FORENSIC ANALYSIS

Performing forensic analysis on simulated web server breach

TABLE OF CONTENTS

1. Introduction
2. Problem Statement
3. Problem objective
4. Architecture
5. Methodology / Process Flow
6. Working Images
7. Conclusion
8. Forensic Report

INTRODUCTION

- Web servers are prime targets for cyberattacks like SQL Injection, Brute Force, and XSS.
- Compromised servers hold critical log data that can provide clues about attack origins and techniques.
- Digital forensics helps in acquiring, preserving, and analyzing such data for investigation and legal validation.
- This project simulates a real-world server attack scenario and performs a structured forensic investigation.

PROBLEM STATEMENT

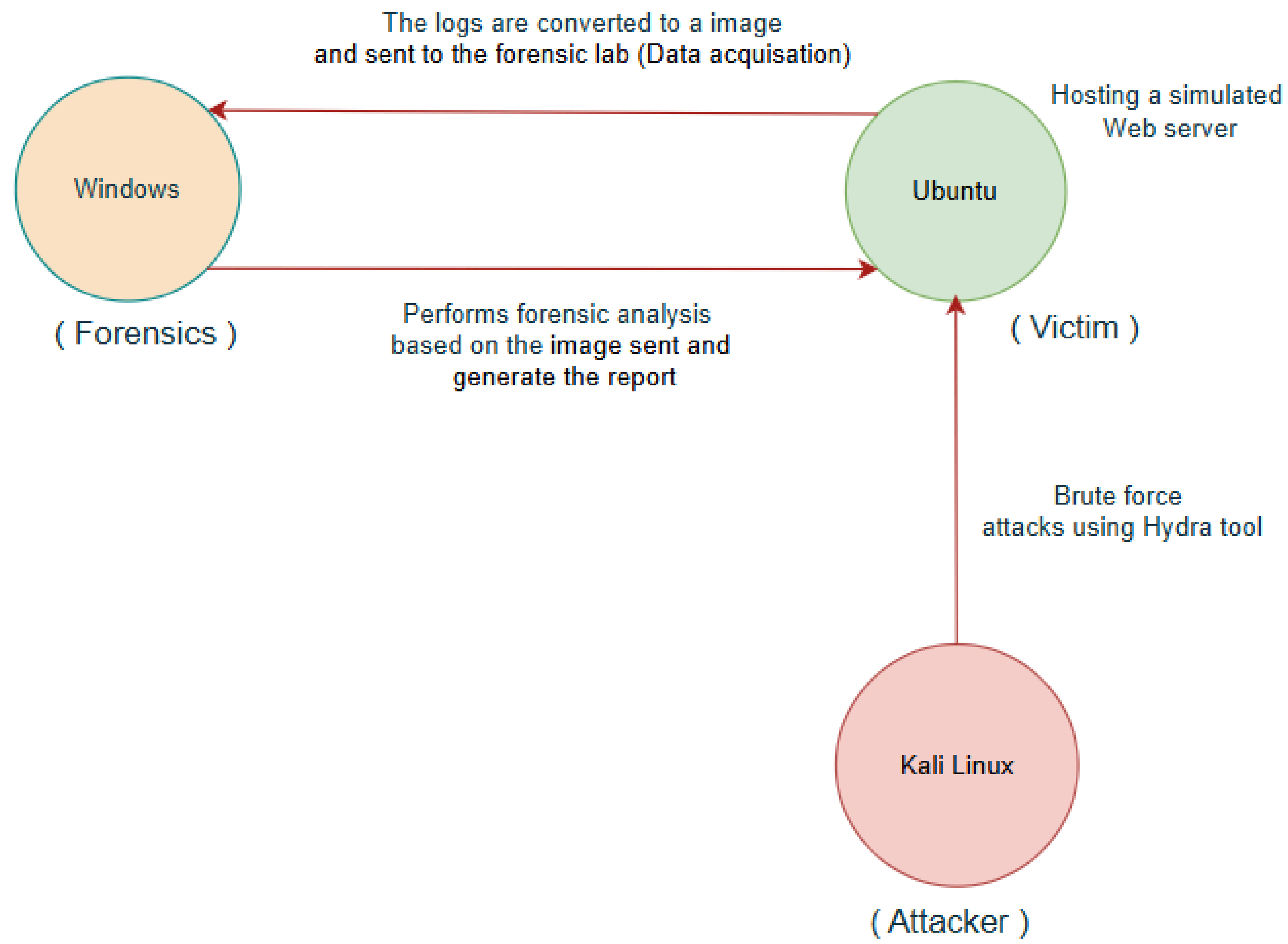
- Web applications are vulnerable to attacks like brute force, SQL injection, and XSS.
- Small and medium servers often lack proper forensic investigation mechanisms.
- Post-attack, critical evidence like logs can get tampered or lost if not preserved early.
- Without proper forensic imaging, tracing attacker behavior and entry points is difficult.
- No standard workflow exists for evidence collection and analysis on local or small servers.
- A forensic system is needed to safely collect, image, and analyze logs for attack traces.

PROJECT OBJECTIVE

- To simulate multiple cyberattacks on a vulnerable web server.
- To perform forensic data acquisition of server log files using tools like dc3dd.
- To generate and verify forensic images (.dd files) with hash values for integrity.
- To analyze the acquired images using Autopsy forensic suite on Windows.
- To prepare a forensic investigation report highlighting findings, attack footprints, and recommendations.

ARCHITECTURE

Q) Perform forensic analysis on a simulated web server breach.



PROCESS FLOW

1) **ATTACK SIMULATION:**

Simulate Brute-force on a vulnerable web server.

2) **LOG COLLECTION:**

Capture logs: access.log, error.log, auth.log.

3) **FORENSIC ACQUISITION:**

Create a .dd image using dc3dd from log directory.

4) **IMAGE TRANSFER:**

Send image to Windows forensic workstation via secure method.

5) **FORENSIC ANALYSIS:**

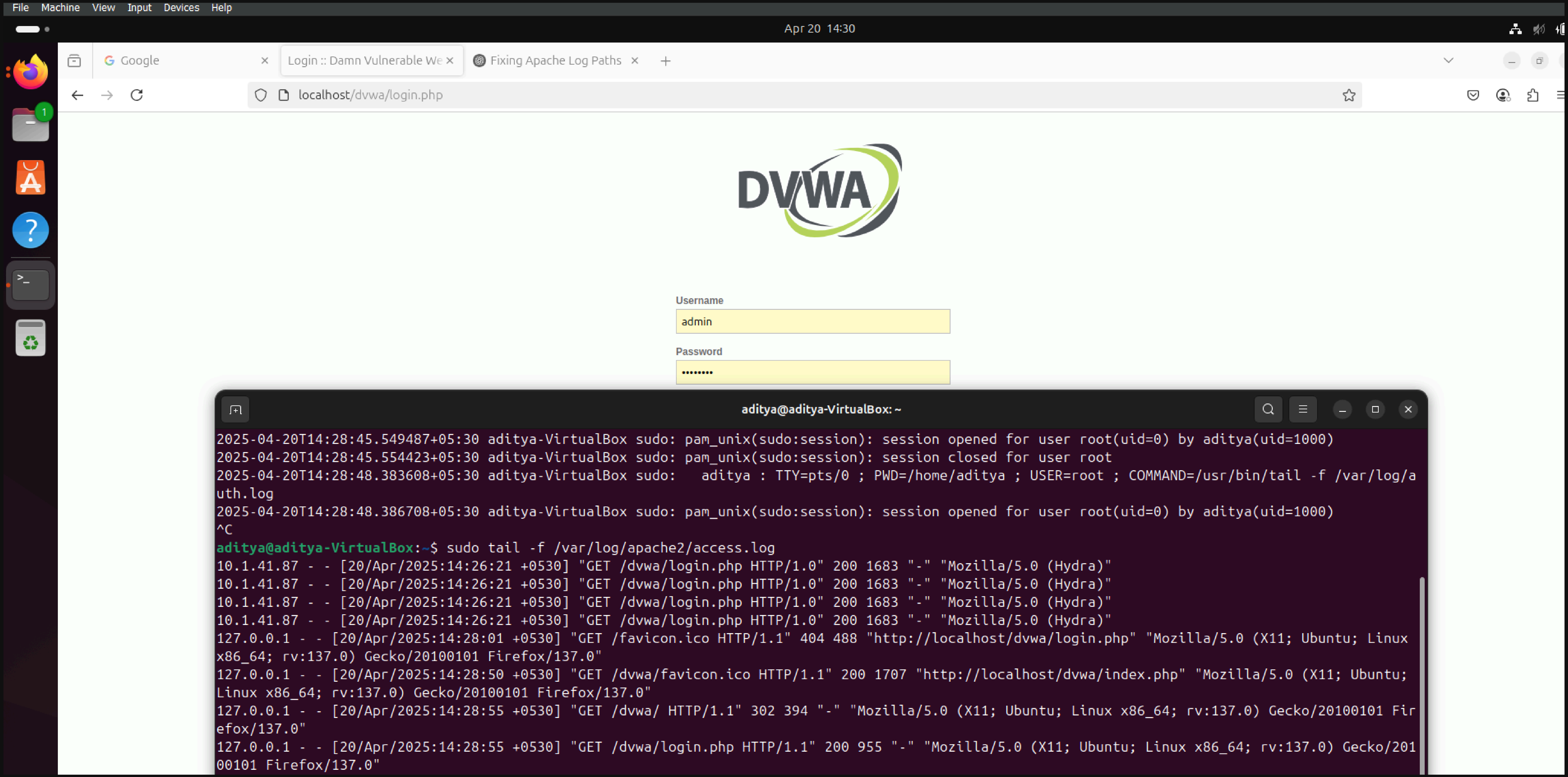
Use Autopsy to analyze the .dd image, extract evidence, detect attack patterns.

6) **REPORT GENERATION:**

Document findings, timestamps, evidence paths, and recommendations.

WORKING IMAGES

VICTIM (UBUNTU)



Username

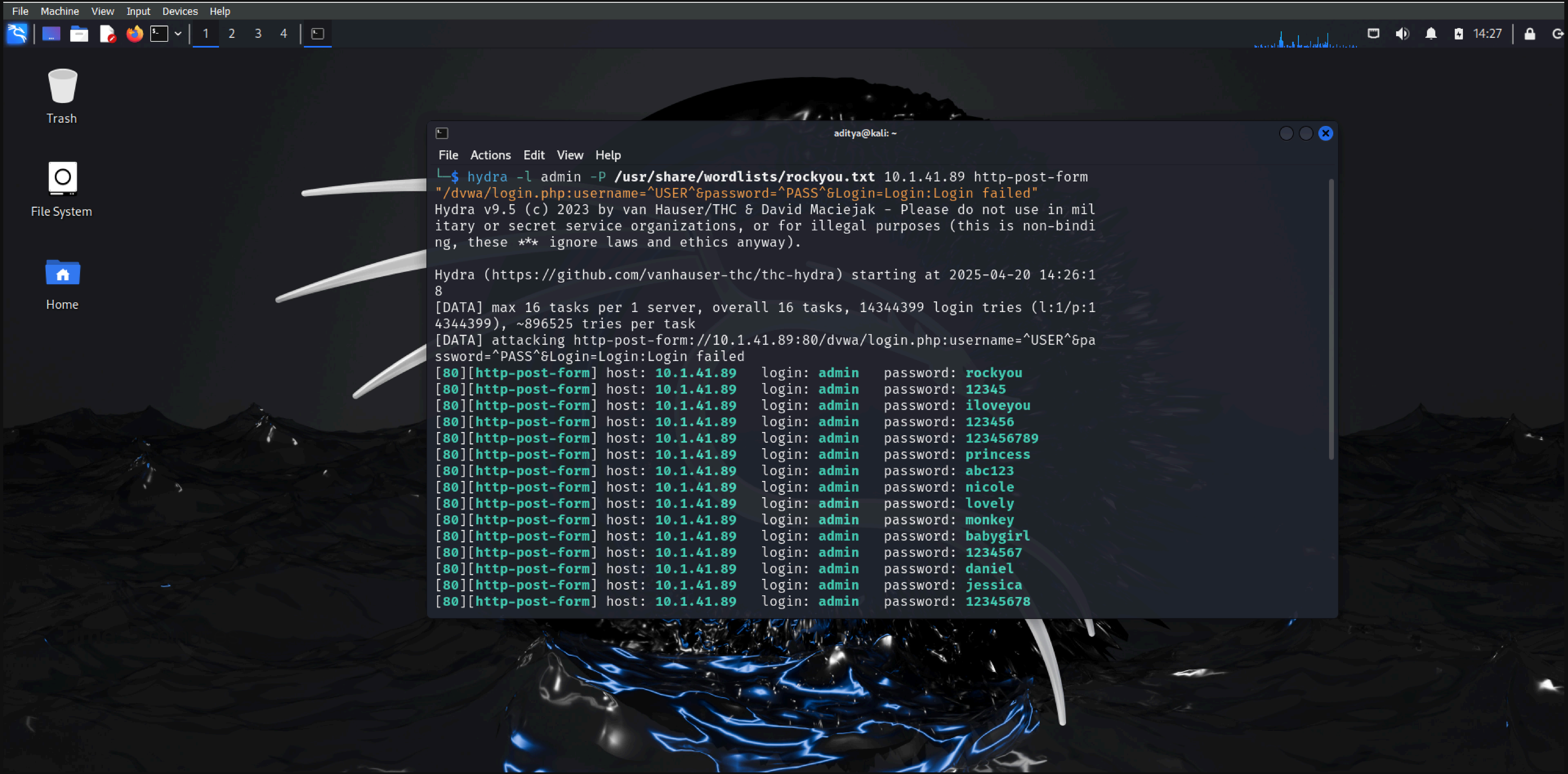
admin

Password

••••••••

```
2025-04-20T14:28:45.549487+05:30 aditya-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by aditya(uid=1000)
2025-04-20T14:28:45.554423+05:30 aditya-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
2025-04-20T14:28:48.383608+05:30 aditya-VirtualBox sudo:   aditya : TTY=pts/0 ; PWD=/home/aditya ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/a
uth.log
2025-04-20T14:28:48.386708+05:30 aditya-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by aditya(uid=1000)
^C
aditya@aditya-VirtualBox:~$ sudo tail -f /var/log/apache2/access.log
10.1.41.87 - - [20/Apr/2025:14:26:21 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1683 "-" "Mozilla/5.0 (Hydra)"
10.1.41.87 - - [20/Apr/2025:14:26:21 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1683 "-" "Mozilla/5.0 (Hydra)"
10.1.41.87 - - [20/Apr/2025:14:26:21 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1683 "-" "Mozilla/5.0 (Hydra)"
10.1.41.87 - - [20/Apr/2025:14:26:21 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1683 "-" "Mozilla/5.0 (Hydra)"
127.0.0.1 - - [20/Apr/2025:14:28:01 +0530] "GET /favicon.ico HTTP/1.1" 404 488 "http://localhost/dvwa/login.php" "Mozilla/5.0 (X11; Ubuntu; Linux
x86_64; rv:137.0) Gecko/20100101 Firefox/137.0"
127.0.0.1 - - [20/Apr/2025:14:28:50 +0530] "GET /dvwa/favicon.ico HTTP/1.1" 200 1707 "http://localhost/dvwa/index.php" "Mozilla/5.0 (X11; Ubuntu;
Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0"
127.0.0.1 - - [20/Apr/2025:14:28:55 +0530] "GET /dvwa/ HTTP/1.1" 302 394 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Fir
efox/137.0"
127.0.0.1 - - [20/Apr/2025:14:28:55 +0530] "GET /dvwa/login.php HTTP/1.1" 200 955 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/201
00101 Firefox/137.0"
```

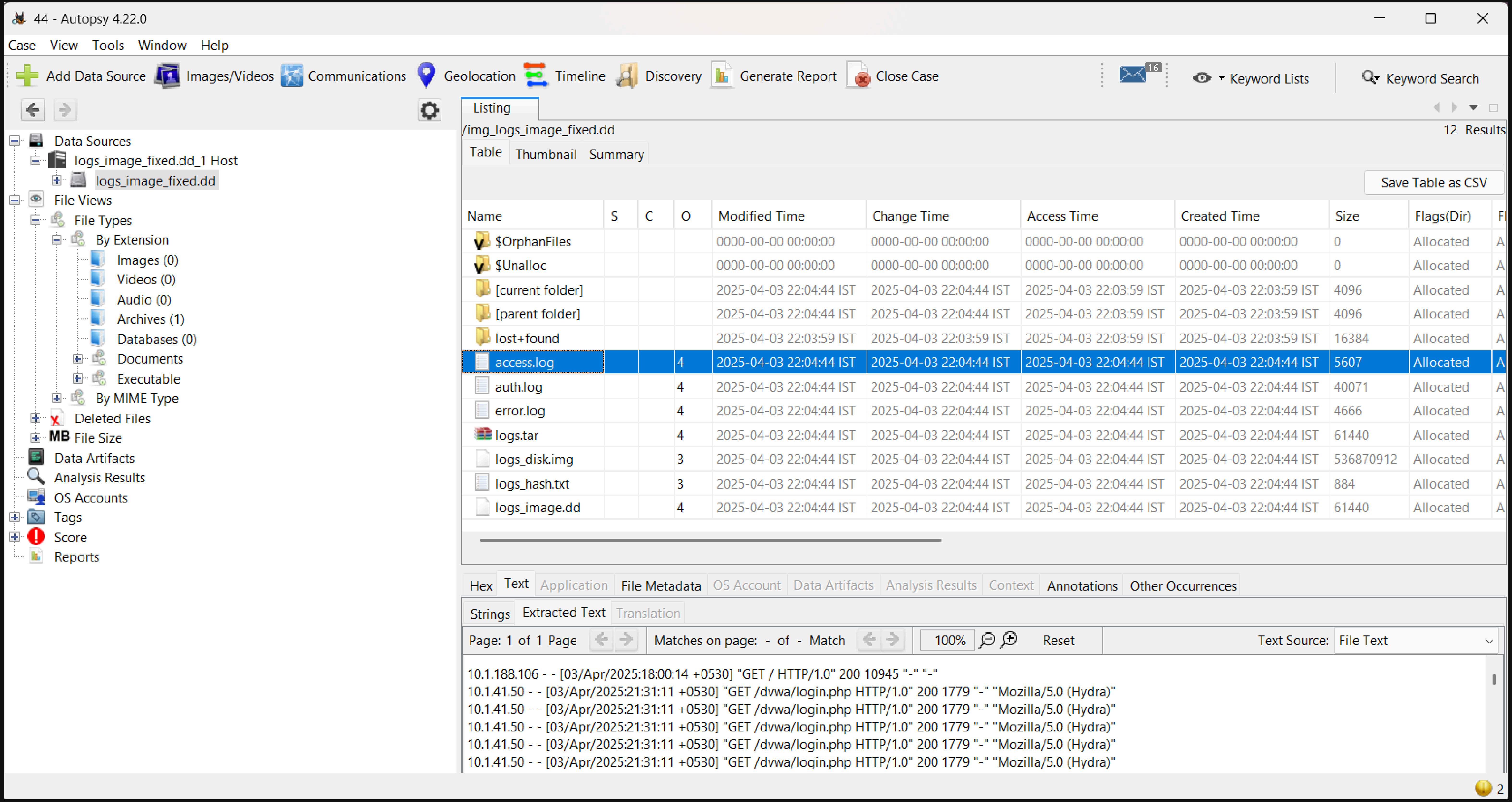
ATTACKER (KALI LINUX)



```
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.1.41.89 http-post-form
"/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mil
itary or secret service organizations, or for illegal purposes (this is non-bindi
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-20 14:26:1
8
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:1
4344399), ~896525 tries per task
[DATA] attacking http-post-form://10.1.41.89:80/dvwa/login.php:username=^USER^&pa
ssword=^PASS^&Login=Login:Login failed
[80][http-post-form] host: 10.1.41.89   login: admin   password: rockyou
[80][http-post-form] host: 10.1.41.89   login: admin   password: 12345
[80][http-post-form] host: 10.1.41.89   login: admin   password: iloveyou
[80][http-post-form] host: 10.1.41.89   login: admin   password: 123456
[80][http-post-form] host: 10.1.41.89   login: admin   password: 123456789
[80][http-post-form] host: 10.1.41.89   login: admin   password: princess
[80][http-post-form] host: 10.1.41.89   login: admin   password: abc123
[80][http-post-form] host: 10.1.41.89   login: admin   password: nicole
[80][http-post-form] host: 10.1.41.89   login: admin   password: lovely
[80][http-post-form] host: 10.1.41.89   login: admin   password: monkey
[80][http-post-form] host: 10.1.41.89   login: admin   password: babygirl
[80][http-post-form] host: 10.1.41.89   login: admin   password: 1234567
[80][http-post-form] host: 10.1.41.89   login: admin   password: daniel
[80][http-post-form] host: 10.1.41.89   login: admin   password: jessica
[80][http-post-form] host: 10.1.41.89   login: admin   password: 12345678
```

AUTOPSY (WINDOWS)



/img_logs_image_fixed.dd 12 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Fl
$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	A
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	A
[current folder]				2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:03:59 IST	2025-04-03 22:03:59 IST	4096	Allocated	A
[parent folder]				2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:03:59 IST	2025-04-03 22:03:59 IST	4096	Allocated	A
lost+found				2025-04-03 22:03:59 IST	2025-04-03 22:03:59 IST	2025-04-03 22:03:59 IST	2025-04-03 22:03:59 IST	16384	Allocated	A
access.log			4	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	5607	Allocated	A
auth.log			4	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	40071	Allocated	A
error.log			4	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	4666	Allocated	A
logs.tar			4	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	61440	Allocated	A
logs_disk.img			3	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	536870912	Allocated	A
logs_hash.txt			3	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	884	Allocated	A
logs_image.dd			4	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	2025-04-03 22:04:44 IST	61440	Allocated	A

Text Source: File Text

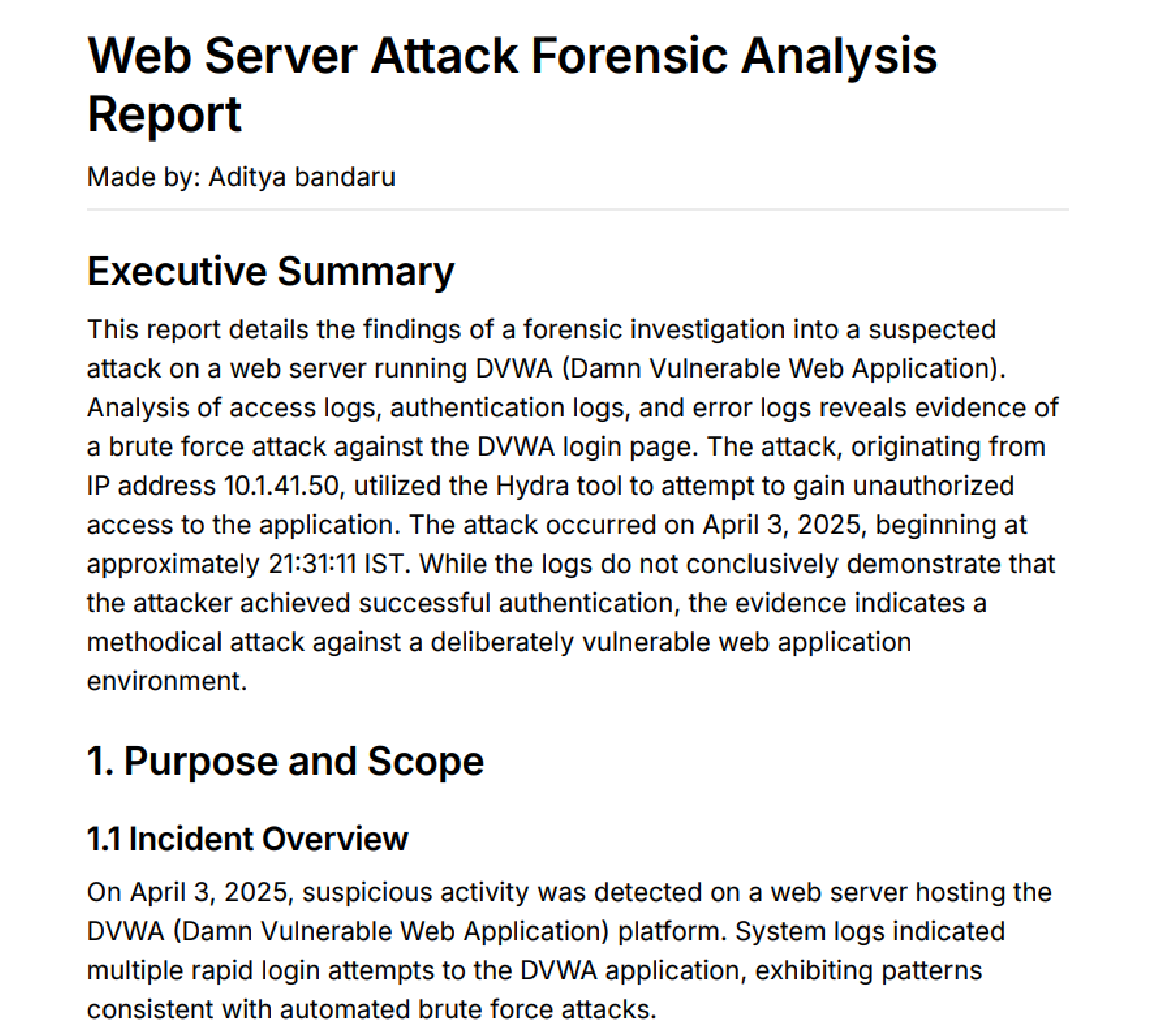
```
10.1.188.106 - - [03/Apr/2025:18:00:14 +0530] "GET / HTTP/1.0" 200 10945 "-" "-"
10.1.41.50 - - [03/Apr/2025:21:31:11 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1779 "-" "Mozilla/5.0 (Hydra)"
10.1.41.50 - - [03/Apr/2025:21:31:11 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1779 "-" "Mozilla/5.0 (Hydra)"
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/2025:21:31:11 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1779 "-" "Mozilla/5.0 (Hydra)"
10.1.41.50 - - [03/Apr/2025:21:31:11 +0530] "GET /dvwa/login.php HTTP/1.0" 200 1779 "-" "Mozilla/5.0 (Hydra)"
```

CONCLUSION & FUTURE SCOPE

At the end of this project:

- Successfully created a forensic image (.dd) from compromised server log files.
- Analyzed the image using Autopsy to extract attack traces and evidence.
- Identified attacker IPs, failed login attempts, and malicious requests.
- Generated a detailed forensic report to aid future security improvements.

FORENSIC REPORT



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.

Click to view full report:

Forensic Report

THANK YOU!

Aditya bandaru

AP22110011563