Log Analysis Report

9-9-24 | By: Barrett Caywood

IDS Log

After analyzing the log file, several suspicious activities have been identified, indicating a potential security incident involving multiple attack vectors, including vulnerability exploits, spyware deployment, and covert communication channels. The incident occurred between February 10, 2023, and February 12, 2023, and affected multiple internal systems, with evidence of lateral movement and data exfiltration attempts.

ICMP Error Messages

The log file shows multiple entries of ICMP error messages with various IP addresses, which could indicate an attempt to exploit a vulnerability in the network's ICMP implementation. These frequent "No Matching Connection For ICMP Error Message" entries suggest reconnaissance attempts, potentially probing the network for open ports or vulnerabilities. For example:

- 02/11/23 8:00:00 AM: ICMP error message from 87.126.70.133 to 192.168.209.1
- 02/11/23 8:00:00 AM: ICMP error message from 87.126.71.75 to 192.168.209.122
- 02/11/23 8:00:00 AM: ICMP error message from 87.126.81.7 to 192.168.209.127

These entries suggest that an attacker may have been attempting to scan the network for open ports or vulnerabilities, potentially using ICMP error messages to gather information about the network's configuration.

Spyware Activity

The log file shows multiple entries of detected spyware activity with various IP addresses, indicating a potential malware infection. The fact that these entries are from the same internal IP address or targeting the same external IP address suggests that a host may have been compromised. The use of ICMP and DNS for command and control (C2) and data exfiltration further supports this theory. For example:

- 02/10/23 2:00:00 PM: Detected spyware activity from 104.243.21.152 to 192.168.10.103
- 02/11/23 7:00:00 AM: Detected spyware activity from 1.82.119.89 to 192.168.209.97
- 02/11/23 12:00:00 AM: Detected spyware activity from 185.35.62.135 to 192.168.10.100

These entries suggest that a malicious actor may have compromised a host and is using it to communicate with external IP addresses, potentially exfiltrating data or receiving commands.

Suspicious Outbound Traffic

The log file shows multiple entries of outbound traffic to unknown or suspicious external IP addresses, particularly involving common ports for malicious activity, such as port 53 for DNS. This could indicate a potential DNS tunneling or amplification attack. For example:

- 02/11/23 7:00:00 AM: Outbound DNS activity from 192.168.209.97 to 1.82.119.89
- 02/10/23 10:00:00 AM: Outbound DNS activity from 192.168.10.15 to 1.9.119.125
- 02/11/23 12:00:00 AM: Outbound DNS activity from 185.35.62.135 to 192.168.10.100

These entries suggest that a malicious actor may be using DNS to exfiltrate data or communicate with external IP addresses, potentially exploiting a vulnerability in the network's DNS implementation.

Firewall Log

This section consolidates the analyzed log data from ACME's Untangled Firewall, identifying potential security threats and vulnerabilities within the network. The findings highlight repeated access denials, potential exploitation attempts, and suspicious activities requiring further investigation.

Denials from External and Internal Hosts

A significant number of entries indicate that requests from both internal and external hosts are being denied access. The frequency of these denials could suggest either benign behavior (e.g., automated systems) or potential scanning activities. Denials from external IPs attempting to access resources may imply attempts to exploit or probe the network from outside. For example:

Process: GoogleUpdateSetup.exe

- west-cp01 (192.168.1.20): Multiple entries denying access.
- west-cp01_outside (192.168.1.12): Multiple entries denying access.

These entries suggest that both internal and external hosts are being actively monitored, and unauthorized access attempts are being blocked

Repeated Denials of Access

Numerous entries indicate that requests from workstations to access the ACME.LOC domain are being denied. This could suggest misconfiguration, unauthorized access attempts, or automated processes trying to reach restricted internal resources. For example:

- Host: west-acme-workstation-jessica7 (192.168.0.15): Multiple entries denying access to 10.7.6.0 ACME.LOC.
- Host: west-acme-workstation-Thomas2 (192.168.6.13): Multiple entries denying access to 10.7.6.0 ACME.LOC.

Apache Server Protection Violations

Multiple entries indicate header injection attempts targeting Apache servers, suggesting potential exploitation attempts by attackers to manipulate HTTP headers for malicious purposes. For example:

- 08/23/24 05:51:17 PM: Apache HTTP Server Header Injection Cross-Site Scripting from IP 192.168.10.110 (Action: monitor).
- 08/21/24 04:20:00 PM: Apache Header Injection from IP 192.168.10.110 (Action: reject).

The repeated attempts at header injection indicate targeted exploitation efforts aimed at Apache servers, potentially leading to Cross-Site Scripting (XSS) vulnerabilities.

Web Server Enforcement Violations

Numerous entries regarding cross-site scripting (XSS) and directory traversal attempts have been recorded, particularly related to Microsoft Exchange and Linux systems. This indicates potential vulnerability exploitation attempts against web applications. For example:

- 08/23/24 04:25:44 PM: Microsoft Exchange OWA cross-site scripting and spoofing (MS04-026) from IP 192.168.0.102 (Action: monitor).
- 08/23/24 04:26:57 PM: Web Servers Malicious URL Directory Traversal from IP 192.168.10.109 (Action: monitor).

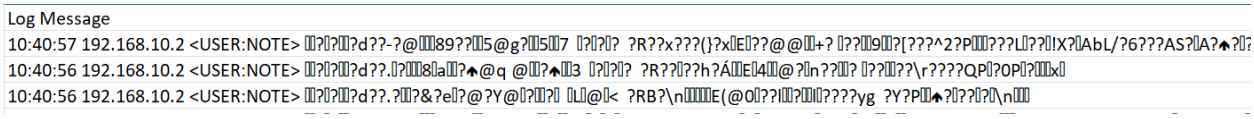
These entries suggest that web applications are being targeted for exploitation, potentially allowing attackers to inject malicious code or access unauthorized resources.

Brocade Log

After reviewing the log file from the Brocade network device, several suspicious activities have been identified. The analysis of these logs reveals several unusual patterns and anomalies that suggest potential security threats or misconfiguration. The log data from the Brocade network device contains a series of 17,213 syslog messages recorded on September 8, 2024, from 9:53 AM to 10:40 AM.

Repeated Malformed Log Messages:

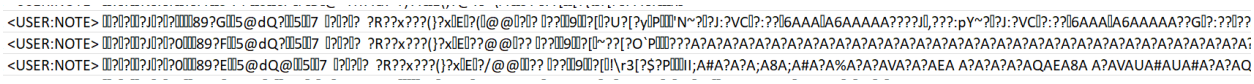
Multiple entries in the log file show repeated malformed log messages, which could indicate an attempt to obscure information or interfere with the logging process. The messages are consistently tagged with "USER:NOTE" and followed by a mix of non-readable characters and garbled text. For example:



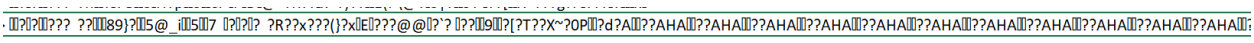
These entries suggest that the device may be experiencing data corruption, encoding issues, or more likely an attempt to hide malicious activity.

Unusual Patterns in Data Transmission:

Multiple entries in the log file show unusual patterns in data transmission, which could indicate an attempt to hide or encrypt data. For example:



Here is another repeating character sequences that can be seen throughout the log file:



These are just some of the examples of recurring patterns of obfuscated or garbled data. These entries suggest that the device may be under attack or experiencing abnormal activity.

High Frequency of Logs in a Short Time Frame:

The log file shows a high frequency of logs in a short time frame, with approximately 6 logs per second. This could indicate that the device is misconfigured or under attack. It is possible this abnormal activity is an automated process or a scanning activity. For example, we are getting 6 per second in the following image: