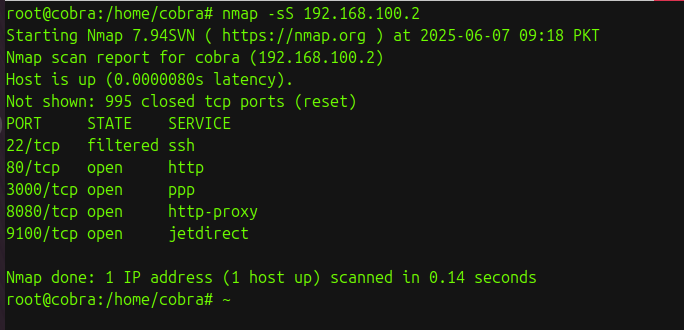
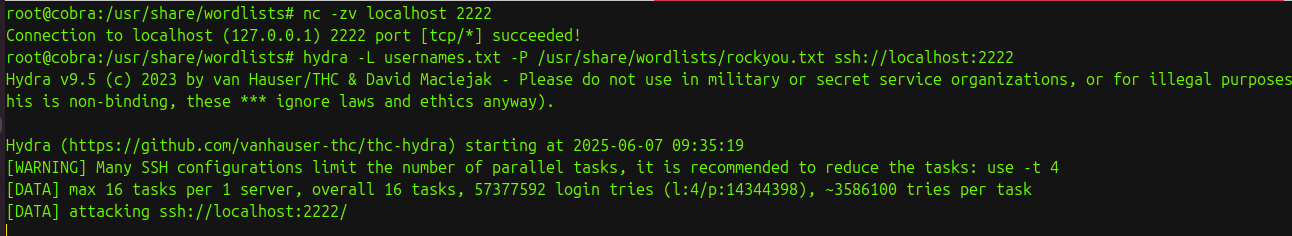
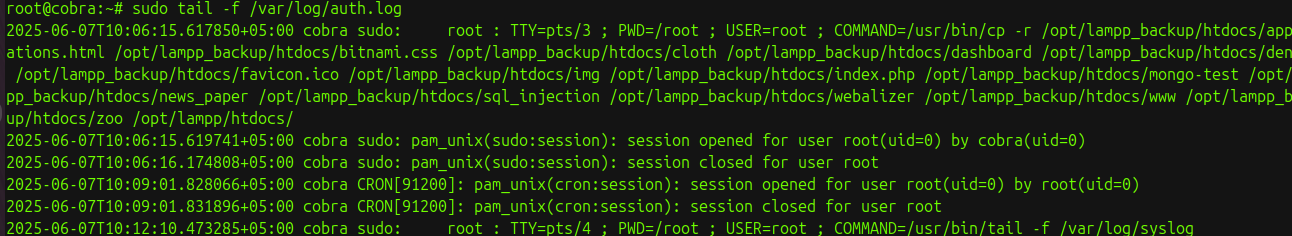
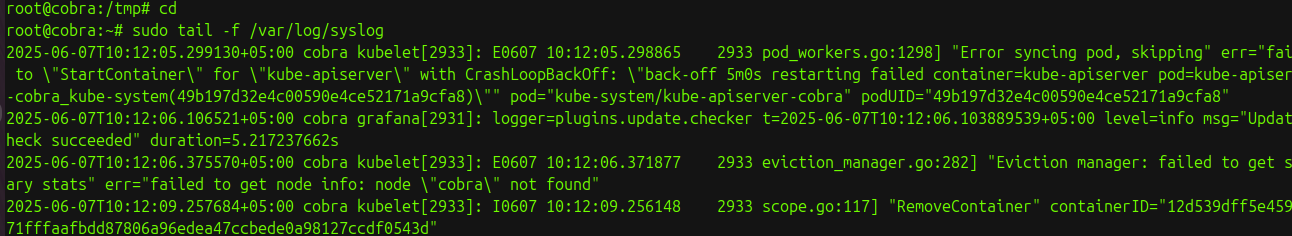
**1.Scanning Victim Machine (Nmap):**



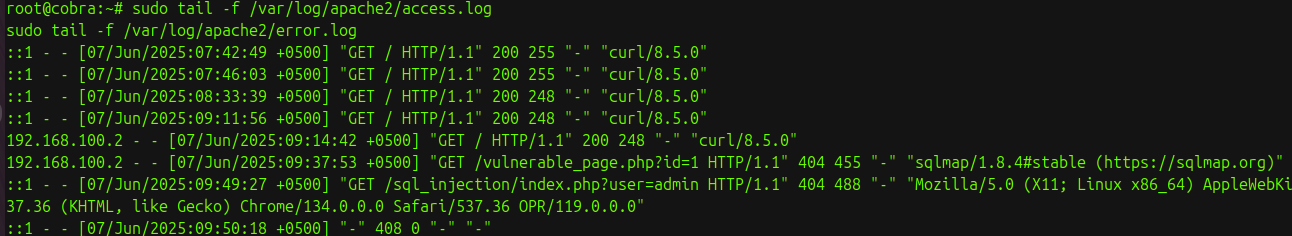
**2. Brute Force Attack using Hydra (SSH example)**



**4.Monitor Logs on Victim Machine:**

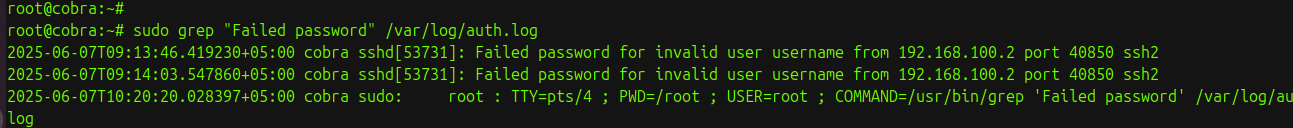


**Description:**(Security log,System log,Application log)



**5.Capture Network Traffic (tcpdump)**

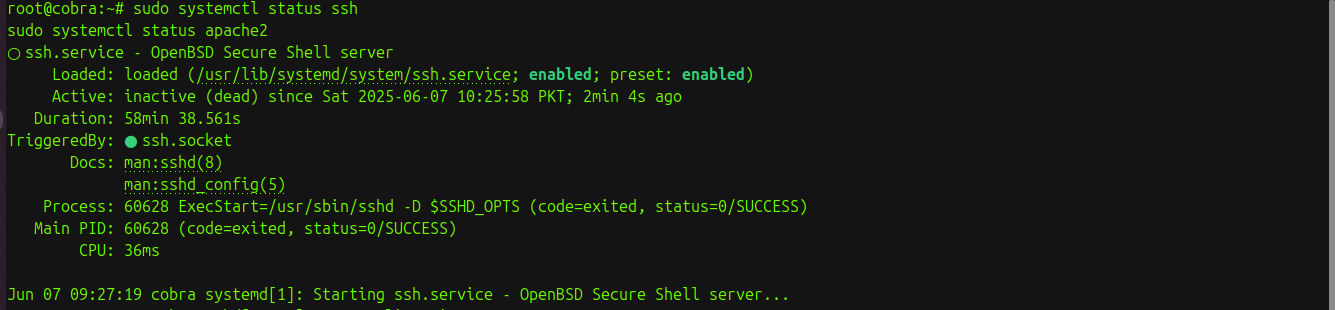
**6.Check Failed Login Attempts**



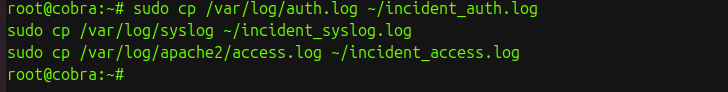
**7. Isolate Victim Machine (Containment) — Block IP using UFW (Uncomplicated Firewall)**



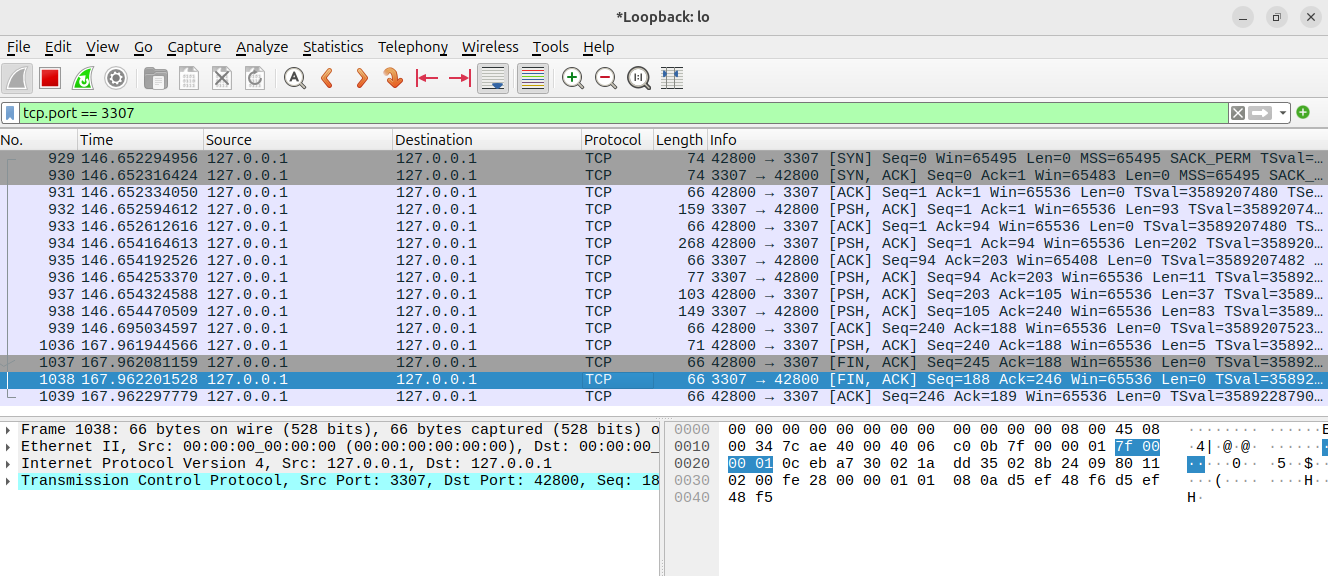
**8.Verify Service Status**



**9.Document Logs for Post-Mortem (Save current logs)**



**10.Use Wireshark to monitor SQL-injection:**



**11. Conclusion:**

Summarize key learnings:

* Importance of structured incident response
* Value of RCA in preventing repeat incidents
* Real-world significance in a cybersecurity operations center (SOC)

**10. Viva Questions (Oral Evaluation):**

1. What are the six phases of the incident response lifecycle?  
 Ans:

* Preparation: Getting ready with policies, tools, and training.
* Identification: Detecting and confirming an incident.
* Containment: Limiting the incident’s impact to prevent further damage.
* Eradication: Removing the cause of the incident (like malware).
* Recovery: Restoring systems back to normal operation.
* Lessons Learned: Reviewing the incident to improve future responses.

2. How does containment differ from eradication?  
 Ans:  
 Containment is about stopping the incident from spreading or causing more damage, often temporarily isolating affected systems. Eradication is the process of completely removing the threat or vulnerability causing the incident.

3. What is the purpose of root cause analysis?  
 Ans:  
 Root cause analysis (RCA) helps identify the fundamental reason an incident occurred so that organizations can fix the problem and prevent similar incidents in the future.

4. What tools can be used for RCA?  
 Ans:  
 Common tools include log analyzers to review system logs, forensic tools to examine affected systems, network analyzers to inspect traffic, and monitoring tools that track system behavior over time.

5. Explain the 5 Whys technique.  
 Ans:  
 The 5 Whys is a problem-solving method where you ask "Why?" repeatedly (typically five times) to peel back layers of symptoms and reach the core cause of an issue.