Computer Security week 2

Khaula Molapo

Year 2 Semester 2

1.

A Distributed Denial of Service (DDoS) attack is a serious cybersecurity threat where multiple compromised systems, often part of a botnet, flood a target server or network with excessive traffic. This overwhelming surge of requests makes the targeted system unavailable to legitimate users, causing downtime and potential financial loss. For example, an e-commerce website may be attacked during a sales event, making it impossible for customers to make purchases. Hackers often use DDoS attacks as a form of blackmail, demanding payment to stop the attack, or as a smokescreen for other malicious activities such as data theft. The main danger of a DDoS attack lies in its simplicity and effectiveness—attackers do not need advanced skills, just access to a network of infected devices. Businesses that are unprepared risk losing revenue, damaging customer trust, and facing significant recovery costs. Prevention requires proactive monitoring and robust protection strategies.

2.

Ransomware is a type of malicious software that encrypts a victim's files and demands payment, usually in cryptocurrency, to restore access. It can spread through phishing emails, malicious downloads, or vulnerabilities in outdated systems. The impact is devastating: businesses face downtime, data loss, and reputational damage, while individuals risk losing personal files. Hospitals, governments, and corporations have been frequent targets, with operations grinding to a halt until the ransom is paid—or data is lost forever. Mitigation involves regular data backups, patching software vulnerabilities, training users against phishing, and deploying strong endpoint security solutions to detect and block ransomware early.

3.

Using Wireshark to analyze a network packet gave me a clear picture of how data travels across a network. I could see packet headers, source and destination IPs, and the type of protocol used. This exercise showed me how attackers might exploit vulnerabilities by injecting malicious traffic or scanning open ports. Similarly, simulating a scan in Kali Linux with Nmap

highlighted how easy it is to identify weaknesses if security is poor. Both tools reinforced the importance of monitoring and securing networks. Understanding these scans and packets helps build stronger defenses against intrusions, ensuring networks remain safe and resilient.

4.

In Canva, I designed a threat mitigation diagram for DoS and DDoS protection. The diagram begins with the attacker's traffic flooding a server. Between the attacker and the target system, I placed layered defenses such as firewalls, intrusion prevention systems, and DDoS scrubbing services. Load balancers were shown distributing traffic evenly to reduce strain on a single server. Monitoring tools and alerts connected to a security team illustrated proactive response. The diagram makes it clear that no single defense is enough; instead, layered security ensures attackers are filtered, blocked, or diverted before reaching critical systems, minimizing downtime and damage