Final Security Report

This report provides an overview of the security posture of the host at **192.168.1.4** following the implementation of recommended remediation measures. The initial vulnerability scan, conducted using the **Nessus tool**, identified several critical and high-severity risks, including outdated software, insecure protocols, and weak configurations. Significant progress has been made in patching vulnerable services and systems. However, certain risks, particularly those related to End-of-Life (EoL) software, remain and require further action.

Implemented Security Measures & Improvements

Based on the initial findings from the Nessus scan, the following actions were taken to address the identified vulnerabilities:

- **Samba Badlock Vulnerability:** The Samba service was successfully upgraded to a patched version (4.4.2 or later), mitigating the risk of man-in-the-middle attacks and unauthorized access.
- **ISC BIND Service Downgrade / Reflected DoS:** The ISC BIND service was upgraded to a fixed version 9.11.19, resolving the denial-of-service and reflection attack vulnerabilities.
- **VNC Server 'password' Password:** The VNC server's weak password was changed to a strong, complex password.
- **phpMyAdmin SQL Injection:** The outdated phpMyAdmin application was upgraded to a secure version 4.9.11, patching the SQL injection vulnerability.
- **Apache Tomcat AJP Connector (Ghostcat):** The Apache Tomcat server was upgraded to a patched version 9.11,which resolved the Ghostcat vulnerability.
- **SSL v2 and v3 Protocol Detection:** The SSL/TLS configuration was updated to disable insecure protocols (SSL 2.0 and SSL 3.0), ensuring that connections only use TLS 1.2 or higher.

Remaining Risks & Outstanding Actions

Despite the successful remediation of several key issues, the following critical risks must still be addressed:

- **Canonical Ubuntu Linux End-of-Life (EoL):** The host is still running Ubuntu Linux version 8.04.x, which is no longer supported by the vendor. This is the most critical outstanding risk as the operating system receives no security patches.
    - **Required Action:** The operating system must be upgraded to a currently supported version of Ubuntu Linux.
- **Apache Tomcat End-of-Life (EoL):** The host is running Apache Tomcat version 5.5, which reached its End-of-Life in 2012.
    - **Required Action:** The Apache Tomcat service must be upgraded to a currently supported version.
- **Debian OpenSSH/OpenSSL Weakness:** All cryptographic keys generated on the host are considered compromised due to a known bug in the Debian/Ubuntu random number generator.
    - **Required Action:** All cryptographic keys (including SSH, SSL, and OpenVPN) must be regenerated on a different, secure system and replaced on the host.

Final Recommendation

While significant progress has been made in improving the security posture of the host at 192.168.1.4, the presence of multiple End-of-Life software components and compromised cryptographic keys presents a severe and ongoing threat. It is highly recommended to prioritize the **upgrade of the entire operating system** and the **regeneration of all cryptographic keys** to fully secure the system.