MIT World Peace University

Attack Research and Documentation
Fourth Year B. Tech, Semester 8

Log Analysis

Lab Assignment 2 Report

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 15

February 24, 2025

Contents

1 Executive Summary

- **Objective:** The purpose of this log analysis is to investigate unauthorized access attempts and potential privilege escalation incidents within the system. The analysis focuses on identifying security threats, compliance violations, and performance anomalies.
- **Key Findings:**
  - Multiple unauthorized access attempts to the `/admin/config` endpoint were detected, all resulting in `403 Forbidden` responses.
  - Several users repeatedly attempted to access restricted areas, potentially indicating privilege escalation attempts.
  - Unauthorized access attempts were observed across multiple timestamps and originated from different users and IP addresses.
- **Recommendations:**
  - Implement stricter access controls for the `/admin/config` endpoint, including IP whitelisting and multi-factor authentication (MFA).
  - Monitor and block suspicious IPs after repeated failed authorization attempts.
  - Set up automated alerts to detect unauthorized access attempts in real-time.
  - Conduct security awareness training for users to prevent accidental privilege escalation attempts.

2 Scope of Analysis

- **Date Range:** 27/Jan/2025 - 28/Jan/2025
- **Systems Analyzed:** Web application servers handling authentication and administrative access.
- **Log Sources:** Apache access logs were analyzed to detect unauthorized access attempts and privilege escalation incidents.
- **Tools Used:** The log file was manually reviewed using text processing tools such as `grep` and `awk`, along with visualization using log analysis frameworks.

3 Findings

3.1 Finding #1: Unauthorized Access Attempt to Admin Configuration

3.1.1 Description

Multiple users attempted to access the `/admin/config` endpoint and received `403 Forbidden` responses. This indicates unauthorized access attempts to a restricted area, potentially a privilege escalation attempt.

3.1.2 Affected Systems/Users

- **IP 192.168.1.21** (Leo) – 28/Jan/2025 08:14:14
- **IP 192.168.1.13** (Dave) – 28/Jan/2025 10:44:09
- **IP 192.168.1.27** (Rachel) – 28/Jan/2025 10:46:11
- **IP 192.168.1.37** (Beth) – 28/Jan/2025 13:35:25
- **IP 192.168.1.36** (Andy) – 28/Jan/2025 19:17:13
- **IP 192.168.1.27** (Rachel) – 28/Jan/2025 19:43:53
- **IP 192.168.1.29** (Tom) – 28/Jan/2025 20:16:55

3.1.3 Timestamp

Various timestamps on January 28, 2025, from early morning to late evening.

3.1.4 Severity

High – Unauthorized attempts to access admin configurations could indicate an insider threat or an external attacker trying to gain higher privileges.

3.1.5 Evidence

Example log entry:

```
192.168.1.21 - leo [28/Jan/2025:08:14:14 +0000]
 "GET /admin/config HTTP/1.1" 403 4430 "-" "Mozilla/5.0"
```

Please refer to the **Appendix** (A.1) for more raw log entries.

3.1.6 Root Cause Analysis

- These requests likely came from users who lacked administrative privileges.
- It could be due to manual attempts to access restricted areas, automated scanning, or a misconfigured permission issue.

3.1.7 Impact

- Potential security risk if an attacker finds a vulnerability to bypass access controls.
- Compliance concerns for sensitive configuration files being targeted.
- Increased server load from unauthorized access attempts.

3.1.8 Recommendation

1. **Review User Permissions:** Ensure only authorized users can access `/admin/config`.
2. **Implement Access Controls:** Restrict the `/admin/config` endpoint further with IP whitelisting or multi-factor authentication (MFA).
3. **Monitor and Block Suspicious IPs:** If a user repeatedly fails authorization, temporarily block the IP.
4. **Log and Alert Security Teams:** Set up automated alerts for unauthorized access attempts to admin areas.
5. **User Education:** If these attempts were from legitimate users, educate them on access policies to prevent accidental unauthorized attempts.

3.2 Finding #2: Unusual Remote Desktop (RDP) Access Attempts

3.2.1 Description

Multiple attempts were made to access port `3389` (RDP) from various internal IPs (`192.168.1.100`, `192.168.1.102`, `192.168.1.101`). Some attempts were **blocked**, while others were **allowed**, raising concerns about unauthorized or unexpected RDP sessions.

3.2.2 Affected Systems/Users

- **192.168.1.100** – Multiple attempts, both **blocked** and **allowed**.
- **192.168.1.101** – Several attempts, mostly **blocked**.
- **192.168.1.102** – Attempted connections, **allowed and blocked** inconsistently.

3.2.3 Timestamp

January 27, 2025, 20:50:17 UTC (all events occurred at the same second, suggesting scripted or automated behavior).

3.2.4 Severity

High – Unauthorized or unexpected RDP access attempts can indicate an internal security threat or an external attack (e.g., brute force attempts or lateral movement by malware).

3.2.5 Evidence

Example log entries:

```
2025-01-27 20:50:17 | Event ID: 5152 | Source IP: 192.168.1.100
| Destination Port: 3389 | Action: BLOCKED
```

Please refer to the **Appendix** (A.1) for more raw log entries.

3.2.6 Root Cause Analysis

- The rapid succession of **allowed and blocked** RDP attempts indicates potential **automated access attempts** (e.g., a script, malware, or unauthorized user testing access).
- If these systems are not authorized RDP clients, an **internal security breach** or **misconfigured firewall rules** could be responsible.

3.2.7 Impact

- **Security Risk:** Potential **unauthorized remote access**, allowing attackers to gain control over critical systems.
- **Compliance Violation:** Unauthorized access to sensitive systems may violate internal security policies and regulatory requirements.
- **Network Anomaly:** Repeated blocked and allowed attempts could indicate **misconfigured firewall rules** or **incomplete security policies**.

3.2.8 Recommendation

1. **Review RDP Access Logs:** Identify authorized vs. unauthorized access attempts.
2. **Restrict RDP Usage:** Disable **RDP access** unless explicitly required. If needed, use a **VPN** or **Zero Trust Access**.
3. **Enforce Multi-Factor Authentication (MFA):** Require MFA for all remote access sessions.
4. **Investigate Firewall Rules:** Ensure consistent security policies to prevent unauthorized access.
5. **Monitor and Alert on RDP Attempts:** Set up **SIEM alerts** to detect and block repeated or unusual RDP attempts.
6. **Check for Malware or Unauthorized Scripts:** Scan affected machines for signs of unauthorized processes or automation tools.

3.3 Finding #3: Suspicious External RDP and SSH Traffic

3.3.1 Description

The firewall logs indicate **multiple Remote Desktop Protocol (RDP) and Secure Shell (SSH) connection attempts** from an **external IP (203.0.113.45)** to an internal network (`10.0.0.1`). Some of these attempts were **allowed**, while others were **dropped**, suggesting inconsistent firewall rules or unauthorized access attempts.

3.3.2 Affected Systems/Users

- **Source IP:** `203.0.113.45` (External)
- **Destination IP:** `10.0.0.1` (Internal Network Gateway)
- **Ports Targeted:**

- **3389 (RDP)** – Remote Desktop
- **22 (SSH)** – Secure Shell
- **445 (SMB)** – File Sharing
- **135 (RPC)** – Remote Procedure Call

3.3.3 Timestamp

January 27, 2025, 20:50:17 UTC (All attempts occurred at the same second, indicating automated scanning or a brute-force attack).

3.3.4 Severity

Critical – Unauthorized external access attempts targeting RDP and SSH suggest an **active intrusion attempt** or **vulnerability scanning**.

3.3.5 Evidence

Example log entries:

```
2025-01-27 20:50:17 ALLOW ICMP 203.0.113.45 10.0.0.1 19219 3389
```

Please refer to the **Appendix** (A.1) for more raw log entries.

3.3.6 Root Cause Analysis

- The **external IP (203.0.113.45)** repeatedly targeted **RDP, SSH, SMB, and RPC services**, suggesting an **automated attack or reconnaissance**.
- Some connections were **allowed**, indicating **misconfigured firewall rules** that are permitting unauthorized access.
- **Inbound ICMP requests** from the same IP suggest an **attempt to map network responses**.

3.3.7 Impact

- **Unauthorized access risk:** If successful, an attacker could gain remote control over internal systems.
- **Compliance violation:** Allowing external RDP/SSH access may breach security policies.
- **Potential data breach:** If SMB or RPC is exploited, internal files and services could be compromised.

3.3.8 Recommendation

1. **Block External RDP/SSH Access:** Disable inbound **RDP (3389)** and **SSH (22)** from external sources unless explicitly required.
2. **Investigate Firewall Rules:** Review and enforce **strict firewall policies** to block unauthorized traffic.

3. **Monitor and Blacklist Malicious IPs:** Add `203.0.113.45` to the **firewall deny list** and monitor for similar patterns.
4. **Enable Intrusion Detection System (IDS):** Deploy **IDS/IPS** to detect and prevent unauthorized access attempts.
5. **Enforce Multi-Factor Authentication (MFA):** If RDP/SSH access is necessary, require **MFA** for all remote logins.
6. **Conduct Log Analysis Regularly:** Automate **log reviews** to detect and mitigate future attacks proactively.

3.4 Finding #4: Repeated Unauthorized Access Attempts to Sensitive Endpoints

3.4.1 Description

The Apache access logs show multiple attempts to access **sensitive endpoints** such as `/admin/`, `/phpmyadmin/`, and `/wp-login.php`. Some requests resulted in **500 Internal Server Errors**, while others returned **403 Forbidden** and **404 Not Found** responses. Several requests originated from an external IP **(203.0.113.45)**, which identifies itself using the **Nmap Scripting Engine**, indicating potential reconnaissance activity.

3.4.2 Affected Systems/Users

- **Internal IPs:**
  - `192.168.1.100` – Attempted access to `/admin/` and `/phpmyadmin/`
  - `192.168.1.101` – Multiple login attempts on `/wp-login.php`
  - `192.168.1.102` – Unauthorized requests to `/contact.html` and `/admin/`
- **External IP:** `203.0.113.45` – Suspicious scanning activity targeting `/admin/` and `/index.html`

3.4.3 Timestamp

January 27, 2025, 20:50:17 UTC – All suspicious requests occurred within a single second, suggesting automated scanning or a bot attack.

3.4.4 Severity

Critical – The combination of repeated unauthorized access attempts and automated scanning activity poses a high security risk.

3.4.5 Evidence

Example log entries:

```
192.168.1.102 - - [2025-01-27 20:50:17] "GET /contact.html HTTP/1.1" 500 - "-" "Mozilla/5.0"
```

Please refer to the **Appendix** (A.1) for more raw log entries.

3.4.6 Root Cause Analysis

- **Automated vulnerability scanning** from external IP `203.0.113.45` using the **Nmap Scripting Engine**.
- **Repeated access attempts** to critical endpoints by internal IPs suggest possible brute-force attempts or unauthorized user activity.
- **500 errors** indicate misconfigured or vulnerable web services that could be exploited.

3.4.7 Impact

- **Potential Exploitation:** Attackers might find a way to bypass authentication and gain unauthorized access.
- **Data Breach Risk:** If successful, access to `/phpmyadmin/` or `/admin/` could lead to database compromises.
- **Downtime Risk:** Repeated **500 Internal Server Errors** indicate possible server instability or misconfiguration.

3.4.8 Recommendation

1. **Block External Scanning:** Blacklist `203.0.113.45` and enable Web Application Firewall (WAF) protections.
2. **Restrict Sensitive Endpoints:** Disable external access to `/admin/`, `/wp-login.php`, and `/phpmyadmin/`.
3. **Monitor and Log Access:** Set up alerts for repeated failed access attempts.
4. **Patch and Secure Web Applications:** Investigate and fix possible vulnerabilities causing **500 errors**.
5. **Enforce Strong Authentication:** Implement Multi-Factor Authentication (MFA) for all admin logins.

4 Summary of Findings and Recommendations

Here is a summary of the key findings from the log analysis:

Finding #	Description	Severity	Impact	Recommendation
1	Unusual dropped packets in firewall logs indicating possible unauthorized access attempts.	Medium	Potential security risk if misconfigured firewall rules allow unauthorized traffic.	Review firewall policies, enforce logging, and restrict unnecessary inbound rules.
2	Dropped and allowed RDP access attempts from multiple internal sources, suggesting privilege escalation attempts.	High	Risk of unauthorized remote access leading to potential system compromise.	Restrict RDP access, enable MFA, monitor suspicious login attempts, and investigate internal access patterns.
3	Suspicious external RDP and SSH connection attempts from `203.0.113.45`, some of which were allowed.	Critical	Possible brute-force attack or vulnerability scanning by an external actor.	Block the external IP, enforce strict firewall rules, enable IDS/IPS, and monitor external access logs.
4	Repeated unauthorized access attempts to `/admin/`, `/phpmyadmin/`, and `/wp-login.php`, including 500 errors and Nmap scans.	Critical	High risk of web application compromise, potential data breaches, and service downtime.	Restrict admin page access, patch vulnerabilities, enforce WAF policies, and enable MFA for all admin logins.

5 Next Steps

- **Further Investigation:**
  - Analyze authentication logs for suspicious login attempts related to Findings #2 and #4.
  - Verify firewall rules to ensure that external access is properly restricted (Findings #1 and #3).
  - Review web server configurations to address **500 Internal Server Errors** and unauthorized admin page access (Finding #4).
- **Security Patching and Configuration Updates:**
  - Apply the latest security patches to servers and applications to mitigate vulnerabilities.
  - Enforce firewall rule updates to block unauthorized RDP and SSH access.
  - Implement Web Application Firewall (WAF) policies to prevent scanning and brute-force attempts.
- **Policy Updates:**

  - Require multi-factor authentication (MFA) for all remote and admin logins.
  - Establish strict access control policies to prevent unauthorized privilege escalation.
  - Automate log analysis and alerting for suspicious activity.

- **Timeline for Remediation:**
  - Immediate (0-24 hours): Block external IPs, review critical firewall rules, enable MFA for privileged accounts.
  - Short Term (1-3 days): Apply security patches, update firewall policies, and configure logging alerts.
  - Medium Term (1-2 weeks): Conduct a security audit, implement an Intrusion Detection System (IDS), and enforce policy updates.

- **Responsible Parties:**
  - **IT Security Team:** Investigate unauthorized access attempts, apply security patches, and enforce access controls.
  - **Network Administrators:** Review firewall rules, block malicious IPs, and restrict RDP/SSH access.
  - **System Administrators:** Monitor server logs, apply updates, and enforce best security practices.

A Appendix

A.1 Raw Logs

Here are some example raw log entries that were analyzed in this report:

```
192.168.1.x - Person 1 [28/Jan/2025:08:14:14 +0000]
 "GET /admin/config HTTP/1.1" 403 4430 "-" "Mozilla/5.0"

 192.168.1.x - Person 2 [28/Jan/2025:10:44:09 +0000]
 "GET /admin/config HTTP/1.1" 403 4430 "-" "Mozilla/5.0"

 192.168.1.x - Person 3 [28/Jan/2025:10:46:11 +0000]
 "GET /admin/config HTTP/1.1" 403 4430 "-" "Mozilla/5.0"

 192.168.1.x - Person 4 [28/Jan/2025:13:35:25 +0000]
 "GET /admin/config HTTP/1.1" 403 4430 "-" "Mozilla/5.0"

 192.168.1.x - Person 5 [28/Jan/2025:19:17:13 +0000]
 "GET /admin/config HTTP/1.1" 403 4430 "-" "Mozilla/5.0"

 192.168.1.x - Person 6 [28/Jan/2025:19:43:53 +0000]
 "GET /admin/config HTTP/1.1" 403 4430 "-" "Mozilla/5.0"

 192.168.1.x - Person 7 [28/Jan/2025:20:16:55 +0000]
 "GET /admin/config HTTP/1.1" 403 4430 "-" "Mozilla/5.0"
```

```
2025-01-27 20:50:17 | Event ID: 5152 | Source IP: 192.168.1.x| Destination Port: 3389 | Action:
2025-01-27 20:50:17 | Event ID: 5152 | Source IP: 192.168.1.x | Destination Port: 3389 | Action:
2025-01-27 20:50:17 | Event ID: 5152 | Source IP: 192.168.1.x | Destination Port: 3389 | Action:
2025-01-27 20:50:17 | Event ID: 5152 | Source IP: 192.168.1.x | Destination Port: 3389 | Action:
2025-01-27 20:50:17 | Event ID: 5152 | Source IP: 192.168.1.x | Destination Port: 3389 | Action:
2025-01-27 20:50:17 | Event ID: 5152 | Source IP: 192.168.1.x | Destination Port: 3389 | Action:

2025-01-27 20:50:17 ALLOW ICMP 203.0.113.x 10.0.0.1 19219 3389
2025-01-27 20:50:17 ALLOW TCP 203.0.113.x 10.0.0.1 37134 22
2025-01-27 20:50:17 DROP TCP 203.0.113.x 10.0.0.1 30673 445
2025-01-27 20:50:17 ALLOW UDP 203.0.113.x 10.0.0.1 16546 445
2025-01-27 20:50:17 DROP ICMP 203.0.113.x 10.0.0.1 41055 445
2025-01-27 20:50:17 ALLOW TCP 203.0.113.x 10.0.0.1 29160 443
2025-01-27 20:50:17 ALLOW UDP 203.0.113.x 10.0.0.1 31392 3389
2025-01-27 20:50:17 DROP ICMP 203.0.113.x 10.0.0.1 11844 80

192.168.1.x - - [2025-01-27 20:50:17] "GET /contact.html HTTP/1.1" 500 - "-" "Mozilla/5.0"
192.168.1.x - - [2025-01-27 20:50:17] "GET /phpmyadmin/ HTTP/1.1" 500 - "-" "Googlebot/2.1"
192.168.1.x - - [2025-01-27 20:50:17] "GET /wp-login.php HTTP/1.1" 500 - "-" "Googlebot/2.1"
192.168.1.x - - [2025-01-27 20:50:17] "GET /admin/ HTTP/1.1" 403 - "-" "Mozilla/5.0"
203.0.113.x - - [2025-01-27 20:50:17] "GET /admin/ HTTP/1.1" 403 - "-" "Nmap Scripting Engine"
192.168.1.x - - [2025-01-27 20:50:17] "GET /phpmyadmin/ HTTP/1.1" 200 - "-" "Mozilla/5.0"
```

A.2 Glossary

- **403 Forbidden:** HTTP status code indicating that the server understands the request but refuses to authorize it.
- **500 Internal Server Error:** HTTP status code indicating that the server encountered an unexpected condition that prevented it from fulfilling the request.
- **RDP (Remote Desktop Protocol):** A protocol developed by Microsoft that provides a user with a graphical interface to connect to another computer over a network connection.
- **SSH (Secure Shell):** A cryptographic network protocol for operating network services securely over an unsecured network.
- **MFA (Multi-Factor Authentication):** A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity.
- **WAF (Web Application Firewall):** A firewall that monitors, filters, and blocks HTTP traffic to and from a web application.
- **IDS (Intrusion Detection System):** A device or software application that monitors a network or systems for malicious activity or policy violations.
- **IPS (Intrusion Prevention System):** A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

References

[1] Apache HTTP Server Documentation. https://httpd.apache.org/docs/

[2] Microsoft Remote Desktop Protocol (RDP). https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/

[3] Secure Shell (SSH) Protocol. https://www.ssh.com/ssh/protocol/

[4] Multi-Factor Authentication (MFA). https://csrc.nist.gov/glossary/term/multi_factor_authentication

[5] Web Application Firewall (WAF). https://owasp.org/www-project-web-application-firewall/

[6] Intrusion Detection System (IDS). https://www.us-cert.gov/ncas/tips/ST04-015

[7] Intrusion Prevention System (IPS). https://www.cisco.com/c/en/us/products/security/intrusion-prevention-system-ips/index.html