Viruses and Related Threats

1. Virus

- **Definition:** A virus is a self-replicating program that attaches itself to clean files and spreads throughout a computer system, usually damaging or altering data.
- **Trigger:** Activation when the infected file is executed.
- **Examples:** File viruses, boot sector viruses, macro viruses.

2. Worm

- **Definition:** A worm is a standalone malware program that replicates itself to spread to other computers.
- **Difference from Virus:** Worms do **not** need a host file to spread.
- **Example:** WannaCry ransomware worm.

3. Trojan Horse

- **Definition:** A program that appears legitimate but performs malicious activities once installed.
- **Behavior:** May create backdoors for attackers to access the system.
- **Example:** Zeus Trojan.

4. Logic Bomb

- **Definition:** Malicious code triggered by specific events (e.g., a certain date, deletion of a user).
- **Hidden:** Inside legitimate programs until triggered.

5. Ransomware

- **Definition:** Malware that encrypts a user's data and demands ransom for decryption keys.
- **Example:** CryptoLocker, REvil.

6. Spyware

- **Definition:** Software that secretly gathers information about a person or organization without consent.
- **Common Usage:** Monitoring user behavior, stealing credentials.

7. Adware

- **Definition:** Software that automatically displays or downloads advertising material.
- **Impact:** Can slow down systems and annoy users.

8. Rootkit

- **Definition:** Software tools that enable an attacker to gain administrator-level access without detection.
- **Danger:** Hides malicious processes from detection tools.

Countermeasures

1. Antivirus Software

- **Role:** Detects, quarantines, and removes malware.
- **Examples:** Norton, McAfee, Kaspersky.
- **Note:** Should be regularly updated to recognize new threats.

2. Firewalls

- **Role:** Block unauthorized access to or from a private network.
- **Types:** Hardware and Software firewalls.

3. Regular System Updates and Patch Management

- **Purpose:** Fix security vulnerabilities that viruses and worms exploit.
- **Method:** Automatic updates or manual patching.

4. Email Security

- **Actions:**
  - Don't open suspicious attachments.
  - Use email scanning and filtering.
  - Educate users about phishing tactics.

5. Backup Strategies

- **Importance:** Regular backups ensure data recovery even if systems are infected.
- **Best Practices:** Use both offline and cloud backups.

6. User Education

- **Training:** Teach safe browsing, recognizing phishing attempts, and proper password management.

7. Secure Configurations

- **Hardening Systems:** Disable unnecessary services, change default passwords, and limit administrative rights.

8. Intrusion Detection and Prevention Systems (IDPS)

- **Function:** Detect and prevent malware activities and intrusion attempts.

9. Sandboxing

- **Technique:** Running suspicious files or programs in a controlled, isolated environment to observe behavior without affecting the actual system.

10. Use of Strong Authentication

- **MFA (Multi-Factor Authentication):** Reduces risks even if passwords are compromised.

Viruses and Related Threats

1. Virus

- **Definition:** A virus is a self-replicating program that attaches itself to clean files and spreads throughout a computer system, usually damaging or altering data.
- **Trigger:** Activation when the infected file is executed.
- **Examples:** File viruses, boot sector viruses, macro viruses.

2. Worm

- **Definition:** A worm is a standalone malware program that replicates itself to spread to other computers.
- **Difference from Virus:** Worms do **not** need a host file to spread.
- **Example:** WannaCry ransomware worm.

3. Trojan Horse

- **Definition:** A program that appears legitimate but performs malicious activities once installed.
- **Behavior:** May create backdoors for attackers to access the system.
- **Example:** Zeus Trojan.

4. Logic Bomb

- **Definition:** Malicious code triggered by specific events (e.g., a certain date, deletion of a user).
- **Hidden:** Inside legitimate programs until triggered.

5. Ransomware

- **Definition:** Malware that encrypts a user's data and demands ransom for decryption keys.
- **Example:** CryptoLocker, REvil.

6. Spyware

- **Definition:** Software that secretly gathers information about a person or organization without consent.
- **Common Usage:** Monitoring user behavior, stealing credentials.

7. Adware

- **Definition:** Software that automatically displays or downloads advertising material.
- **Impact:** Can slow down systems and annoy users.

8. Rootkit

- **Definition:** Software tools that enable an attacker to gain administrator-level access without detection.
- **Danger:** Hides malicious processes from detection tools.

Countermeasures

1. Antivirus Software

- **Role:** Detects, quarantines, and removes malware.
- **Examples:** Norton, McAfee, Kaspersky.
- **Note:** Should be regularly updated to recognize new threats.

2. Firewalls

- **Role:** Block unauthorized access to or from a private network.
- **Types:** Hardware and Software firewalls.

3. Regular System Updates and Patch Management

- **Purpose:** Fix security vulnerabilities that viruses and worms exploit.
- **Method:** Automatic updates or manual patching.

4. Email Security

- **Actions:**
  - Don't open suspicious attachments.
  - Use email scanning and filtering.
  - Educate users about phishing tactics.

5. Backup Strategies

- **Importance:** Regular backups ensure data recovery even if systems are infected.
- **Best Practices:** Use both offline and cloud backups.

6. User Education

- **Training:** Teach safe browsing, recognizing phishing attempts, and proper password management.

7. Secure Configurations

- **Hardening Systems:** Disable unnecessary services, change default passwords, and limit administrative rights.

8. Intrusion Detection and Prevention Systems (IDPS)

- **Function:** Detect and prevent malware activities and intrusion attempts.

9. Sandboxing

- **Technique:** Running suspicious files or programs in a controlled, isolated environment to observe behavior without affecting the actual system.

10. Use of Strong Authentication

- **MFA (Multi-Factor Authentication):** Reduces risks even if passwords are compromised.