Security Scan Report

Generated: 2025-11-09T01:08:51.298245Z

AI-Generated Vulnerability Summary

Chunk 1

Executive Summary
A recent security scan identified several vulnerabilities across two hosts, primarily related to unencrypted services and exposed ports. High-severity issues include the use of Telnet and Remote Desktop Protocol (RDP) without adequate security measures. Immediate remediation is recommended to mitigate risks associated with unauthorized access and data exposure.

Vulnerability Findings

1. Telnet Service Exposure
- **Severity:** High
- **Evidence:**
- Host: 192.0.2.10
- Port: 23
- Service: Telnet
- State: Open
- **Detailed Description:** The Telnet service is unencrypted, allowing potential attackers to intercept sensitive data transmitted over the network. This poses a significant risk of unauthorized access and data breaches.
- **Remediation Steps:**
1. Disable the Telnet service.
2. Implement SSH (Secure Shell) as a secure alternative for remote access.

```
#### 2. Remote Desktop Protocol (RDP) Exposure
- **Severity:** High
- **Evidence:**
  - Host: 192.0.2.10
  - Port: 3389
  - Service: ms-wbt-server
  - Product: Microsoft Terminal Services
  - State: Open
- **Detailed Description:** The RDP service is exposed to the internet, which can be exploited by attackers to g
- **Remediation Steps:**
  1. Restrict RDP access to trusted IP addresses using a firewall.
  2. Implement a VPN for remote access.
  3. Enable Multi-Factor Authentication (MFA) for RDP sessions.

---

#### 3. SMB Service Vulnerability
- **Severity:** High
- **Evidence:**
  - Host: 192.0.2.10
  - Port: 445
  - Service: microsoft-ds
  - Product: Samba
  - Version: 4.3.11
```

```
  - State: Open
- **Detailed Description:** The SMB service is exposed, which can lead to unauthorized file access and potentia
- **Remediation Steps:**
  1. Ensure that the Samba service is updated to the latest version.
  2. Enable SMB signing to enhance security.
  3. Limit access to the SMB service to trusted users and networks.

---

#### 4. SSH Weakness
- **Severity:** Medium
- **Evidence:**
  - Host: 192.0.2.10
  - Port: 22
  - Service: ssh
  - Product: OpenSSH
  - Version: 7.6p1
- **Detailed Description:** The SSH service is operational, but it is essential to verify that weak ciphers and
- **Remediation Steps:**
  1. Review and configure SSH settings to disable weak ciphers.
  2. Enforce key-based authentication and disable password authentication.

---
```

5. HTTP Service Exposure (Printer)
- **Severity:** Medium
- **Evidence:**
- Host: 192.0.2.10
- Port: 80
- Service: http
- Product: nginx
- Version: 1.14.0
- **Detailed Description:** The HTTP service is available, which may expose default pages or outdated server configurations that could be exploited by attackers.
- **Remediation Steps:**
1. Check for and remove any default pages.
2. Ensure the nginx server is updated to the latest version.
3. Disable directory listing.

```
#### 6. Database Exposure
- **Severity:** Medium
- **Evidence:**
  - Host: 198.51.100.5
  - Port: 3306
  - Service: mysql
  - Product: MySQL
  - Version: 5.7.31
  - State: Open
- **Detailed Description:** The MySQL database is exposed to the internet, which can lead to unauthorized acces
- **Remediation Steps:**
  1. Implement strong authentication mechanisms for database access.
  2. Restrict database access to trusted IP addresses.
  3. Regularly update MySQL to the latest version.

---

#### 7. HTTP Service Exposure (Web Application)
- **Severity:** Medium
- **Evidence:**
```

```
  - Host: 198.51.100.5
  - Port: 80
  - Service: http
  - Product: Apache httpd
  - Version: 2.4.18
- **Detailed Description:** The Apache HTTP service is operational, which may expose default pages or outdated c
- **Remediation Steps:**
  1. Check for and remove any default pages.
  2. Ensure the Apache server is updated to the latest version.
  3. Disable directory listing.

---
```

Final Prioritized Checklist
1. Disable Telnet and implement SSH.
2. Secure RDP with VPN and MFA.
3. Update Samba and enable SMB signing.
4. Review SSH configurations for weak ciphers.
5. Secure HTTP services on both hosts by removing default pages and updating servers.
6. Restrict MySQL access and implement strong authentication.
7. Regularly review and update all services to their latest versions.

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": []
  }
]
```