

# Security Scan Report

Generated: 2025-11-09T01:17:07.834047Z

# AI-Generated Vulnerability Summary

## Chunk 1

## **\*\*Executive Summary\*\***

The recent vulnerability scan identified several critical security issues across two hosts, primarily involving unencrypted services and exposed remote access points. Immediate attention is required to mitigate high-risk vulnerabilities, particularly those related to Telnet, Remote Desktop, and SMB services. Implementing recommended remediation steps will significantly enhance the security posture of the affected systems.

## **\*\*Vulnerability Findings\*\***

### **\*\*Title: Unencrypted Telnet Service\*\***

Severity: High

Evidence: Telnet service is open on port 23.

Detailed Description: The Telnet service on the printer.local host is unencrypted, allowing potential attackers to intercept sensitive data transmitted over the network. This poses a significant risk as it can lead to unauthorized access and data breaches.

Remediation Steps: Disable Telnet and replace it with SSH for secure communication.

### **\*\*Title: Exposed Remote Desktop Protocol (RDP)\*\***

Severity: High

Evidence: Microsoft Terminal Services is open on port 3389.

Detailed Description: The Remote Desktop service is exposed, which can be exploited by attackers to gain unauthorized access to the system. It is recommended to implement a Virtual Private Network (VPN) or Multi-Factor Authentication (MFA) to secure access.

Remediation Steps: Restrict RDP access to trusted IPs, implement VPN, and enable MFA.

### **\*\*Title: Vulnerable SMB Service\*\***

Severity: High

Evidence: Samba version 4.3.11 is open on port 445.

Detailed Description: The SMB service can expose sensitive files and directories, especially if not properly configured. The current version is outdated and may contain known vulnerabilities.

Remediation Steps: Ensure all patches are applied, enable SMB signing, and consider upgrading to a more recent version of Samba.

### **\*\*Title: Potential Weakness in SSH Configuration\*\***

Severity: Medium

Evidence: OpenSSH version 7.6p1 is running on port 22.

Detailed Description: While SSH is a secure protocol, weak ciphers and password authentication can still pose risks. It is essential to review the configuration for any vulnerabilities.

Remediation Steps: Disable weak ciphers, enforce key-based authentication, and regularly update OpenSSH.

### **\*\*Title: HTTP Service Exposed on Printer\*\***

Severity: Medium

Evidence: Nginx version 1.14.0 is running on port 80.

Detailed Description: The HTTP service is available, which may expose default pages or outdated server configurations. This can lead to information disclosure or exploitation of known vulnerabilities.

Remediation Steps: Review the web server configuration, remove default pages, and ensure the server is updated.

**\*\*Title: Exposed MySQL Database\*\***

Severity: Medium

Evidence: MySQL version 5.7.31 is open on port 3306.

Detailed Description: The MySQL database is exposed to the internet, which can lead to unauthorized access if not properly secured.

Remediation Steps: Implement strong authentication, limit access to trusted IPs, and regularly update MySQL.

**\*\*Title: HTTP Service Exposed on Web Application\*\***

Severity: Medium

Evidence: Apache httpd version 2.4.18 is running on port 80.

Detailed Description: Similar to the printer's HTTP service, this web application may also expose sensitive information or be vulnerable to attacks if not properly configured.

Remediation Steps: Review server settings, remove default pages, and ensure the server is updated.

**\*\*Final Prioritized Checklist\*\***

1. Disable Telnet and implement SSH.
2. Secure Remote Desktop access with VPN and MFA.
3. Update and secure SMB service.
4. Review and strengthen SSH configuration.
5. Secure HTTP services on both hosts.
6. Protect MySQL database with strong authentication and access controls.

## Appendix: Raw Scan Data (JSON)

```
[
  {
    "host": "192.0.2.10",
    "hostname": "printer.local",
    "mac": "00:11:22:33:44:55",
    "port": "22",
    "protocol": "tcp",
    "state": "open",
    "service": "ssh",
    "product": "OpenSSH",
    "version": "7.6p1",
    "extra_info": "protocol 2.0",
    "scripts": [
      {
        "id": "ssh-hostkey",
        "output": "2048 SHA256:ABCDEF... (RSA)"
      }
    ]
  },
  {
    "host": "192.0.2.10",
    "hostname": "printer.local",
    "mac": "00:11:22:33:44:55",
    "port": "23",
    "protocol": "tcp",
    "state": "open",
    "service": "telnet",
    "product": null,
    "version": null,
    "extra_info": null,
    "scripts": []
  },
  {
    "host": "192.0.2.10",
    "hostname": "printer.local",
    "mac": "00:11:22:33:44:55",
    "port": "80",
    "protocol": "tcp",
    "state": "open",
    "service": "http",
    "product": "nginx",
    "version": "1.14.0",
    "extra_info": "Ubuntu",
    "scripts": [
      {
        "id": "http-title",
        "output": "Example Printer Web Interface"
      },
      {
        "id": "http-server-header",
        "output": "nginx/1.14.0 (Ubuntu)"
      }
    ]
  },
  {
    "host": "192.0.2.10",
    "hostname": "printer.local",
    "mac": "00:11:22:33:44:55",
    "port": "445",
    "protocol": "tcp",
```

```

    "state": "open",
    "service": "microsoft-ds",
    "product": "Samba",
    "version": "4.3.11",
    "extra_info": "Windows domain",
    "scripts": [
      {
        "id": "smb-os-discovery",
        "output": "OS: Windows 7 or Samba 4.3.11; Server: Samba 4.3.11"
      }
    ]
  },
  {
    "host": "192.0.2.10",
    "hostname": "printer.local",
    "mac": "00:11:22:33:44:55",
    "port": "3389",
    "protocol": "tcp",
    "state": "open",
    "service": "ms-wbt-server",
    "product": "Microsoft Terminal Services",
    "version": null,
    "extra_info": null,
    "scripts": []
  },
  {
    "host": "198.51.100.5",
    "hostname": "webapp.example.com",
    "mac": null,
    "port": "80",
    "protocol": "tcp",
    "state": "open",
    "service": "http",
    "product": "Apache httpd",
    "version": "2.4.18",
    "extra_info": null,
    "scripts": [
      {
        "id": "http-title",
        "output": "Vulnerable Demo App"
      },
      {
        "id": "http-headers",
        "output": "Server: Apache/2.4.18 (Ubuntu)"
      }
    ]
  },
  {
    "host": "198.51.100.5",
    "hostname": "webapp.example.com",
    "mac": null,
    "port": "3306",
    "protocol": "tcp",
    "state": "open",
    "service": "mysql",
    "product": "MySQL",
    "version": "5.7.31",
    "extra_info": null,
    "scripts": []
  }
]

```