Objective

The main objective is to analyze the vulnerabilities that Nmap found and create a detailed report. This report includes information such as the service, description, CVE reference, recommendations, and severity for each vulnerability.

Process

From a Linux terminal, I used the command **nmap -sV 192.168.199.129** (This IP belongs to Metasploitable), which identified the active services, versions, and protocols. Then, I used the searchsploit command followed by the name of a service to find known vulnerabilities. After that, I conducted an investigation into some of these vulnerabilities to find details on the affected service, risks, and solutions.

1-

- **Name:** Terrapin Vulnerability in OpenSSH
- **Service Affected:** OpenSSH 4.7 on port 22.
- **Vulnerability Description:** This security vulnerability, known as the Terrapin Attack, affects SSH and its implementations. It allows threat actors to bypass integrity checks during the SSH handshake, which can lead to the reduction or disabling of security features. Specifically, attackers can exploit a flaw in the initial handshake to remove messages, including those related to countermeasures against keystroke timing attacks.
- **CVE Reference:** CVE-2023-48795
- **Common Vulnerability Scoring System (CVSS):**
    - Score: 5.9
    - Severity: Medium
    - Attack Vector: Network
    - Attack Complexity: High
    - Privileges Required: None
    - User Interaction: None
    - Scope: Unchanged
    - Confidentiality: None
    - Integrity: High
    - Availability: None

Mitigation: The most recommended mitigation is to update the SSH implementation to a patched version. This vulnerability is a protocol flaw, and a new protocol extension was introduced to fix it. Both the client and server need to be updated to be fully protected. Updating only one side is not sufficient.

2-

- **Name:** File Copy Vulnerability
- **Service Affected:** ProFTPD 1.3.5b on port 2121.
- **Vulnerability Description:** This is an arbitrary file copy vulnerability that allows attackers to copy files from the server to another location on the same server. This

could lead to information disclosure or remote code execution, even without authentication or with limited user credentials. The issue stems from the mod_copy module.

- **CVE Reference:** CVE-2019-12815
- **Common Vulnerability Scoring System (CVSS):**
    - Score: 9.8
    - Severity: Critical
    - Attack Vector: Network
    - Attack Complexity: Low
    - Privileges Required: None
    - User Interaction: None
    - Scope: Unchanged
    - Confidentiality: High
    - Integrity: High
    - Availability: High

Mitigation: The recommended action is to update ProFTPD to a patched version. This vulnerability affects versions from 1.3.1 up to 1.3.6.

3-

- **Name:** Cryptographic Vulnerability in VNC
- **Service Affected:** VNC on port 5900.
- **Vulnerability Description:** The VNC authentication mechanism is based on a challenge-response system where the server and client use the same password for encryption. The server sends a challenge to the client, the client encrypts it and sends it back. The server then performs the same encryption, and if the responses match, the client is authenticated. An attacker can potentially exploit this because the communication itself is unencrypted, allowing them to intercept the challenge and response to derive the password.
- **CVE Reference:** CVE-2025-27458
- **Common Vulnerability Scoring System (CVSS):**
    - Score: 6.5
    - Severity: Medium
    - Attack Vector: Network
    - Attack Complexity: Low
    - Privileges Required: None
    - User Interaction: Required
    - Scope: Unchanged
    - Confidentiality: High
    - Integrity: None
    - Availability: None

Mitigation: The most effective solution is to install the latest firmware or software update from the vendor. These updates should contain a fix that addresses the vulnerability. You can also use a VPN or an authentication gateway to ensure that only authorized users can connect.