🗒️ Task 5 – Incident Response & Forensics

Intern: Deepak Kumar Rajbhar
Offer Letter ID: APSPL2520740
Duration: Days 49–60
Internship Domain: Cybersecurity & Ethical Hacking

🎯 Objective

To learn how to detect, respond to, and analyze cybersecurity incidents using forensic tools and logs. Perform log collection, evidence preservation, and forensic investigation on a simulated attack scenario.

⚙️ Environment & Tools Used

Kali Linux / Windows (forensic analysis)

Autopsy / FTK Imager / Volatility / Wireshark

Event Viewer / Log Parser / Log2Timeline

Browser History & Registry Analyzer

Linux log tools (grep, cat /var/log/auth.log, etc.)

🪜 Practical Steps / Tasks

1) Simulate an Incident

Create a controlled security breach such as:

Unauthorized login attempts

Malware execution or data exfiltration simulation

2) Evidence Collection

Capture memory dump using Volatility or DumpIt

Collect log files from:

Windows Event Viewer (Security, System, Application logs)

Linux /var/log/ directory

3) Forensic Analysis

Analyze system logs for suspicious activity

Review timestamps, file modifications, and login attempts

Examine browser history and registry keys for abnormal entries

4) Tool Usage

Use Autopsy to open a forensic image and locate deleted files

Use Wireshark to track suspicious network packets or attacker IPs

Use Volatility for memory forensics (commands like pslist, netscan, dlllist)

5) Reporting Findings

Prepare a timeline of attack:

Entry point

Actions taken by attacker

Data compromised

Suggest mitigation and prevention methods

6) Mitigation Steps

Change compromised credentials

Apply OS patches and updates

Enable SIEM/IDS alerting

Conduct periodic log review

📸 Screenshot Placeholders

(Insert your actual screenshots in these sections while creating PDF)

1. System logs showing suspicious activity

2. Autopsy forensic analysis result

3. Wireshark capture of attack trace

4. Volatility analysis (memory dump)

5. Recovered deleted files or browser history

6. Incident timeline diagram

📘 Report Structure (Use This Format)

1. Executive Summary

2. Tools & Setup

3. Evidence Collection (commands, logs)

4. Forensic Analysis (Autopsy, Volatility, Wireshark)

5. Findings & Timeline

6. Mitigation Recommendations

7. Conclusion

🎥 Video Script (8 Minutes Demo)

Intro (20s):
“Hello, my name is Deepak Kumar Rajbhar. This is Task-5 Incident Response & Forensics walkthrough.”

Incident Simulation (60s):
Show unauthorized login attempt or malware alert.

Evidence Collection (90s):
Show how you collected logs and memory dump.

Analysis (90s):
Show Autopsy or Volatility output and explain findings.

Network Analysis (60s):
Demonstrate Wireshark packets and attacker IP trace.

Timeline & Findings (60s):
Summarize attack sequence and response.

Mitigation (40s):
Explain preventive steps (patches, passwords, monitoring).

Conclusion (30s):
Summarize what was learned and mention your GitHub link.

🗒️ Portal Submission Text (Copy-Paste Ready)

Full Name: Deepak Kumar Rajbhar
Email ID: gk1978307@gmail.com
Degree Course: BCA (Cyber Security Specialization)
Internship Domain Name: Cybersecurity & Ethical Hacking
Offer Letter ID: APSPL2520740
Explanation Video Task-5: <Paste your LinkedIn Video Link here>
GitHub Repository Link Task-5: <Paste your GitHub repo link here>

⚠️ Ethical Note

Perform all testing only in your lab environment. Never attempt forensic analysis on unauthorized systems. Always maintain integrity of evidence and use proper tools for analysis.