1. Lab Title & Source

PacketMaze – CyberDefenders

---

2. Objective

Analyze the provided network traffic (PCAP) to investigate unusual outbound connections and potential data exfiltration, using multiple protocols—FTP, DNS, TLS, HTTP—to extract IOCs and determine the method of compromise.

---

3. Tools & Technologies Used

- **Wireshark** – Core tool for filtering and dissecting packets across various protocols (FTP, DNS, TLS, HTTP)

---

4. Scenario Summary

A corporate server exhibited abnormal outbound traffic to an unknown external IP, raising suspicions of insider activity or data exfiltration. Analysts are given network captures and must analyze packet-level data to track the attacker's actions and uncover artifacts.

---

5. Methodology / Steps Taken

Based on official instructions and detailed write-ups:

1. Load the PCAP into **Wireshark** and review protocol distribution (FTP, DNS, HTTP, TLS).

2. Filter for **FTP** traffic to extract credentials and file transfer details (e.g., FTP password).

3. Filter **DNS** traffic to identify server addresses and IPv6 queries/responses.
4. Locate specific packets (e.g., packet 15174) to determine domains looked up by the user.

5. Count **UDP packets** between specific IPs (e.g., 192.168.1.26 → 24.39.217.246).
6. Identify the **MAC address** of the monitored system via Ethernet headers. Extract embedded files, such as image `20210429_152157.jpg`, via **FTP-data stream** analysis and view metadata (e.g., camera model).
7. Analyze **TLS sessions**—locate session IDs and extract elements like server public keys and TLS 1.3 client random.
8. Use **MAC lookup tools** to determine geographic registration of a MAC (e.g., FTP server).
9. Investigate **FTP directory listings** to derive timestamps of folder creation (e.g., time of non-standard folder creation).
10. Identify the domain user connected to in a particular packet (e.g., packet 27300) using name resolution.

---

6. Findings & IOCs

Key Discoveries:

- **FTP Password:** `AfricaCTF2021`
- **DNS IPv6 Server Address:** `fe80::c80b:adff:feaa:1db7`
- **Looked-up Domain (Packet 15174):** `www.7-zip.org`
- **Number of UDP Packets (192.168.1.26 → 24.39.217.246):** 10
- **System MAC Address:** `c8:09:a8:57:47:93`
- **Camera Model (Image Metadata):** `LM-Q725K`
- **Server Certificate Public Key (TLS session):** (long hex string)
- **TLS 1.3 Client Random (ProtonMail):** `24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70`
- **MAC Registration Country (FTP server):** United States

- **Non-standard Folder Created (FTP):** Created at `17:53` on April 20
- **Connected Domain (Packet 27300):** `dfir.science`

---

7. Skills Demonstrated

- **Multi-protocol PCAP Analysis** – Skilled at inspecting FTP, DNS, HTTP, TLS traffic using Wireshark.
- **Credential Extraction** – Retrieved cleartext FTP password from network captures.
- **DNS Forensics** – Parsed IPv6 DNS server info and looked up domain behavior.
- **UDP Traffic Analysis** – Quantified specific UDP communication flows.
- **MAC & Hardware Attribution** – Extracted MAC addresses and determined geographic origin.
- **File Extraction & Metadata Analysis** – Exported a JPEG over FTP-data and identified camera model.
- **TLS Decryption Artifacts** – Pulled certificate public key and TLS client random from encrypted sessions.
- **Timeline Crafting** – Used FTP metadata to timestamp suspicious directory creation.
- **Domain Resolution via Packets** – Mapped IP to domain name for specific packet-level activity.
- **Protocol-based Triage Across Multiple Layers** – Demonstrated versatility across a wide range of protocols and extraction methods.