1. Lab Title & Source

Webstrike - Cyberdefenders

---

2. Objective

Analyze the PCAP file to determine the origins and determine the extent of the malicious activity.

---

3. Tools & Technologies Used

List all tools (include versions if possible).

- **Packet Analysis:** Wireshark 4.2
- **IP Finder:** https://ipgeolocation.io

---

4. Scenario Summary

Briefly describe the environment or the incident scenario.
Example:

> A simulated corporate network experienced unusual outbound traffic to suspicious domains. PCAP logs were captured for analysis to determine if malware was present and what data may have been exfiltrated.

---

5. Methodology / Steps Taken

1. Loaded and filtered PCAP in Wireshark.
2. Mapped attacker's IP to geographic origin.
3. Extracted User-Agent from HTTP metadata.
4. Tracked upload of malicious web shell (`image.jpg.php`).
5. Located upload directory on server.

6. Identified reverse shell port (8080).

7. Captured exfiltration attempt via `curl` posting `/etc/passwd`.

---

6. Findings & IOCs

- **Attacker IP:** Originated from Tianjin, China.
- **User-Agent:** Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/117.0 (used in malicious requests).
- **Malicious File:** Web shell uploaded as image.jpg.php.
- **Upload Directory:** /reviews/uploads/.
- **Reverse Shell Port:** TCP port 8080 used for attacker communication.
- **Targeted File for Exfiltration:** /etc/passwd accessed via curl POST request.
-
- **Tactics & Techniques:**
- **T1190 – Exploit Public-Facing Application** (uploading malicious PHP shell through a vulnerable web form).
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell** (executing commands via the uploaded shell).
- **T1505.003 – Server Software Component: Web Shell** (maintaining access via the PHP shell).
- **T1071.001 – Application Layer Protocol: Web Protocols** (reverse shell traffic over HTTP port 8080).
- **T1041 – Exfiltration Over C2 Channel** (sending `/etc/passwd` over established connection).

---

7. Skills Demonstrated

- **PCAP Analysis & Network Forensics** – Used Wireshark to filter traffic, follow streams, and identify malicious activity.
- **Indicator of Compromise (IOC) Extraction** – Pulled attacker IPs, malicious file names, ports, and User-Agent strings from network data.
- **Threat Actor Profiling** – Correlated IP with geolocation to help profile the attacker's origin.
- **Web Attack Detection** – Identified malicious PHP web shell upload via HTTP POST requests.
- **Command & Control (C2) Analysis** – Determined reverse shell traffic patterns and communication port (8080).
- **Exfiltration Detection** – Traced data theft activity (`/etc/passwd`) from attacker commands.
- **MITRE ATT&CK Mapping** – Mapped observed attacker behavior to relevant TTPs for structured reporting.
- **Incident Reporting** – Organized findings into a clear investigative sequence for escalation.