NetHawk Security Report

Overall Security Assessment:

The network appears to have several security vulnerabilities and misconfigurations, making it an attractive target for potential attackers. The exposure of various services, including SMB, SSH, HTTP, and others, increases the attack surface. The presence of outdated software and potential vulnerabilities in services like OpenSSH and Apache HTTP Server further exacerbates the risk.

Detailed Service Analysis:

1. **192.168.11.1**:

 * Port 139: SMB service, likely Windows-based. The error message suggests a potential encoding issue, but it's unclear if this is a vulnerability.

 * Port 445: SMB service, likely Windows-based. This is a common port for SMB, but it's exposed externally, which is a security risk.

2. **192.168.11.2**:

 * Port 53: DNS service. This is a standard port for DNS, but it's unusual to see it exposed externally.

3. **192.168.11.128**:

 * Port 21: FTP service. This is an outdated protocol and should be replaced with a more secure alternative like SFTP.

 * Port 22: SSH service, version OpenSSH 6.6.1p1 (Ubuntu-2ubuntu2.13). This version has known vulnerabilities, such as CVE-2015-6565 (information disclosure) and CVE-2016-0777 (use-after-free).

* Port 80: HTTP service, version Apache/2.4.7 (Ubuntu). This version has known vulnerabilities, such as CVE-2014-0226 (SSL/TLS MITM vulnerability) and CVE-2017-15710 (optionsbleed).

* Port 631: CUPS service, version 1.7. This version has known vulnerabilities, such as CVE-2014-5021 (denial-of-service) and CVE-2015-1158 (arbitrary code execution).

* Port 3306: MySQL service. The error message suggests a potential encoding issue, but it's unclear if this is a vulnerability.

* Port 3500: WEBrick service, version 1.3.1 (Ruby/2.3.8/2018-10-18). This version has known vulnerabilities, such as CVE-2017-17742 (directory traversal) and CVE-2019-5420 (denial-of-service).

* Port 6697: IRC service. This is an unusual service to expose externally.

* Port 8080: Jetty service, version 8.1.7.v20120910. This version has known vulnerabilities, such as CVE-2013-2052 (denial-of-service) and CVE-2015-5254 (information disclosure).

Potential Attack Vectors:

1. Exploitation of SMB vulnerabilities on 192.168.11.1 and 192.168.11.128.

2. Exploitation of OpenSSH vulnerabilities on 192.168.11.128.

3. Exploitation of Apache HTTP Server vulnerabilities on 192.168.11.128.

4. Exploitation of CUPS vulnerabilities on 192.168.11.128.

5. Exploitation of WEBrick vulnerabilities on 192.168.11.128.

6. Brute-force attacks on SSH, FTP, and other services.

7. Scanning for potential vulnerabilities in other services.

Recommendations for Exploitation:

1. Perform a thorough vulnerability scan using tools like Nmap, Nessus, or OpenVAS.

2. Use exploit frameworks like Metasploit to test for known vulnerabilities in services like OpenSSH, Apache HTTP Server, and CUPS.

3. Attempt to brute-force passwords for SSH, FTP, and other services using tools like Hydra or John the Ripper.

4. Analyze network traffic to identify potential security issues.

Mitigation Strategies:

1. Restrict external access to services like SMB, SSH, and FTP.

2. Update OpenSSH, Apache HTTP Server, CUPS, and other services to the latest versions.

3. Implement strong password policies and enable two-factor authentication.

4. Configure firewalls to restrict incoming traffic to only necessary ports and services.

5. Regularly perform vulnerability scans and penetration testing to identify security issues.

6. Implement a patch management process to ensure timely updates of software and services.

Historical Context:

Without historical data, it's difficult to determine if there have been changes in service exposure or vulnerabilities over time.

Anomalies Detected:

1. The presence of an IRC service on port 6697 is unusual.

2. The exposure of SMB services on 192.168.11.1 and 192.168.11.128 is a security risk.

3. The use of outdated software and services, such as OpenSSH 6.6.1p1 and Apache HTTP Server 2.4.7, increases the attack surface.