Web Server Attack Forensic Analysis Report

Made by: Aditya bandaru

Executive Summary

This report details the findings of a forensic investigation into a suspected attack on a web server running DVWA (Damn Vulnerable Web Application). Analysis of access logs, authentication logs, and error logs reveals evidence of a brute force attack against the DVWA login page. The attack, originating from IP address 10.1.41.50, utilized the Hydra tool to attempt to gain unauthorized access to the application. The attack occurred on April 3, 2025, beginning at approximately 21:31:11 IST. While the logs do not conclusively demonstrate that the attacker achieved successful authentication, the evidence indicates a methodical attack against a deliberately vulnerable web application environment.

1. Purpose and Scope

1.1 Incident Overview

On April 3, 2025, suspicious activity was detected on a web server hosting the DVWA (Damn Vulnerable Web Application) platform. System logs indicated multiple rapid login attempts to the DVWA application, exhibiting patterns consistent with automated brute force attacks.

1.2 Investigation Objectives

- Determine the nature and extent of the suspicious activity
- Identify the attack vector and methods used
- Establish a timeline of events
- Assess potential system compromise
- Provide recommendations for security improvements

1.3 Evidence Sources

The investigation relied on the following log files:

- Web server access logs
- System authentication logs
- Web server error logs

2. System Information

2.1 System Configuration

- Operating System: Ubuntu Linux
- Web Server: Apache 2.4.58
- Application: DVWA (Damn Vulnerable Web Application)
- Hostname: aditya-VirtualBox
- System appears to be running in a VirtualBox environment

3. Timeline of Events

Date/Time (IST)	Event	Source
2025-04-03 17:55:50	Apache server started and configured	Error log
2025-04-03 18:00:14	Initial access to server root (/)	Access log
2025-04-03 18:13:29	System reboot initiated	Auth log, Error log
2025-04-03 18:14:08	Apache server restarted	Error log
2025-04-03 18:17:47	System reboot initiated	Auth log, Error log
2025-04-03 18:18:25	Apache server restarted	Error log
2025-04-03 18:28:49	System reboot initiated	Auth log, Error log
2025-04-03 18:29:13	Apache server restarted	Error log

2025-04-03 18:35:10	System reboot initiated	Auth log, Error log
2025-04-03 18:35:31	Apache server restarted	Error log
2025-04-03 21:20:50	Apache server restarted or reconfigured	Error log
2025-04-03 21:31:11	**Attack begins - Initial GET requests to /dvwa/login.php**	Access log
2025-04-03 21:31:12	Multiple POST requests to /dvwa/login.php	Access log
2025-04-03 21:31:12	PHP warnings about undefined array key "user_token"	Error log
2025-04-03 21:31:13	Continued GET/POST requests to /dvwa/login.php	Access log
2025-04-03 21:31:13	Multiple PHP warnings in error logs	Error log

4. Attack Analysis

4.1 Attack Vector

The attacker targeted the login page of the DVWA application (/dvwa/login.php) using an automated tool. Based on the user agent string "Mozilla/5.0 (Hydra)" in the access logs, the attacker utilized the Hydra tool, a well-known password cracking utility designed for brute force attacks.

4.2 Attack Methodology

1. **Reconnaissance**: The attack began with GET requests to the DVWA login page, likely to establish the form structure and parameters.
2. **Brute Force Attempt**: The attacker then launched multiple POST requests to the login page in rapid succession (within seconds), characteristic of an automated brute force attack.
3. **Tool Identification**: The user agent string "Mozilla/5.0 (Hydra)" clearly identifies the attack tool.
4. **Attack Pattern**:

    - Multiple GET requests to /dvwa/login.php (17 requests within 2 seconds)
    - Multiple POST requests to /dvwa/login.php (15 requests within 1 second)
    - Additional GET requests to the login page

5. **PHP Errors**: The error logs show multiple warnings about an undefined array key "user_token", which is likely related to DVWA's anti-CSRF token mechanism. The attacker's requests did not include this token, indicating either:
    - The tool was not configured to handle CSRF tokens
    - The attacker was unaware of the token requirement
    - The attacker was deliberately testing the application's resistance to basic brute force attempts

4.3 Technical Evidence

From access logs:

```
10.1.41.50 - - [03/Apr/2025:21:31:11 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1779 "-" "Mozilla/5.0 (Hydra)"
10.1.41.50 - - [03/Apr/2025:21:31:12 +0530] "POST /dvwa/login.php HTTP/1.0" 302 412 "-" "Mozilla/5.0 (Hydra)"
```

From error logs:

```
[Thu Apr 03 21:31:12.861512 2025] [php:warn] [pid 1305] [client 10.1.41.50:41758] PHP Warning: Undefined array key "user_token" in /var/www/html/dvwa/login.php on line 18
```

4.4 Attacker Information

- Source IP: 10.1.41.50 (internal IP address, suggesting the attack originated from within the local network)
- Tool: Hydra brute force utility
- Attack timing: April 3, 2025, at 21:31 IST
- Ports used by attacker: Various ephemeral ports (41758, 41774, 41780, etc.)

5. Impact Assessment

5.1 System Compromise

The available logs do not definitively indicate whether the attacker successfully gained access to the DVWA application. The HTTP status code 302 (redirect) in response to the POST requests could indicate either:

- Successful authentication and redirect to a welcome page
- Failed authentication and redirect back to the login page with an error message

Without additional logs such as DVWA application logs or session logs, it's not possible to conclusively determine if the attack was successful.

5.2 Data Exposure

No evidence of data exfiltration was found in the analyzed logs. However, if the attacker did gain access to the DVWA application, they would potentially have access to:

- Any data stored within the DVWA application
- Potential launching point for further attacks against the system

5.3 System Integrity

The authentication logs show multiple system reboots throughout the day, but these appear to be related to system maintenance rather than the attack, as they occurred before the attack timestamp.

6. Conclusions

Based on the forensic analysis of the provided logs, we can conclude that:

1. The web server hosting a DVWA application was targeted by a brute force attack on April 3, 2025.
2. The attack originated from IP address 10.1.41.50 using the Hydra password cracking tool.
3. The attacker made multiple rapid authentication attempts against the DVWA login page.

4. The attack methodology was relatively unsophisticated, as it did not account for CSRF protection mechanisms.
5. The available logs do not conclusively demonstrate whether the attack was successful in gaining unauthorized access.
6. The attack appears to be targeted specifically at the DVWA application, which is intentionally designed to be vulnerable for security testing and training purposes.

7. Recommendations

7.1 Immediate Actions

- Block the attacking IP address (10.1.41.50) at the network firewall level
- Reset any potentially compromised credentials
- Review active sessions and terminate suspicious connections
- Verify system and application integrity

7.2 Short-Term Mitigations

- Implement rate limiting for login attempts
- Enable CAPTCHA protection on authentication forms
- Enforce strong password policies
- Consider implementing IP-based access controls for sensitive applications

7.3 Long-Term Security Improvements

- Deploy a Web Application Firewall (WAF) to detect and block common attack patterns
- Implement comprehensive logging and monitoring solutions
- Consider intrusion detection/prevention systems
- Regularly review and update security configurations
- Conduct periodic security assessments and penetration testing

7.4 Monitoring Recommendations

- Increase log retention periods

- Implement centralized log collection and analysis
- Configure alerts for suspicious authentication patterns
- Monitor for brute force attack signatures

8. Appendices

8.1 Log Samples

Access Log Sample

```
10.1.41.50 - - [03/Apr/2025:21:31:11 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1779 "-" "Mozilla/5.0 (Hydra)"
10.1.41.50 - - [03/Apr/2025:21:31:12 +0530] "POST /dvwa/login.php HTTP/1.0" 302 412 "-" "Mozilla/5.0 (Hydra)"
10.1.41.50 - - [03/Apr/2025:21:31:13 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1683 "-" "Mozilla/5.0 (Hydra)"
```

Error Log Sample

```
[Thu Apr 03 21:31:12.861512 2025] [php:warn] [pid 1305] [client 10.1.41.50:41758] PHP Warning: Undefined array key "user_token" in /var/www/html/dvwa/login.php on line 18
[Thu Apr 03 21:31:12.865671 2025] [php:warn] [pid 4425] [client 10.1.41.50:41774] PHP Warning: Undefined array key "user_token" in /var/www/html/dvwa/login.php on line 18
```

Auth Log Sample

```
2025-04-03T17:55:47.011733+05:30 aditya-VirtualBox systemd-logind[640]: New seat seat0.
2025-04-03T18:00:52.378226+05:30 aditya-VirtualBox dbus-daemon[583]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
```

8.2 Attack Statistics

- Total GET requests to login page: 32

- Total POST requests to login page: 15
- Attack duration: Approximately 2 seconds
- Error messages generated: 16

8.3 Tools Used in Investigation

- Log analysis tools
- Timeline reconstruction techniques
- Pattern matching for attack signatures

9. Report Information

- **Report Date**: April 18, 2025
- **Investigation Period**: April 3-18, 2025
- **Report Version**: 1.0
- **Classification**: Confidential