Digital Forensics Lab

Cyber Security Department

CYL-2002

Fall 2024

Lab #12

Instructor:

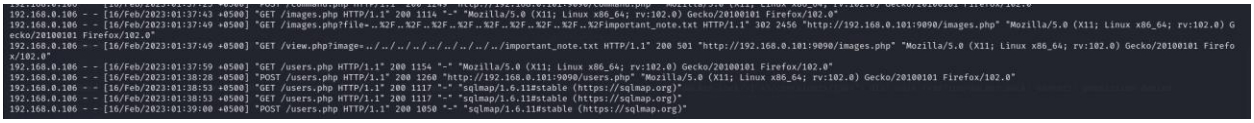
Ubaid Ullah

Fahad Waheed

You are a cyber security specialist who has been called upon to investigate a major cyber security breach. The company's web server has been compromised, and the attacker has attempted to exploit multiple vulnerabilities. You've been given the task of piecing together the attacker's intentions and uncovering the extent of the damage. With that in mind, your challenge is to answer the following questions:

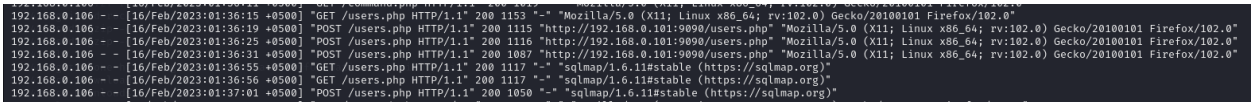
1. What IP address does the attack seem to be originating from?

   192.168.0.106



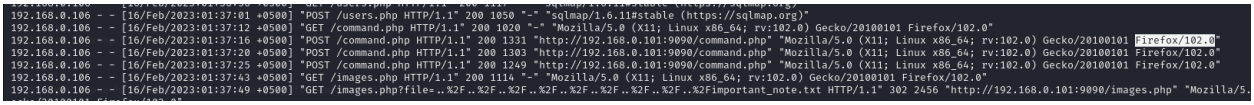
2. Which vulnerabilities do you think are being exploited, and what evidence do you have to support your findings?

   - Path Traversal
   - Remote File Inclusion
   - SQL Injection
   - Command Injection



3. How can we determine what web browser the attacker is using?

   Firefox 102



4. Did the attacker use any automated tools during the attack? If so, can you identify the name of the tool and its purpose?

   Attacker used sqlmap for sql injection

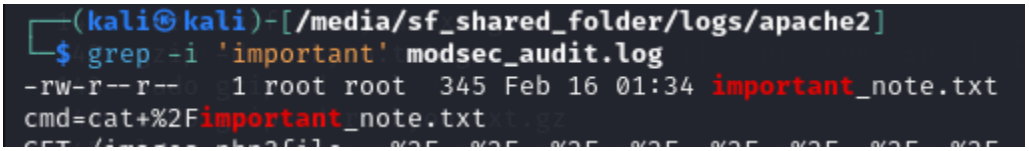
5. Which file was the attacker trying to access but couldn't due to limited server access?

/database.php

6. Did the attacker gain access to any confidential data? If yes, how much data was compromised?

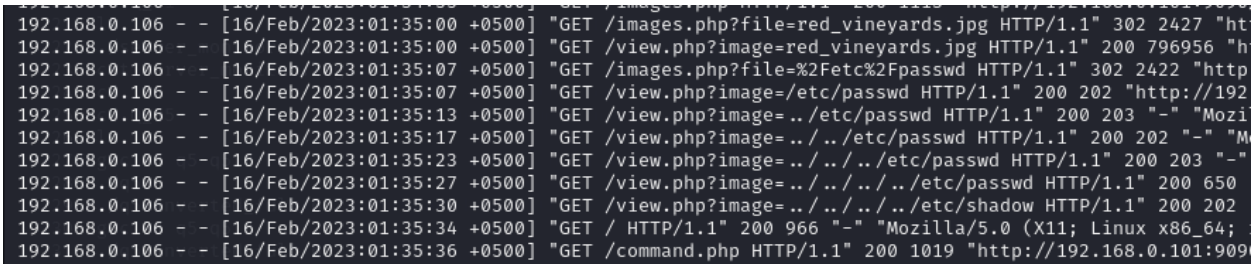
The /etc/passwd was compromised.

7. An important secret was compromised. Can you figure it out? Hint: The secret you're looking for is not in a .sql or a .php file.



8. The attacker left a message for the server administrator. Find out what the message said, and also mention how you were able to find it.

9. What were some indicators that confirmed that an attack had taken place? What were your key takeaways from this attack?



10. Based on this attack, what indicators of compromise can be used to detect future attacks?

- logs and alert are to be used to detect future attacks.
- Monitor logs and alerts
- Use IDS and IPS