# Lab #12 – Solved

## Objective:

- To understand the key phases of incident response.

- To simulate an incident response process using a real-world scenario.

- To perform root cause analysis (RCA) on the identified security incident.

- To document findings and recommend preventative measures.

## Prerequisites:

- Basic knowledge of cybersecurity principles.

- Familiarity with network and system logs.

- Understanding of operating system (Linux/Windows) commands.

- Tools: Wireshark, Event Viewer, Splunk (optional), ELK Stack (optional), or any log analysis tool.

## Tools & Software Required:

- Virtual Machine (Kali Linux, Windows)

- Wireshark

- Sysinternals Suite / Event Viewer

- Text Editor (Notepad++, Sublime, etc.)

- Internet connection for updates/tools

## Lab Setup:

- Prepare two virtual machines: Attacker (Kali Linux), Victim (Windows/Ubuntu).

- Ensure logging is enabled on the victim machine: System, Security, Application Logs.

- Set up basic services (SSH, HTTP server) for exploitation.

## Lab Procedure:

### Part A: Simulating an Incident

- Used Nmap to discover open ports on the victim system.

- Launched a brute force attack using Hydra on SSH service.

- Monitored Event Viewer and Wireshark for detection of abnormal login attempts.

- Captured suspicious traffic and login failures.

### Part B: Incident Response Process

- [Preparation] Verified logs are functional and assigned roles.

- [Identification] Detected multiple failed login attempts via Event Viewer.

- [Containment] Blocked attacker's IP using firewall rules.

- [Eradication] Removed any detected malicious scripts and patched services.

- [Recovery] Restarted affected services and ensured normal operation.

- [Lessons Learned] Documented the timeline and recommendations.

### Part C: Root Cause Analysis (RCA)

- [Define the Problem] Multiple unauthorized login attempts detected on SSH.

- [Collect Data] Reviewed system logs, Wireshark captures, and Event Viewer.

- [Identify Root Cause] Weak password policy identified as the entry point.

- [Corrective Actions] Enforced strong password policies, updated firewall rules, and reviewed incident playbooks.

## Observations and Screenshots:

Included logs of failed SSH logins, Wireshark packet capture of brute-force attack, and blocked IP entries.

## Results:

Incident: Brute force attack on SSH service detected using Event Viewer and Wireshark.

Detection: Multiple failed login attempts and suspicious IP detected.

Root Cause: Weak SSH password and open port exposure.

Mitigation: Blocked attacker's IP, enforced password policy, patched system.

## Conclusion:

The lab demonstrated the importance of a structured incident response plan. Root Cause Analysis helped identify underlying weaknesses and led to improved system security.

## Viva Questions – Sample Answers

* Q: What are the six phases of the incident response lifecycle?

A: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned.

* Q: How does containment differ from eradication?

A: Containment isolates the threat; eradication removes it from the system.

* Q: What is the purpose of root cause analysis?

A: To identify the underlying cause of an incident and prevent recurrence.

* Q: What tools can be used for RCA?

A: 5 Whys, Fishbone Diagram, Timeline Analysis.

* Q: Explain the 5 Whys technique.

A: A method of asking 'Why?' five times to drill down to the root cause of a problem.