Buildables Fellowship

Buildables Cybersecurity Capstone Project

- **Title: Investigate, Exploit, Analyze, and Report a Simulated Cyber Attack**
- **Environment:** Kali Linux (attacker), DVWA/Metasploitable (victim)
- **FINAL REPORT (Days 1–6)**
- **Fellow:** Muhammad Zohaib

1. Executive Summary (Non-Technical Overview)

A controlled cyberattack was simulated inside a virtual lab to understand how real attacks happen and how a security team responds.

The attacker targeted a vulnerable web application (DVWA) and successfully exploited a **command injection vulnerability**, gaining the ability to run system commands on the server.
The investigation showed signs of the attack in logs, network traffic, and modified files. A complete response plan and security policy were created based on these findings.

Impact Summary:

- Unauthorized command execution
- Access to sensitive system files
- Tampering with web directory

Final Result:
We demonstrated the full security lifecycle:

recon → exploitation → forensics → detection → response → policy improvement.

2. Reconnaissance Findings (Day 1)

Target Discovery

- Kali attacker identified victim IP using ifconfig + ping sweep.
- Performed basic Nmap scan:

```
nmap -sV 192.168.1.67
```

Key Open Ports

Port	Service	Version	Risk
22	SSH	OpenSSH	Medium
80	Apache Web Server	2.x	High
3306	MySQL	5.x	Medium
139/445	SMB	Samba	High

Possible Exploitable Points

- DVWA running on port 80 with low security settings
- FTP (vsftpd) known backdoor version
- Outdated Apache + PHP
- Weak web application input validation

3. Exploitation Walkthrough (Day 2)

Vulnerability Selected:

Command Injection (DVWA – Low Security)

How the Vulnerability Works

The application takes user input (an IP address) but does not filter out special characters like ;. This allows attackers to append system commands.

Example malicious input:

```
8.8.8.8; cat /etc/passwd
```

DVWA executes the entire string, resulting in:

- Ping to `8.8.8.8`
- PLUS execution of cat /etc/passwd on the server

Exploitation Steps

1. Navigate to **DVWA → Command Injection**
2. Enter payload:
3. 8.8.8.8; cat /etc/passwd
4. Server returned system file → proves remote code execution.
5. Attacker created/deleted test files using similar commands.

DVWA interface

Mentioned On linkedin

https://www.linkedin.com/posts/muhammad-zohaib-46436a282_cybersecurity-infosec-websecurity-activity-7384654505348333570-1O6e?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETAsAwBZoUAQNM3nJFz-LbZiBX3XJdqsXI

4. Forensic Evidence & Analysis (Day 3)

Log Evidence

Apache Access Log

```
GET /dvwa/vulnerabilities/exec/?ip=8.8.8.8;cat%20/etc/passwd
```

Auth Log

www-data executed command: `cat /etc/passwd`

Indicates web server user triggered OS-level commands.

System Logs

Show file creation and timestamp changes in /var/www/html/.

File System Evidence

- Used **Autopsy** and Linux tools to review file changes
- Found modified or newly created files
- Recovered deleted file test.txt showing attacker activity

Forensic Conclusion

The system was successfully exploited; malicious actions were logged, timestamped, and fully re-constructable.

5. Detection & Threat Analysis (Day 4)

How SOC Detected the Attack

- Unusual URL patterns caught in logs
- RCE indicators: www-data executing commands
- Wireshark captured malicious HTTP payloads
- Large response sizes indicated sensitive file exfiltration

Kill Chain Mapping

Stage	Evidence
Recon	Nmap scans
Weaponization	Crafted payload ; cat /etc/passwd
Delivery	HTTP GET request
Exploitation	RCE via DVWA
Installation	File creation on server

Alerts Created

1. **Command Injection URL Pattern Alert**
2. **Web User OS Command Execution Alert**
3. **Abnormal File Changes Alert**
4. **High Response Size Alert**
5. **Unauthorized Directory Access Alert**

6. Response & Remediation Plan (Day 5)

Incident Response (IR) Steps

Identification

Discovered malicious URL patterns and unauthorized command execution.

Containment

- Block attacker IP
- Disable vulnerable page
- Stop Apache temporarily

Eradication

- Patch DVWA and server components
- Remove attacker artifacts
- Ensure no backdoors remain

Recovery

- Restore clean files from backups
- Restart services
- Increased monitoring for 72 hours

Remediation Controls

1. Patch management
2. Firewall rules & segmentation
3. Strong passwords & MFA
4. Principle of least privilege
5. Backup & recovery strategy
6. WAF for web application protection
7. Centralized logging + SIEM

Small Business Security Policy (Summary)

- Acceptable use
- Password & MFA rules
- System hardening
- Log monitoring
- Backup policy
- Web app security (OWASP guidelines)
- Incident response steps
- Mandatory cybersecurity training

FINAL SUMMARY

This project demonstrated the full lifecycle of a cyber incident—from discovering a vulnerable service all the way to exploitation, forensics, detection, and response.
The final deliverable includes both technical and non-technical explanations, suitable for SOC teams and business leadership.