Vulnerability

- **Definition**: A flaw, weakness, or misconfiguration in software, hardware, or a system that can be **exploited** by attackers.
- **Key Idea**: It is a security gap or opportunity for attack.
- **Example**:
  - A weak password, outdated software, or an unpatched server.
  - **Heartbleed** in OpenSSL is a vulnerability.
- **Think**: A vulnerability **invites attacks** but doesn't directly cause harm unless exploited.

Malware

- **Definition**: Malicious software specifically designed to **harm**, compromise, or control a system.
- **Key Idea**: It is the actual **tool or program** attackers use to cause damage or steal information.
- **Example**:
  - Viruses, worms, rootkits, ransomware, or trojans.
  - **Mirai Botnet** or **Erebus Ransomware** are types of malware.
- **Think**: Malware **exploits vulnerabilities** to enter or damage systems.

Types of Vulnerabilities

1. **Direct Vulnerabilities**

   - Flaws attackers can exploit immediately.
   - **Example**: Weak root password or unpatched software.
   - **Easy Definition**: Direct flaws that attackers directly use without help.
2. **Indirect Vulnerabilities**

   - Attackers use intermediaries or third-party software.
   - **Example**: Man-in-the-Middle (MitM) attacks or dependency exploits.
   - **Easy Definition**: Weaknesses that need other systems or software to attack.
3. **Veiled Vulnerabilities**

   - Hidden flaws embedded in malware; hard to detect.
   - **Example**: Rootkits modify system commands to hide processes.
   - **Easy Definition**: Hidden vulnerabilities attackers conceal.
4. **Conditional Vulnerabilities**

   - Exploitable only under specific configurations.
   - **Example**: Heartbleed vulnerability in OpenSSL (specific versions).
   - **Easy Definition**: Flaws that need certain conditions to exist.

Examples of Linux Vulnerabilities

- **Heartbleed (OpenSSL)**:
  - Allows attackers to read server memory.
  - **Cause**: Enabled Heartbeat feature in OpenSSL v1.0.1-1.0.1f.
- **Shellshock (Bash)**:
  - Affects specific Bash versions and allows remote code execution.
- **Spectre & Meltdown**:
  - CPU vulnerabilities that exploit speculative execution.

Tip: Always update software and disable unused features.

Security Measures

1. **SSH Key Pair for Secure Authentication**
   - **Command**: `ssh-keygen -t rsa -b 4096 -C "user@example.com"`
   - Generates a secure key pair for authentication.
   - **Benefit**: More secure than password-based logins.
2. **Scanning Log Files**
   - Analyze logs for anomalies or failed login attempts.
   - **Commands**:
     - `grep "Failed password" /var/log/auth.log`
     - `tail -f /var/log/syslog`
3. **Identifying and Closing Hidden Ports**
   - **To Find Open Ports**:
     - `sudo ss -tuln` (shows listening sockets).
     - `sudo nmap -sT localhost` (scans for open ports).
   - **To Close Ports**:
     - `sudo systemctl stop service_name` (stop unused services).
     - `sudo systemctl disable service_name` (disable at boot).
     - `sudo iptables -A INPUT -p tcp --dport 8080 -j DROP` (block ports).

Linux Malware

1. **Botnets**
   - **Definition**: Group of infected devices controlled remotely.
   - **Example**: Mirai Botnet.
   - **Prevention**: Use SSH, disable Telnet, monitor unusual traffic.
2. **Ransomware**
   - **Definition**: Malware that encrypts files and demands payment.
   - **Example**: Erebus Ransomware.

- **Prevention**: Backups, file integrity tools, and read-only mounts.

3. **Rootkits**

   - **Definition**: Malware that hides attackers' activities and grants root-level access.
   - **Example**: Linux.Lady Rootkit.
   - **Detection Tools**: `chkrootkit`, `rkhunter`.