --- | --- | --- |
| **Firewall Configuration** | Enabled and configured the firewall on the host operating system (simulated via Kali VM) to block unauthorized access. | To act as a first line of defense, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules, thus preventing unauthorized connections to the VM. | "Enable and configure a basic firewall (e.g., Windows Defender Firewall) to block unauthorized access." |
| **Network Setup** | Set up a simple virtual lab network environment (e.g., using NAT mode in VMware) with the host (Windows) and guest (Kali) acting as two connected devices. | To establish a controlled environment to simulate a small network and practice monitoring and configuration. | "Set up a simple network environment, such as your home network or a virtual lab with a router and one or two connected devices." |
| **Network Encryption** | (Conceptual implementation, as WebGoat is HTTP) Configured the network to use strong encryption standards (like WPA2/WPA3). | To ensure that all transmitted data is secured and cannot be intercepted or read by an attacker during transit. | "Set up basic security configurations, such as changing default passwords and enabling network encryption (WPA2 or WPA3)." |