Week 4 - Practical Task: The Web Shell

Objective

This task simulates a "threat hunt" where you must use *two different log sources* (firewall and web server) to find an attack. You must correlate events across logs to tell the full story.

Scenario

You are a Tier 1 Analyst on a "threat hunt." The web team reported the main website (www.company.com / 10.0.0.5) "feels slow," but no alerts have fired. You decide to look for anomalous activity.

You pull all logs from the last hour for further analysis.

Log Export (Firewall & Web Server)

Log Source 1: firewall.log
Format: Timestamp | action | src_ip | dest_ip | dest_port
14:28:01 | ALLOW | 100.17.5.10 | 17.1.0.5 | 53
14:30:01 | DENY | 88.198.5.10 | 10.0.0.5 | 22
14:30:02 | DENY | 88.198.5.10 | 10.0.0.5 | 3389
14:30:03 | DENY | 88.198.5.10 | 10.0.0.5 | 445
14:30:04 | ALLOW | 88.198.5.10 | 10.0.0.5 | 80
14:30:05 | ALLOW | 88.198.5.10 | 10.0.0.5 | 80
14:30:05 | ALLOW | 100.17.5.10 | 17.1.0.5 | 80
14:30:06 | ALLOW | 88.198.5.10 | 10.0.0.5 | 80
14:30:06 | ALLOW | 100.17.5.10 | 17.1.0.5 | 80
14:30:07 | ALLOW | 88.198.5.10 | 10.0.0.5 | 80
14:30:08 | ALLOW | 88.198.5.10 | 10.0.0.5 | 80
14:30:09 | DENY | 100.17.5.10 | 17.1.0.5 | 443
14:30:09 | ALLOW | 88.198.5.10 | 10.0.0.5 | 80
14:30:10 | ALLOW | 88.198.5.10 | 10.0.0.5 | 80
14:30:15 | DENY | 100.17.5.10 | 17.1.0.5 | 80

Log Source 2: webserver.log
Format: Timestamp | src_ip | method | uri | status_code | user_agent
14:30:04 | 88.198.5.10 | GET | /index.html | 200 | curl/7.68
14:30:05 | 88.198.5.10 | GET | /admin.php | 404 | curl/7.68
14:30:05 | 100.17.5.10 | GET | /secret.php | 301 | curl/7.68
14:30:06 | 88.198.5.10 | GET | /config.txt | 404 | curl/7.68
14:30:07 | 100.17.5.10 | GET | /soup.img | 302 | curl/7.68
14:30:07 | 88.198.5.10 | GET | /backup.zip | 404 | curl/7.68

14:30:08 | 88.198.5.10 | GET | /upload.php | 200 | curl/7.68
14:30:09 | 100.17.5.10 | POST | /secret.php | 200 | curl/7.68
14:30:09 | 88.198.5.10 | POST | /upload.php | 200 | curl/7.68
14:30:10 | 100.17.5.10 | GET | /uploads/shell.php?cmd=ifconfig | 200 | curl/7.68
14:30:10 | 88.198.5.10 | GET | /uploads/shell.php?cmd=whoami | 200 | curl/7.68

Your Task

Analyze both log files and answer the following questions.

1. **Firewall Analysis:**
    - What is the attacker's IP address? What is the server's IP?
    - What 3 ports did the attacker try to connect to that were **blocked**?
    - What is one port that was **open**?
2. **Web Server Analysis:**
    - The attacker starts scanning the web server. What 3 *filenames* did they look for that **did not exist**?
    - What *filename* did they find that **did exist**?
    - What user_agent is the attacker using? Does this look like a normal web browser?
3. **The Breach (Correlation):**
    - At 14:30:09, the attacker makes a POST request. What do you think they were doing?
    - At 14:30:10, the "smoking gun" appears. What is the **full URI** of this request?
    - What *specific command* did the attacker run on the server?
4. **Tying it to Frameworks:**
    - What **MITRE ATT&CK Tactic** does the stream of 404 errors represent?
    - What **MITRE ATT&CK Technique** is shell.php?cmd=whoami?
5. **Final Recommendation:**
    - Is this a **True Positive** or a **False Positive**?
    - What is your **immediate next step** for the web server?
    - What is your **immediate next step** for the attacker's IP?

Submission

- Please write up your answers to these 5 questions in a .txt or .md file.
- Submit the file to the Google Classroom assignment.