Security Scan Report

Generated: 2025-11-09T01:29:37.836096Z

AI-Generated Vulnerability Summary

Chunk 1

Executive Summary: A security scan of the network has identified several vulnerabilities that require immediate attention. High-severity issues include unencrypted Telnet access, exposed Remote Desktop Protocol, and SMB services that could lead to unauthorized file access. Medium-severity findings involve potential weaknesses in SSH configurations and exposed HTTP services that may contain outdated or default content.

Finding 1: Telnet Service Exposure
Severity: High
Evidence: Telnet service is open on port 23.
Detailed Description: The Telnet service is unencrypted, making it susceptible to eavesdropping and man-in-the-middle attacks. It is recommended to replace Telnet with a more secure protocol such as SSH.
Remediation Steps: Disable Telnet service and configure SSH for remote access.

Finding 2: Remote Desktop Protocol Exposure
Severity: High
Evidence: Remote Desktop service is open on port 3389.
Detailed Description: The Remote Desktop Protocol (RDP) is exposed, which can allow unauthorized access to the system. It is advisable to implement a VPN or Multi-Factor Authentication (MFA) to secure access.
Remediation Steps: Restrict RDP access to trusted IPs, implement VPN, and enable MFA for RDP connections.

Finding 3: SMB Service Vulnerability
Severity: High
Evidence: SMB service is open on port 445, running Samba version 4.3.11.
Detailed Description: The SMB service can expose sensitive files and directories. Without proper patches and SMB signing, it poses a significant risk of data leakage and unauthorized access.
Remediation Steps: Ensure all patches are applied to Samba, enable SMB signing, and restrict access to necessary users only.

Finding 4: SSH Configuration Weakness
Severity: Medium
Evidence: SSH service is open on port 22, running OpenSSH version 7.6p1.
Detailed Description: The SSH service may be configured with weak ciphers or allow password authentication, which can be exploited by attackers.
Remediation Steps: Review and strengthen SSH configurations by disabling weak ciphers and enforcing key-based authentication.

Finding 5: HTTP Service Exposure on Printer
Severity: Medium
Evidence: HTTP service is open on port 80, running nginx version 1.14.0.
Detailed Description: The HTTP service may expose default pages or outdated content, which can be leveraged by attackers for exploitation.
Remediation Steps: Review the web server for default pages, ensure it is updated, and disable directory listing.

Finding 6: Database Exposure
Severity: Medium
Evidence: MySQL service is open on port 3306, running version 5.7.31.
Detailed Description: The MySQL database is exposed, which can lead to unauthorized access if not properly secured.
Remediation Steps: Implement strong authentication, limit access to trusted IPs, and ensure the database is not publicly accessible.

Finding 7: HTTP Service Exposure on Web Application
Severity: Medium
Evidence: HTTP service is open on port 80, running Apache httpd version 2.4.18.
Detailed Description: The HTTP service may expose default pages or outdated content, which can be leveraged by attackers for exploitation.
Remediation Steps: Review the web server for default pages, ensure it is updated, and disable directory listing.

Final Prioritized Checklist:
1. Disable Telnet and configure SSH for remote access.
2. Restrict RDP access, implement VPN, and enable MFA.
3. Apply patches to Samba, enable SMB signing, and restrict access.
4. Strengthen SSH configurations by disabling weak ciphers and enforcing key-based authentication.
5. Review and secure HTTP services on the printer and web application.
6. Implement strong authentication and limit access to the MySQL database.

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": []
  }
]
```