# Forensic Analysis Report

## 1. Log Analysis

### 1.1 Web Server Access Logs

The web server access logs (`phl\_access\_log.txt`) were examined for access patterns, including timestamps, IP addresses, and user agents. The logs revealed the following key observations:

- \*\*Benign Bot Activity\*\*:

- IP `136.243.111.17` and `138.201.202.232` made legitimate requests using the `SiteCheckerBotCrawler/1.0` user agent.

- \*\*Suspicious Scanning Activity\*\*:

- IP `138.68.92.163` made numerous GET requests to various paths (e.g., `/randomfile1`, `/frand2`), most of which returned 404 Not Found.

- Successful access to `/uploads/` and `/uploads/shell.php` indicated a potential directory traversal attack.

- \*\*Web Shell Upload\*\*:

- A POST request to `/uploads/shell.php` with `curl/7.68.0` user agent suggests a web shell upload.

### 1.2 Database Access Logs

The database access logs (`phl\_database\_access\_log.txt`) were reviewed for SQL queries executed:

- \*\*Data Exfiltration\*\*:

- Successful access to the `phl` database and execution of `SELECT \* FROM customers`.

- Use of `mysqldump` to export the `phl` database.

- \*\*Unauthorized Access Attempts\*\*:

- No unauthorized access attempts were noted, but the use of root credentials was concerning.

### 1.3 System Logs

System logs were analyzed for login attempts and process executions:

- \*\*Login Attempts\*\*:

- Multiple login attempts with weak credentials (`phl/phl123`) were successful.

- \*\*Process Executions\*\*:

- Execution of `mysqldump` and `scp` for data exfiltration.

## 2. Network Traffic Analysis

### 2.1 PCAP Overview

The PCAP files (`phlwebserver.pcap` and `phldatabase.pcap`) were analyzed for network traffic:

- \*\*Key Events\*\*:

- Reverse shell connection from `138.68.92.163` to the web server.

- TELNET sessions from the web server to the database server.

- Data exfiltration to an external server (`178.62.228.28`).

### 2.2 Key Packet Details

- \*\*Packet 789\*\*:

- POST request to `/uploads/shell.php` from `138.68.92.163` to `134.122.33.221`.

- Payload contained a Python reverse shell command.

- \*\*Packet 790\*\*:

- Acknowledgment of the POST request, confirming the upload of `shell.php`.

- \*\*Packet 786\*\*:

- SSH connection established between `92.255.85.135` and the database server.

### 2.3 Timeline of Network Events

- \*\*19/Feb/2022 21:58:22\*\*: Initial GET requests from `138.68.92.163`.

- \*\*19/Feb/2022 21:59:04\*\*: POST request to `/uploads/shell.php`.

- \*\*20/Feb/2022 03:01:46\*\*: Database dump and exfiltration.

## 3. File and Artifact Analysis

### 3.1 Web Shell Analysis

- \*\*shell.php\*\*:

- Analyzed for embedded commands and scripts.

- Confirmed as a web shell capable of executing arbitrary commands.

### 3.2 Malicious Script Breakdown

- \*\*Python Reverse Shell\*\*:

- Command: `python -c 'import socket, subprocess, os; ...'`

- Established a reverse shell from the web server to `138.68.92.163`.

## 4. System and Configuration Review

### 4.1 /uploads/ Directory Misconfiguration

- \*\*Misconfiguration\*\*:

- Directory listing enabled and writable by unauthorized users.

- \*\*Recommendations\*\*:

- Disable directory listing and restrict file uploads to specific types.

- Implement strict file validation and permissions.

### 4.2 TELNET Usage and Weak Credentials

- \*\*Risks\*\*:

- Use of TELNET and weak passwords (`phl/phl123`).

- \*\*Recommendations\*\*:

- Transition to SSH for secure remote access.

- Enforce strong password policies and multi-factor authentication.

## 5. Tools and Techniques

### 5.1 Forensic Tools Used

- \*\*Wireshark\*\*: For network traffic analysis.

- \*\*Log Analysis Software\*\*: For parsing and analyzing web and database logs.

- \*\*TCPdump\*\*: For capturing network packets.

### 5.2 Analysis Methods

- \*\*Log Correlation\*\*: Cross-referencing web, database, and system logs.

- \*\*Network Traffic Analysis\*\*: Using Wireshark to identify malicious packets.

- \*\*File Dissection\*\*: Analyzing `shell.php` and other artifacts.

## 6. Findings and Conclusions

### 6.1 Summary of Analytical Findings

- \*\*Attack Vector\*\*:

- Exploitation of misconfigured `/uploads/` directory to upload a web shell.

- Use of TELNET and weak credentials to access the database server.

- \*\*Extent of Compromise\*\*:

- Successful exfiltration of the `phl` database, including customer data.

### 6.2 Recommendations Based on Analysis

- \*\*Immediate Actions\*\*:

- Remove the web shell and block attacker IPs.

- Change compromised credentials and secure database access.

- \*\*Long-term Improvements\*\*:

- Implement a WAF and regular security audits.

- Harden systems and enforce strong access controls.

- \*\*Ongoing Monitoring\*\*:

- Centralize logging and deploy IDS/IPS for real-time threat detection.

### Figures and Tables

- \*\*Figure 1\*\*: Flowchart of the attack sequence.

- \*\*Table 1\*\*: Summary of key PCAP events with timestamps and descriptions.

---

This forensic analysis provides a comprehensive understanding of the incident, detailing the attack sequence, impact, and recommendations for enhancing security measures.