SENTRY SECURITY FORENSICS REPORT

Generated: 2026-02-10 09:54:41.671350

THREAT: Brute Force (Line 1)

Why it's dangerous: High risk of unauthorized system access via password guessing.

```
Log Evidence: Feb 10 08:01:22 server sshd[123]: Failed password for root from 192.168.1.55 por
```

THREAT: Brute Force (Line 2)

Why it's dangerous: High risk of unauthorized system access via password guessing.

```
Log Evidence: Feb 10 08:01:24 server sshd[123]: Failed password for root from 192.168.1.55 por
```

THREAT: Brute Force (Line 3)

Why it's dangerous: High risk of unauthorized system access via password guessing.

```
Log Evidence: Feb 10 08:01:26 server sshd[123]: Failed password for root from 192.168.1.55 por
```

THREAT: SQL Injection (Line 5)

Why it's dangerous: Attempt to steal or corrupt the database via malicious queries.

```
Log Evidence: Feb 10 08:10:45 server httpd: 192.168.1.55 - - [10/Feb/2026:08:10:45] "GET /logi
```

THREAT: Suspicious Script (Line 5)

Why it's dangerous: Execution of scripts in temporary directories, often indicating malware.

```
Log Evidence: Feb 10 08:10:45 server httpd: 192.168.1.55 - - [10/Feb/2026:08:10:45] "GET /logi
```

THREAT: Suspicious Script (Line 6)

Why it's dangerous: Execution of scripts in temporary directories, often indicating malware.

```
Log Evidence: Feb 10 08:12:00 server ftp: 10.0.0.5 downloaded malware_installer.exe
```

THREAT: Path Traversal (Line 7)

Why it's dangerous: Attempt to access restricted system files (like /etc/passwd).

```
Log Evidence: Feb 10 08:15:30 server httpd: 192.168.1.55 "GET /../../etc/passwd HTTP/1.1" 403
```