Day 7

What is Ransomware?

Ransomware is a type of malicious software that encrypts files or locks systems, demanding payment (usually in cryptocurrency) to restore access. It's a form of cyber extortion where attackers threaten to destroy or withhold access to important data unless a ransom is paid.

How to Detect Ransomware

1. Monitor System Changes

- File Encryption: Look for sudden changes in file extensions or the appearance of new file types. Ransomware often encrypts files and changes their extensions, making them inaccessible.
- Unusual File Activity: Track rapid or large-scale file modifications, especially in a short period, which can indicate ransomware encrypting files.

2. Watch for Unusual System Behavior
   - Performance Issues: Slowdowns, crashes, or high CPU usage may signal ransomware activity.
   - Unusual Pop-Ups or Alerts: Unexpected pop-ups or ransom notes demanding payment or giving instructions for decryption are common signs of a ransomware attack.
3. Monitor Network Activity
   - Suspicious Network Traffic: Look for unusual outbound connections or increased network traffic to unfamiliar IP addresses, which can indicate communication with a ransomware command-and-control server.
   - Blocked Network Access: Ransomware may block access to network resources or backup servers to prevent recovery.
4. Review Security Alerts and Logs
   - Antivirus and Anti-Malware Alerts: Ensure your security software is up-to-date and configured to alert you to potential ransomware activity.
   - System and Security Logs: Regularly review logs for unusual activities, such as unexpected file changes or unauthorized access attempts.