Log Analysis Case Study: Honeynet Project

# Case Title

Log Analysis from a Compromised Honeynet Server

# Objective

Analyze log files captured from a Honeynet to identify indicators of compromise (IoCs), attacker behavior, exploited vulnerabilities, and mitigation strategies.

# Background

A low-interaction Honeynet (running a Linux-based web server) was deployed with intentionally vulnerable configurations. After 48 hours, unusual traffic patterns were observed. You are tasked with performing forensic log analysis to reconstruct the attack timeline.

# Materials Provided

* Apache access and error logs (access.log, error.log)
* Auth log (auth.log)
* TCPDump capture or NetFlow data (network\_traffic.pcap)
* System messages (syslog, messages)
* Cron log (cron.log)
* Hashes and metadata of modified files (file\_changes.txt)

# Tasks - Part 1: Initial Reconnaissance and Entry Point (20%)

* Identify the first timestamp of suspicious activity.
* Determine the attacker’s IP address(es).
* What type of reconnaissance techniques were used? (e.g., directory brute-forcing, user-agent anomalies)
* What vulnerability was likely exploited for initial access?
* Hint: Look for common scanning tools (e.g., Nikto, DirBuster) and payloads in URL parameters.

# Tasks - Part 2: Privilege Escalation and Persistence (25%)

* Analyze auth.log for failed/successful login attempts.
* Were any suspicious users added or existing accounts compromised?
* Check for privilege escalation signs—sudo access, root shell access.
* Was persistence established (e.g., cron jobs, backdoors)?

# Tasks - Part 3: Post-Exploitation and Network Behavior (25%)

* Analyze network\_traffic.pcap for outbound connections:
* • Was data exfiltrated?
* • Any communication with known Command & Control (C2) servers?
* Look for payloads or tools downloaded post-compromise (e.g., Netcat, reverse shells).
* Check cron.log and syslog for indicators of automation or scheduled attacks.

# Tasks - Part 4: Indicators of Compromise (15%)

* List at least:
* • 3 IP addresses
* • 3 suspicious file paths or binaries
* • 2 URLs or domains used in the attack
* • 2 hashes (MD5/SHA256) of malicious files or scripts

# Tasks - Part 5: Summary and Mitigation (15%)

* Provide a timeline of the attack (from initial access to post-exploitation).
* What security controls failed or were missing?
* Recommend 3 preventive and 3 detective measures.
* If this was a real production server, what would your incident response steps be?

# Deliverable Format

* PDF Report (max 10 pages) or Markdown
* Include screenshots of logs and evidence
* Visual timeline is a plus (e.g., using draw.io or any timeline tool)

# Optional Tools You May Use

* Wireshark
* Splunk or ELK stack (for log ingestion)
* Logwatch or GoAccess
* VirusTotal (for hash checking)
* GeoIP lookup for attacker IPs

# Summit to [prinya.homanek@gmail.com](mailto:prinya.homanek@gmail.com)

# Deadline (both assignments and group presentation)

28 April 2025