Nemesys Security Report

Executive Summary

The security analysis of the provided system enumeration data reveals several critical vulnerabilities and configuration issues that pose a significant risk to the system's security. The overall risk rating is High, with multiple areas of concern that require immediate attention.

The primary areas of concern include outdated kernel versions, misconfigured services, and weak system configurations. These vulnerabilities can be exploited by attackers to gain unauthorized access, execute malicious code, or disrupt system operations.

Introduction

This security report is based on the analysis of system logs, configurations, and active services of a Linux-based system, specifically an Ubuntu 14.04 LTS server. The purpose of this evaluation is to identify potential security risks and provide recommendations for improving the system's security posture.

System Overview

The system is running Ubuntu 14.04 LTS with kernel version 3.13.0-24-generic. This kernel version is outdated and has known vulnerabilities, including CVE-2014-3153, which can be exploited to gain elevated privileges.

Identified Vulnerabilities and Risks

1. **Kernel Vulnerabilities**: The outdated kernel version is vulnerable to multiple exploits, including CVE-2014-3153, which can be used to gain elevated privileges.
2. **Misconfigured Services**: The system has multiple unnecessary services running, including the Apache web server, which can be exploited by attackers to gain access to the system.
3. **Weak System Configurations**: The system has weak file permissions, allowing unauthorized access to sensitive files and directories.

Insecure Configurations

1. **Improper File Permissions**: The system has weak file permissions, allowing unauthorized access to sensitive files and directories.
2. **Exposed Ports**: The system has open ports, including port 80, which can be exploited by attackers to gain access to the system.

Running Services Analysis

1. **Unnecessary Services**: The system has multiple unnecessary services running, including the Apache web server, which can be exploited by attackers to gain access to the system.
2. **Outdated Software**: The system is running outdated software, including the Apache web server, which can be exploited by attackers to gain access to the system.

Network Security Assessment

1. **Open Ports**: The system has open ports, including port 80, which can be exploited by attackers to gain access to the system.

2. **Firewall Settings**: The system's firewall settings are not configured to block incoming traffic, allowing attackers to access the system.

Elevated Accounts and Potential Malware Detection

1. **Elevated Accounts**: The system has multiple elevated user accounts, including the root user, which can be exploited by attackers to gain elevated privileges.
2. **Potential Malware Detection**: The system shows signs of potential malware infection, including unusual process behaviors and system crashes.

Security Recommendations

1. **Apply Patches**: Apply the latest security patches to the kernel and system software to address known vulnerabilities.
2. **Configure Firewalls**: Configure the system's firewall to block incoming traffic and restrict access to sensitive ports.
3. **Secure User Permissions**: Secure user permissions to prevent unauthorized access to sensitive files and directories.
4. **Disable Unnecessary Services**: Disable unnecessary services, including the Apache web server, to prevent exploitation by attackers.
5. **Implement Malware Detection**: Implement malware detection tools to identify and remove potential malware infections.

Detected Anomalies

1. **Unknown Services**: The system has unknown services running, which may indicate malicious

activity or misconfigurations.

2. **Unusual Log Entries**: The system's log files show unusual entries, including failed login attempts and system crashes, which may indicate malicious activity.

Conclusion

The system's security posture is critical, with multiple areas of concern that require immediate attention. The identified vulnerabilities and configuration issues can be exploited by attackers to gain unauthorized access, execute malicious code, or disrupt system operations. It is essential to address these issues by applying patches, configuring firewalls, securing user permissions, disabling unnecessary services, and implementing malware detection tools to enhance system security and reduce potential risks.