International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN (Online): 3048-7722
Volume 2, Issue 6, Nov-Dec- 2024, PP: 1-15

Vulnerability Mapping in Unix Servers Using Tenable and Log Correlation

Varun Deshmukh, Ananya Paul, Jatin Mehta, Swati Tripathi
Government Science College, Bengaluru, India

***Abstract* – In today's evolving digital ecosystem, ensuring the security of Unix-based servers is vital for the integrity of enterprise infrastructures. Vulnerability mapping serves as a crucial technique to identify, assess, and mitigate potential security risks before they can be exploited. This paper provides a comprehensive review of vulnerability mapping approaches in Unix environments, focusing on the integration of Tenable's vulnerability scanning tools—particularly Nessus—and log correlation methods. By leveraging automated scanning and advanced log analytics, organizations can proactively detect known vulnerabilities, monitor suspicious activity, and respond effectively to threats. The study emphasizes the value of combining these technologies to create a robust and responsive security posture for Unix systems.**

Keywords – : Vulnerability Mapping, Unix Servers, Tenable, Nessus, Log Correlation, Security Monitoring, Vulnerability Scanning, Incident Response.

I. INTRODUCTION

In today's fast-paced digital world, managing vulnerabilities in IT infrastructures is a critical task for system administrators, particularly for Unix-based servers. These servers host a wide variety of applications and services that must remain secure, resilient, and compliant with various security standards. A significant challenge for administrators is the ability to identify, prioritize, and mitigate vulnerabilities before they are exploited by malicious actors. Vulnerability mapping provides an essential approach to identifying and addressing these weaknesses, helping to ensure that security measures are robust and comprehensive.

Two powerful tools that can be used for vulnerability mapping in Unix servers are Tenable and log correlation techniques. Tenable provides vulnerability scanning capabilities through its suite of products, such as Nessus, which identifies and assesses vulnerabilities in Unix systems. Log correlation tools, on the other hand, allow for the aggregation and analysis of logs from different sources to identify suspicious activity and correlate events that may indicate security weaknesses or breaches.

This paper explores the process of vulnerability mapping in Unix servers using Tenable's vulnerability scanning tools and the power of log correlation. We will discuss how to integrate these technologies to build a comprehensive security framework that helps administrators monitor, detect, and respond to vulnerabilities and security incidents. The goal is to provide a structured approach to managing vulnerabilities in Unix servers and protecting critical infrastructure from potential threats.

II. OVERVIEW OF VULNERABILITY MAPPING IN UNIX SERVERS

Vulnerability mapping refers to the process of identifying, categorizing, and prioritizing security weaknesses within an IT infrastructure. The primary objective of vulnerability mapping is to ensure that known vulnerabilities are addressed in a timely manner to mitigate the risk of exploitation by attackers. In the case of Unix servers, this involves evaluating the server's operating system, installed software, and network configurations for vulnerabilities that could be targeted by attackers.

Unix servers are widely used in many organizations, hosting everything from web applications to databases, making them prime targets for cyberattacks. The Unix operating system is highly flexible, and its open-source nature means that security vulnerabilities can be introduced via misconfigurations, outdated software, or inadequate patching practices. Given the complexity of Unix systems and the variety of attack vectors available to hackers, vulnerability mapping becomes a fundamental activity in any Unix-based environment.

The two primary methods for vulnerability mapping are:

- Automated vulnerability scanning using tools like Tenable to identify known vulnerabilities and provide a detailed inventory of potential risks.
- Log correlation, which involves analyzing logs from various systems (servers, firewalls, intrusion detection systems) to identify anomalous patterns or behaviors that might indicate security breaches or weaknesses.

By combining these techniques, organizations can achieve comprehensive visibility into their Unix server environments and address vulnerabilities before they become exploitable.

III. TENABLE FOR VULNERABILITY SCANNING IN UNIX SERVERS

Tenable provides advanced vulnerability scanning solutions, with Nessus being one of its most well-known products. Nessus is an automated scanner that helps system

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN (Online): 3048-7722
Volume 2, Issue 6, Nov-Dec- 2024, PP: 1-15

administrators identify vulnerabilities in Unix servers, such as missing patches, misconfigurations, and security flaws in installed software. It scans systems for a wide range of vulnerabilities, including network vulnerabilities, OS vulnerabilities, and application vulnerabilities, and generates detailed reports that administrators can use to prioritize and address the issues.

Vulnerability Scanning with Nessus

Nessus performs an in-depth scan of Unix servers, looking for common vulnerabilities and exposures (CVEs), misconfigurations, and potential security weaknesses. It checks for:

- Unpatched software: Nessus scans for software that may be outdated or not properly patched, which could be a potential entry point for attackers.
- Configuration issues: It identifies incorrect or weak configurations, such as improper user permissions or weak passwords.
- Unnecessary services: Nessus can identify unnecessary or unused services running on the Unix system that could be exploited.
- Security flaws in applications: Nessus checks for known vulnerabilities in applications running on the server, such as database servers, web servers, or other critical services.

Automated Vulnerability Assessment

One of the key benefits of using Tenable products like Nessus for vulnerability mapping is automation. Nessus automates the entire vulnerability assessment process, making it easier for administrators to identify potential weaknesses without having to manually inspect each system. The automation also ensures consistency across scans, as the same set of criteria is used for every scan.
Once the scan is complete, Nessus provides a report that highlights vulnerabilities by their severity (critical, high, medium, low), enabling administrators to prioritize remediation efforts. The report also provides suggestions for addressing each identified vulnerability, such as applying patches, reconfiguring settings, or disabling certain services.

Continuous Scanning and Monitoring

Vulnerabilities in Unix systems are constantly emerging, and ensuring that systems remain secure requires continuous monitoring. Nessus allows administrators to schedule regular scans of Unix servers, ensuring that new vulnerabilities are identified and addressed promptly. This continuous monitoring helps ensure that any system updates, software patches, or new vulnerabilities are quickly detected, reducing the window of exposure to threats.

IV. LOG CORRELATION FOR ENHANCED VULNERABILITY MAPPING

While vulnerability scanners like Nessus are powerful tools for identifying known vulnerabilities, they are not always sufficient for detecting potential threats that do not yet have publicly disclosed vulnerabilities. In such cases, log correlation provides an additional layer of security by helping administrators analyze logs from various systems to identify patterns that could indicate security issues or vulnerabilities.

What is Log Correlation?

Log correlation involves aggregating and analyzing logs from multiple sources—such as system logs, application logs, security logs, and network logs—to detect suspicious activity or inconsistencies that might indicate a vulnerability or security breach. Logs typically contain timestamps, user actions, and error messages that can provide valuable insight into the behavior of systems. By correlating these logs, administrators can identify patterns or anomalies that suggest vulnerabilities or attacks.
For example, a pattern of failed login attempts from an unusual IP address or a sudden spike in traffic to a specific port may indicate a brute-force attack or an attempt to exploit a vulnerability. Log correlation tools help highlight these anomalies and alert administrators before an attack succeeds or a vulnerability is exploited.

Benefits of Log Correlation for Vulnerability Mapping

Log correlation can enhance vulnerability mapping in Unix servers by identifying:

- Unusual system behavior: Logs often reveal unexpected behaviors, such as increased CPU usage or changes in file permissions, which may signal an attempted exploit of a vulnerability.
- Unauthorized access attempts: Log correlation can detect unauthorized access to system files, which may indicate an attempt to exploit a weakness in the system.
- Indicator of compromise (IoC): By correlating logs from different sources, log correlation tools can identify indicators of compromise, such as IP addresses involved in previous attacks or known malicious payloads.

By combining log correlation with vulnerability scanning, administrators gain a more comprehensive view of their server environment. They can map known vulnerabilities (via Nessus scans) alongside suspicious activities detected through log correlation, enabling a more proactive approach to security.

Using Log Correlation Tools

Popular log correlation tools, such as Splunk, Elastic Stack (ELK), and SolarWinds, can be integrated with Nessus and

other vulnerability management systems to provide real-time alerts, dashboards, and comprehensive reports on system activity. These tools consolidate log data and apply correlation rules to identify potential security risks, enabling administrators to respond more quickly to incidents.

V. INTEGRATING TENABLE AND LOG CORRELATION FOR COMPREHENSIVE VULNERABILITY MAPPING

While both Tenable (via Nessus) and log correlation tools are valuable individually, their integration provides a more holistic approach to vulnerability mapping in Unix servers. Vulnerability scanners focus on identifying known issues, while log correlation offers real-time monitoring of system behavior and potential vulnerabilities that might not yet be documented.

Correlating Scan Results with Log Data

By correlating the results of vulnerability scans with log data, administrators can get a clearer picture of the security posture of Unix servers. For example, if Nessus identifies a vulnerability in a specific service running on a Unix server, log correlation tools can be used to track whether there has been any unusual access to that service or any indications of an attempted exploit.

Proactive Incident Response

Combining vulnerability scans with log correlation allows for a more proactive incident response. Rather than waiting for an attack to occur, organizations can use log data to detect early signs of suspicious behavior and use the vulnerability scan data to assess which weaknesses could be exploited. This combined approach allows security teams to prioritize remediation efforts more effectively and take action before critical vulnerabilities are exploited.

Enhanced Reporting and Compliance

For organizations that need to comply with regulations such as HIPAA, PCI-DSS, or SOX, the integration of Nessus and log correlation tools ensures that they can provide comprehensive reports on their security posture. These reports can demonstrate that known vulnerabilities have been addressed and that suspicious activities have been detected and investigated, providing a clear audit trail for compliance audits.

VI. CHALLENGES AND BENEFITS OF VULNERABILITY MAPPING

Challenges

One of the main challenges in vulnerability mapping is data volume. Both vulnerability scanning and log correlation generate large amounts of data that must be managed and analyzed. Administrators must ensure that their vulnerability scanning schedules are appropriately managed and that logs are collected and retained efficiently. Additionally, the complexity of Unix server environments and the sheer number of potential vulnerabilities can make it difficult to prioritize risks effectively.

Benefits

The integration of Tenable and log correlation tools offers several benefits, including improved security posture, enhanced proactive detection of vulnerabilities, and the ability to meet compliance requirements. By using automated tools to continuously monitor, detect, and address vulnerabilities and suspicious activities, organizations can reduce their exposure to cyberattacks and improve overall system integrity.

VII. CONCLUSION

Vulnerability mapping is an essential part of securing Unix servers, and the combination of Tenable's vulnerability scanning tools and log correlation technologies offers a comprehensive solution. By automating the detection of known vulnerabilities through vulnerability scanning and using log correlation to identify suspicious activities, organizations can proactively address vulnerabilities, improve security, and ensure compliance with regulatory requirements. As the landscape of cyber threats continues to evolve, integrating these tools provides a robust security framework that enhances the resilience of Unix-based environments against emerging threats.

REFERENCES

1. Namunaba, F. M. (2017). An evaluation of network vulnerability assessment tools (Doctoral dissertation).
2. Chauhan, A. S. (2018). Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus. Packt Publishing Ltd.
3. Alzahrani, M. E. (2018, March). Auditing Albaha University network security using in-house developed penetration tool. In Journal of Physics: Conference Series (Vol. 978, No. 1, p. 012093). IOP Publishing.
4. Joshi, R. C., Pilli, E. S., Joshi, R. C., & Pilli, E. S. (2016). Network forensic tools. Fundamentals of Network Forensics: A Research Perspective, 71-93.
5. Quadrant, M. (2016). Magic quadrant for security information and event management. Magic Quadrant.
6. Gawron, M., Cheng, F., & Meinel, C. (2017, April). PVD: Passive vulnerability detection. In 2017 8th International Conference on Information and

Communication Systems (ICICS) (pp. 322-327). IEEE.

7. Wang, L., Jajodia, S., Singhal, A., Singhal, A., & Ou, X. (2017). Security risk analysis of enterprise networks using probabilistic attack graphs (pp. 53-73). Springer International Publishing.
8. McConnell Jr, J. P. (2020). UNIX Administrator Information Security Policy Compliance: The Influence of a Focused Seta Workshop and Interactive Security Challenges on Heuristics and Biases (Doctoral dissertation, Nova Southeastern University).
9. Madamanchi, S. R. (2021). Linux server monitoring and uptime optimization in healthcare IT: Review of Nagios, Zabbix, and custom scripts. International Journal of Science, Engineering and Technology, 9(6), 1–8.
10. Madamanchi, S. R. (2021). Disaster recovery planning for hybrid Solaris and Linux infrastructures. International Journal of Scientific Research & Engineering Trends, 7(6), 1–8.
11. Madamanchi, S. R. (2021). Mastering enterprise Unix/Linux systems: Architecture, automation, and migration for modern IT infrastructures.
12. Madamanchi, S. R. (2022). The rise of AI-first CRM: Salesforce, copilots, and cognitive automation.
13. Madamanchi, S. R. (2023). Efficient Unix system management through custom Shell, AWK, and Sed scripting. International Journal of Scientific Development and Research, 8(9), 1295–1314.
14. Vanharanta, J. (2017). Integrating Attack Graph Analysis System in Semi-Isolated Network Environment.
15. Coffey, K., Smith, R., Maglaras, L., & Janicke, H. (2018). Vulnerability analysis of network scanning on SCADA systems. Security and Communication Networks, 2018(1), 3794603.
16. Johansen, G., Allen, L., Heriyanto, T., & Ali, S. (2016). Kali Linux 2–Assuring Security by Penetration Testing. Packt Publishing Ltd.
17. Lee, N. M. Z., Ooi, S. Y., Lee, Y. K., & Pang, Y. H. ALabeled NETWORK-BASED ANOMALY INTRUSION DETECTION SYSTEM (IDS) DATASET. SECURITY AND AUTHENTICATION, 181.