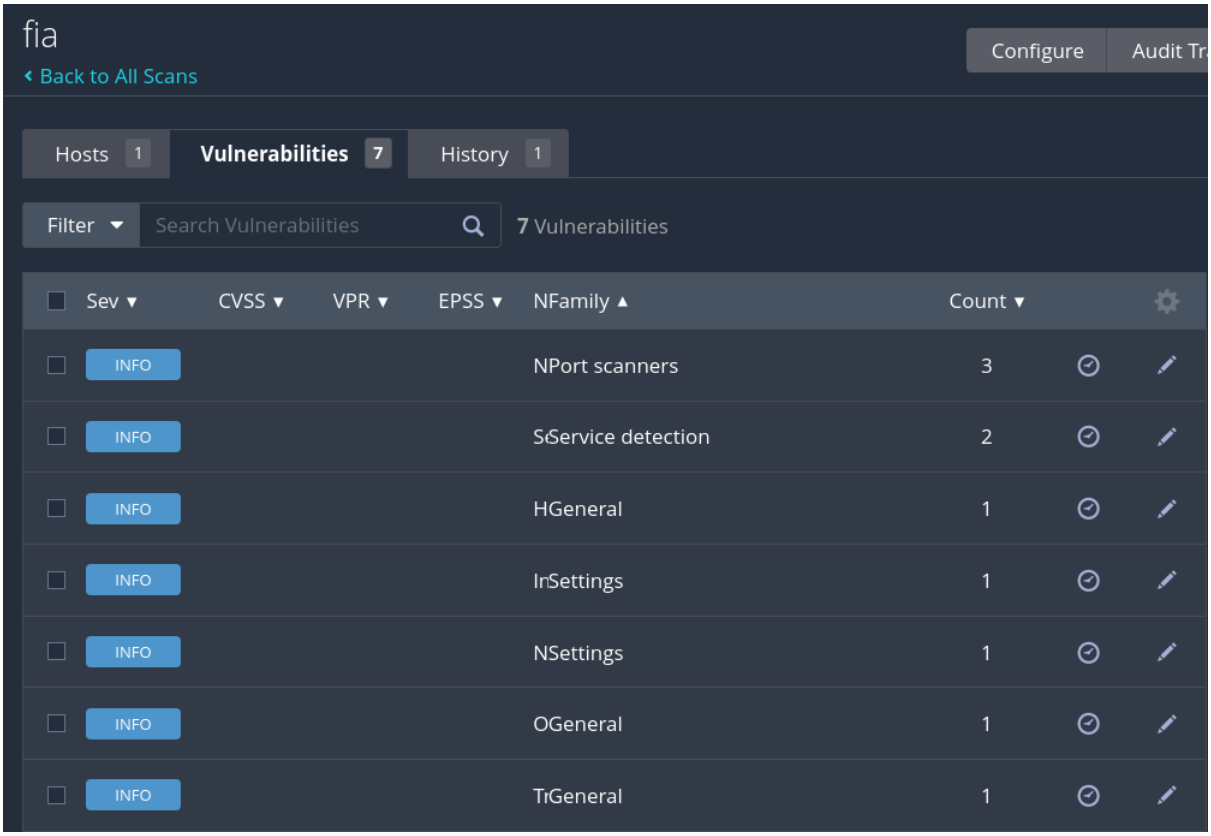
# Ahmed Umar

# Nessus-Report

# Vulnerability Assessment & Reverse Engineering

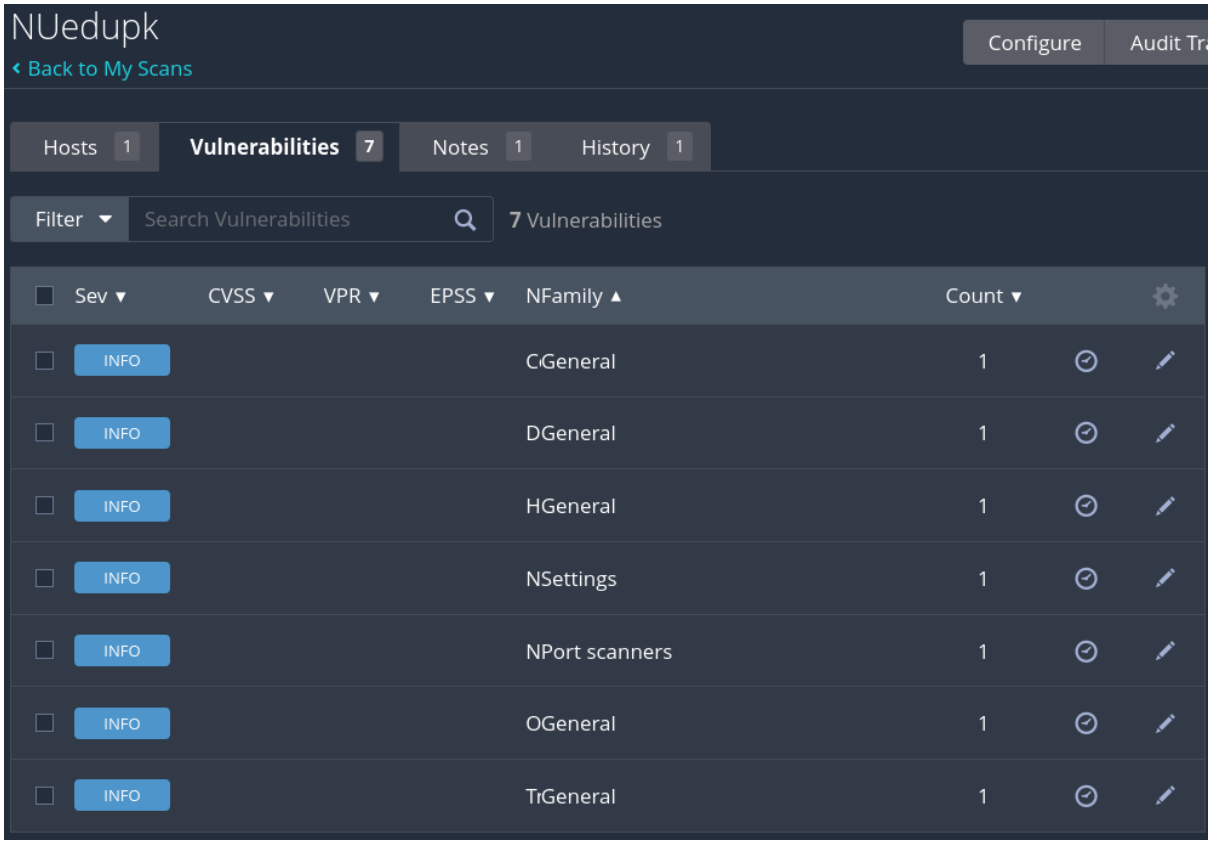



The Nessus report analyzes security vulnerabilities for the domain **fia.gov.pk** and provides scan details. However, this report does not list **critical, high, medium, or low** vulnerabilities, meaning there are **no major security threats** detected. It mostly includes **informational findings** such as:

1. **Host Fully Qualified Domain Name (FQDN) Resolution (Plugin ID: 12053)**
    - The system resolves the host's domain name.
    - **Mitigation:** No action is required; this is an informational finding.
2. **Nessus SYN Scanner (Plugin ID: 11219)**
    - It detects open **TCP ports**, specifically **port 443 (HTTPS)**.
    - **Mitigation:** Secure the system with an IP filter or a firewall.
3. **Nessus Scan Information (Plugin ID: 19506)**

- It provides details about the scan process, including Nessus version and scanning method.
- **Mitigation:** No mitigation required; this is for reporting purposes only.

4. **Traceroute Information (Plugin ID: 10287)**
    - Identifies the path (hops) data packets take to reach the target.
    - **Mitigation:** If you want to restrict traceroute results, configure **firewall rules** to block ICMP Time Exceeded messages




**Findings & Mitigation Steps:**

**1. Common Platform Enumeration (CPE) - (Plugin ID: 45590)**

- **Issue:** The scan identified the operating system as **Cisco PIX Firewall 7.0**.
- **Risk:** Attackers can use this information to find known vulnerabilities for this OS.
- **Mitigation:**
    - Upgrade to a **newer, supported version** of Cisco firewall software.

    - Disable services that expose OS details.
    - Use **firewall rules** to restrict information leakage.

---

**2. Device Type Detection - (Plugin ID: 54615)**

- **Issue:** The scan identified the remote system as a **firewall device** with 70% confidence.
- **Risk:** Attackers can use this knowledge to craft targeted attacks.
- **Mitigation:**
    - Configure the firewall to limit **response to fingerprinting attempts**.
    - Implement **security through obscurity** (e.g., modify banners, disable unused protocols).

---

**3. Host Fully Qualified Domain Name (FQDN) Resolution - (Plugin ID: 12053)**

- **Issue:** The system's **domain name is publicly resolvable** (host2021228.comsatshosting.com).
- **Risk:** Attackers can use this information to **identify hosting services** and potential vulnerabilities.
- **Mitigation:**
    - Consider using **private DNS records** for internal services.
    - Restrict **zone transfers** and **public DNS exposure**.

---

**4. Open TCP Port Detected - (Plugin ID: 11219)**

- **Issue: Port 5060 (SIP - Session Initiation Protocol) is open**.
- **Risk:** This port is commonly targeted for **VoIP hacking, call fraud, and DDoS attacks**.
- **Mitigation:**
    - **If VoIP services are not needed**, close **port 5060**.
    - **If VoIP is required**, use:
        - **SIP authentication & encryption (TLS, SRTP)**
        - **Firewall rules to limit SIP access to trusted IPs**
        - **Intrusion detection systems (IDS) to monitor VoIP traffic**

---

**5. OS Identification - (Plugin ID: 11936)**

- **Issue:** The system's **operating system (Cisco PIX 7.0) is identifiable**.
- **Risk:** Attackers can use this to find **known vulnerabilities**.
- **Mitigation:**
  - **Upgrade the OS** to a more **secure, supported** version.
  - **Disable OS version disclosures** in network responses.

---

**6. Traceroute Information - (Plugin ID: 10287)**

- **Issue:** The scan was able to perform **a traceroute** to the system.
- **Risk:** Traceroute data can help attackers **map the network topology**.
- **Mitigation:**
  - **Disable ICMP Time Exceeded messages** in firewall settings.
  - Restrict **ICMP traceroute requests** from external sources.

---

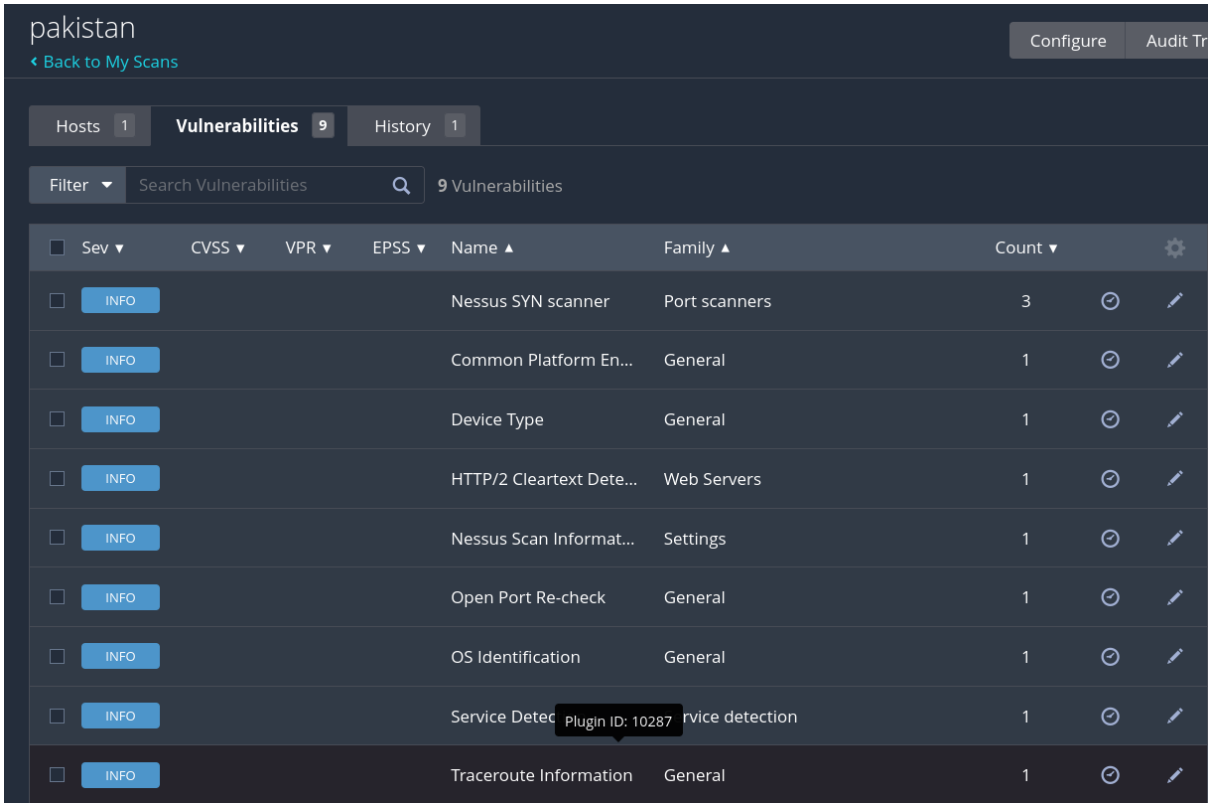
**7. Nessus Scan Information - (Plugin ID: 19506)**

- **Issue:** Provides scan details (Nessus version, plugin set, etc.).
- **Risk:** No security risk, but it's informational.
- **Mitigation:** No action needed.

---

**General Security Recommendations**

- **Apply System & Firmware Updates:** Upgrade Cisco PIX firewall to the latest supported version.
- **Enable a Strong Firewall Policy:** Block unnecessary ports and restrict open services.
- **Monitor Network Traffic:** Set up **Intrusion Detection Systems (IDS)** to detect malicious activities.
- **Restrict Public Exposure:** Minimize publicly accessible services unless required.
- **Use Strong Authentication:** Implement **multi-factor authentication (MFA)** for admin access.




This **Nessus vulnerability report** analyzes security risks for **pakistan.gov.pk**. It identifies **informational findings** rather than critical vulnerabilities. However, some **security improvements** are recommended to mitigate potential risks.

---

**Findings & Mitigation Steps**

**1. Common Platform Enumeration (CPE) - (Plugin ID: 45590)**

- **Issue:** The system was identified as **Cisco PIX Firewall 7.0**.
- **Risk:** Attackers can search for vulnerabilities in this specific firewall version.
- **Mitigation:**
  - **Upgrade to a newer firewall OS** (PIX 7.0 is outdated).
  - **Restrict system information leakage** by disabling banner disclosure.

---

**2. Device Type Detection - (Plugin ID: 54615)**

- **Issue:** The scan identified the system as a **firewall**.
- **Risk:** Attackers may target firewall-specific vulnerabilities.
- **Mitigation:**

- **Disable unnecessary services** that reveal device type.
- **Enable firewall hardening settings** to limit scanning responses.

---

**3. Open Ports Detected (SYN Scanner - Plugin ID: 11219)**

The report shows **several open ports**, which could be exploited if not secured properly.

**Open Ports & Risks:**

| Port | Service | Risk |
|---|---|---|
| 80 (TCP) | HTTP | Web-based attacks (e.g., SQL injection, XSS) |
| 443 (TCP) | HTTPS | Possible misconfigurations in SSL/TLS |
| 2000 (TCP) | Cisco SCCP | Exploitable if not properly secured |
| 5060 (TCP) | SIP (VoIP) | VoIP fraud & call interception |
| 8008 (TCP) | Alternative HTTP port | Potential web vulnerabilities |

**Mitigation for Open Ports:**

- **If a port is not needed, close it in the firewall.**
- **For essential ports (80, 443, 5060):**
  - Use **IP whitelisting** to restrict access.
  - **Enable SSL/TLS security** for HTTPS.
  - Monitor VoIP traffic for **fraudulent activity** on port 5060.
  - Use **Web Application Firewall (WAF)** to protect HTTP-based services.

---

**4. OS Identification - (Plugin ID: 11936)**

- **Issue:** The scan detected **Cisco PIX 7.0**.
- **Risk:** Attackers can target outdated OS vulnerabilities.
- **Mitigation:**
  - **Upgrade Cisco PIX to a newer version**.
  - **Block OS fingerprinting attempts** by configuring the firewall.

---

**5. Service Detection - (Plugin ID: 22964)**

- **Issue:** Services on **port 80 and 443** were identified but **closed the connection**.
- **Risk:** Attackers may attempt to bypass restrictions.
- **Mitigation:**
  - Ensure **TCP wrappers** and **firewall rules** are correctly set.
  - Disable unnecessary error messages **to prevent information leakage**.

---

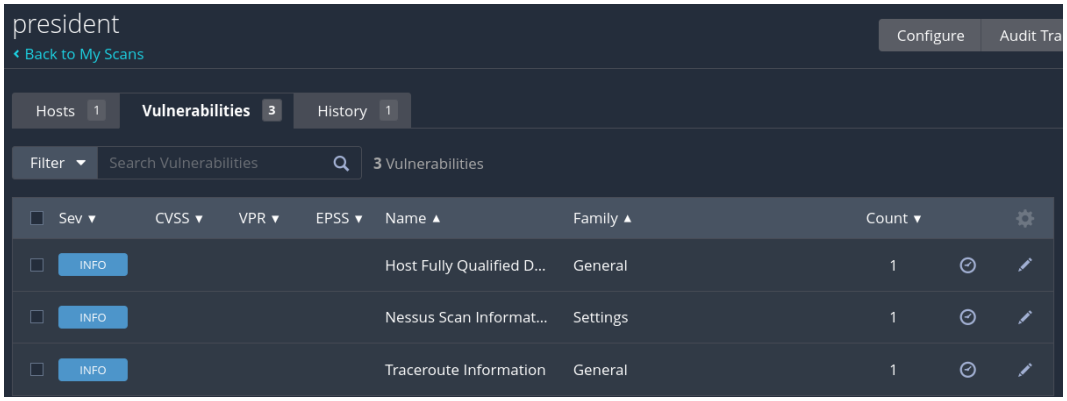
**6. Traceroute Information - (Plugin ID: 10287)**

- **Issue:** Traceroute was successful, revealing **network path details**.
- **Risk:** Attackers can **map the network** and find weak points.
- **Mitigation:**
  - **Disable ICMP Time Exceeded messages** in the firewall.
  - Use **firewall rules to block external traceroute attempts**.

---

**General Security Recommendations**

✓ **Upgrade Cisco PIX firewall** to a newer, more secure version.
✓ **Restrict open ports** & close unused ones to minimize attack risks.
✓ **Enable Web Application Firewall (WAF)** for ports 80 & 443.
✓ **Use VoIP security measures** (TLS encryption, SIP authentication) for port 5060.
✓ **Monitor & log network activity** to detect unauthorized access.
✓ **Disable system information leakage** to reduce reconnaissance risks.



**Detailed & Simple Explanation of Nessus Report (president.gov.pk)**

This Nessus scan report for **president.gov.pk** mainly contains **informational findings** rather than critical vulnerabilities. However, some security improvements can **reduce the risk of attacks**. Below is a breakdown of the key issues and how to mitigate them.

---

**Findings & Mitigation Steps**

**1. Common Platform Enumeration (CPE) - (Plugin ID: 45590)**

- **Issue:** The system was identified as **Cisco PIX Firewall 7.0**.
- **Risk:** Attackers can search for known vulnerabilities in this firewall.
- **Mitigation:**
  - **Upgrade to a newer firewall OS** (PIX 7.0 is outdated).
  - **Disable system information leakage** in the firewall settings.

---

**2. Device Type Detection - (Plugin ID: 54615)**

- **Issue:** The scan identified the system as a **firewall**.
- **Risk:** Attackers can use this information for targeted attacks.
- **Mitigation:**
  - **Restrict responses to scanning attempts** using firewall rules.
  - **Use firewall obfuscation techniques** to hide device type.

---

**3. Host Fully Qualified Domain Name (FQDN) Resolution - (Plugin ID: 12053)**

- **Issue:** The domain name www.president.gov.pk is publicly resolvable.
- **Risk:** Attackers can use this information to conduct **phishing** or **social engineering attacks**.
- **Mitigation:**
  - **Use private DNS records for internal services.**
  - **Restrict zone transfers** to prevent domain information leakage.

---

**4. Open Ports Detected (SYN Scanner - Plugin ID: 11219)**

The scan found **several open ports**, which could be **potential entry points for attackers**.

**Open Ports & Risks:**

| Port | Service | Risk |
|---|---|---|
| **80 (TCP)** | HTTP | Exposed web services may be vulnerable to attacks (e.g., SQL injection, XSS). |
| **443 (TCP)** | HTTPS | If SSL/TLS is not configured securely, it may be exploited. |
| **5060 (TCP)** | SIP (VoIP) | Can be targeted for **VoIP fraud, call hijacking, and DDoS attacks**. |

**Mitigation for Open Ports:**

- **Close unused ports** to minimize attack risks.
- **For essential ports (80, 443, 5060):**
  - **Enable a Web Application Firewall (WAF)** to protect against web-based threats.
  - **Use SSL/TLS encryption** with secure ciphers for HTTPS.
  - **Secure VoIP services** with:
    - **SIP authentication & encryption (TLS, SRTP).**
    - **Firewall rules to restrict access.**
    - **VoIP fraud detection tools.**

---

**5. OS Identification - (Plugin ID: 11936)**

- **Issue:** The scan detected **Cisco PIX 7.0**.
- **Risk:** Attackers can use this to find **known vulnerabilities**.
- **Mitigation:**
  - **Upgrade to a newer OS version.**
  - **Disable OS version disclosure** in network responses.

---

**6. Open Port Re-check - (Plugin ID: 10919)**

- **Issue:** Some previously open ports were found to be **closed or unresponsive**.
- **Risk:** Could indicate **an intrusion detection system (IDS) blocking scans** or **service instability**.
- **Mitigation:**
  - **Verify network stability** to ensure no essential services are impacted.
  - **Review firewall and IDS logs** to confirm if any security policies blocked the scan.

---

**7. Service Detection - (Plugin ID: 22964)**

- **Issue:** Services on **port 80 (HTTP) and 443 (HTTPS)** were detected.
- **Risk:** Attackers might attempt to exploit **web vulnerabilities**.
- **Mitigation:**
  - **Ensure all web applications are updated** with the latest security patches.
  - **Enable HTTP security headers** (e.g., Content Security Policy, HSTS).

---

**8. Traceroute Information - (Plugin ID: 10287)**

- **Issue:** The scan was able to perform a **traceroute**, revealing network path details.
- **Risk:** Attackers can **map the network** and find weak points.
- **Mitigation:**
  - **Block ICMP Time Exceeded messages** in the firewall.
  - **Restrict external traceroute requests** using firewall rules.

---

**General Security Recommendations**

✓ **Upgrade Cisco PIX firewall** to a newer, more secure version.
✓ **Close unnecessary ports** and **restrict access** to critical services.
✓ **Use a Web Application Firewall (WAF)** for ports **80 and 443**.
✓ **Secure VoIP communications** on **port 5060** using authentication & encryption.
✓ **Monitor network traffic & set up alerts** for **suspicious activity**.
✓ **Harden web servers** by implementing **strong security policies**

WindowsXP

‹ Back to My Scans

Configure | Audit Tr

Hosts 1 | Vulnerabilities 25 | Remediations 1 | History 1

Filter | Search Vulnerabilities | 25 Vulnerabilities

| Sev | CVSS | VPR | EPSS | Name | Family | Count |
|---|---|---|---|---|---|---|
| CRITICAL | 10.0 | | | Microsoft Windows X... | Windows | 1 |
| MIXED | ... | ... | ... | 19 Microsoft Windo... | Windows | 19 |
| HIGH | 7.3 | 6.6 | 0.0202 | SMB NULL Session Au... | Misc. | 1 |
| MIXED | ... | ... | ... | 2 SMB (Multiple Iss... | Misc. | 2 |
| LOW | 3.3 * | 4.2 | 0.2572 | Multiple Ethernet Driv... | Misc. | 1 |
| LOW | 2.1 * | 2.2 | 0.8939 | ICMP Timestamp Req... | General | 1 |
| INFO | ... | ... | ... | 8 SMB (Multiple Iss... | Windows | 9 |
| INFO | | | | Nessus SYN scanner | Port scanners | 5 |
| INFO | | | | DCE Services Enumer... | Windows | 4 |
| INFO | | | | Common Platform En... | General | 1 |
| INFO | | | | Device Type | General | 1 |
| INFO | | | | Ethernet Card Manufa... | Misc. | 1 |

This Nessus vulnerability scan **detected multiple critical vulnerabilities** on a **Windows XP machine**, including **remote code execution**, **SMB exploits**, and **unsupported OS risks**. Below is a breakdown of the findings and **how to mitigate the risks** effectively.

---

**Findings & Mitigation Steps**

**1. Windows XP is Unsupported (Plugin ID: 73182, 108797)**

- **Issue:** Windows XP support **ended in 2014**, meaning no new security updates are available.
- **Risk:** The system is vulnerable to multiple **exploits and malware (e.g., WannaCry, EternalBlue).**
- **Mitigation:**
  - **Upgrade to a supported OS** like **Windows 10 or 11**.
  - **If upgrading is not possible**, follow strict **network isolation and security hardening** (firewalls, limited internet access).

---

**2. MS08-067: Windows Server Service Remote Code Execution (Plugin ID: 34477)**

- **Issue:** A critical vulnerability in Windows XP allows **attackers to execute remote code**.
- **Risk:** Can be exploited using **Metasploit (EternalBlue)**, leading to **full system takeover**.
- **Mitigation:**
  - **Apply Microsoft Patch KB958644** Link.
  - **Disable SMBv1** to prevent lateral movement attacks.
  - **Restrict access to TCP port 445** using a firewall.

---

**3. MS09-001: Windows SMB Remote Code Execution (Plugin ID: 35362)**

- **Issue:** The SMB protocol has **memory corruption vulnerabilities** that allow **unauthenticated remote attacks**.
- **Risk:** Attackers can **execute code remotely or crash the system**.
- **Mitigation:**
  - **Apply Microsoft Patch KB958687** Link.
  - **Disable SMBv1** as recommended by **Microsoft and US-CERT**.
  - **Block SMB ports (TCP 445, 139 and UDP 137, 138)** on the firewall.

---

**4. MS17-010: EternalBlue SMB Exploit (Plugin ID: 97833)**

- **Issue:** This vulnerability was used in **WannaCry, Petya, and EternalRocks malware** attacks.
- **Risk:** Attackers can gain **full system control** remotely.
- **Mitigation:**
  - **Apply Microsoft Patch KB4013389** Link.
  - **Disable SMBv1 completely**.
  - **Restrict SMB traffic** by blocking TCP ports **445, 139** and UDP **137, 138** at the firewall.

---

**5. SMB NULL Session Authentication (Plugin ID: 26920)**

- **Issue:** Attackers can **connect to the system without a password** and gather system info.
- **Risk:** Can be used for **privilege escalation and network reconnaissance**.
- **Mitigation:**
  - **Disable NULL session authentication** in the Windows registry:

ini

CopyEdit

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]

"RestrictAnonymous"=dword:00000001

- **Enforce SMB authentication** and disable guest access.

---

**6. SMB Signing Not Required (Plugin ID: 57608)**

- **Issue:** SMB communication **is not signed**, allowing attackers to intercept and modify network traffic.
- **Risk:** Makes SMB connections vulnerable to **Man-in-the-Middle (MitM) attacks**.
- **Mitigation:**
  - **Enable SMB signing** using Group Policy:

pgsql

CopyEdit

Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

Enable: "Microsoft network client: Digitally sign communications (always)"

---

**7. SMBv1 Enabled (Plugin ID: 96982)**

- **Issue:** SMBv1 is **outdated and insecure**, making it **highly exploitable**.
- **Risk:** SMBv1 was used in **WannaCry and EternalBlue attacks**.
- **Mitigation:**
  - **Disable SMBv1** using PowerShell:

sql

CopyEdit

Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force

  - **Block SMB ports (445, 139, 137, 138)** on firewalls.

---

**8. ICMP Timestamp Disclosure (Plugin ID: 10114)**

- **Issue:** The system **responds to ICMP timestamp requests**, allowing attackers to estimate uptime.

- **Risk:** Can be used for **network fingerprinting and attacks**.
- **Mitigation:**
    - **Block ICMP timestamp requests** using a firewall rule:

pgsql

CopyEdit

netsh advfirewall firewall add rule name="Block ICMP Timestamps" dir=in action=block protocol=ICMPv4:13

---

**9. Open Ports Detected**

The system has **several open ports**, which can be **entry points for attacks**:

| Port | Service | Risk | Mitigation |
|---|---|---|---|
| 135 (TCP) | DCOM/RPC | Remote execution risk | Block this port if not needed |
| 139 (TCP) | NetBIOS | SMB vulnerabilities | Disable NetBIOS if not needed |
| 445 (TCP) | SMB | EternalBlue & WannaCry exploit | Block SMB traffic or upgrade OS |
| 123 (UDP) | NTP | Time-based attacks | Restrict NTP access to internal devices |

---

**General Security Recommendations**

✓ **Upgrade Windows XP to Windows 10/11** (Most important).
✓ **Disable SMBv1** and apply all **Microsoft security patches**.
✓ **Use a firewall to block TCP ports 445, 139, 135** and UDP ports **137, 138**.
✓ **Disable NULL session authentication** to prevent anonymous access.
✓ **Enforce SMB signing** to prevent tampering.
✓ **Restrict ICMP timestamps** to prevent system fingerprinting.
✓ **Monitor network traffic** for unusual activity.