Lab: Wireshark ACME Corporate Breach

Purpose

In this lab, we are going to demonstrate how **Wireshark** can be used to conduct effective forensic investigation in case of data breach in a realistic corporate network.

Pre-Requisite

Before you can start the lab, you need to run the lab script which will setup everything. Open the **Labs** folder on Desktop then right-click and "Open Terminal Here". Or open a terminal and cd to Desktop/Labs folder, then issue the command:

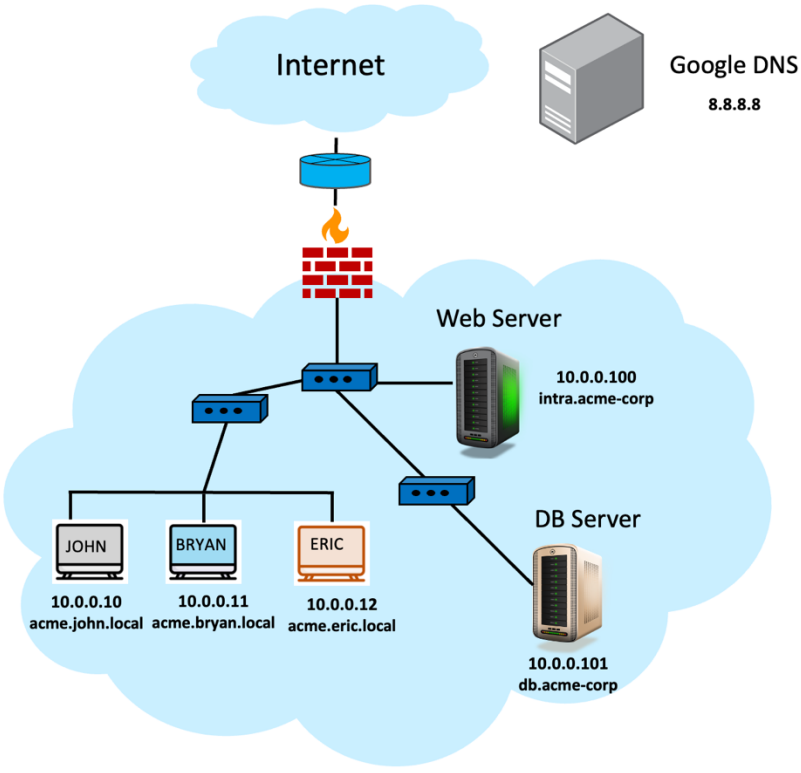
```
sudo ./main_script.sh
```

Select **Wireshark ACME Corporate Breach Lab** option from the lab menu.

Scenario

ACME Corp's security team has been alerted to suspicious activity on their internal network. An alert flagged potential unauthorized access to sensitive data. Your task is to analyse the captured network traffic and reconstruct the sequence of events, especially how the attack happened.

A **pcapng network capture** (`acme-corporate-forensics.pcapng`) from the company's monitoring system has been handed over to you to conduct forensic investigation. Please open the file `/home/kali/Desktop/Labs/wireshark-acme-corporate/acme-corporate-forensics.pcapng` in Wireshark.



LOGIX ACADEMY

Device / Role	Hostname	IP Address
John's workstation	john.acme.local	10.0.0.10
Bryan's workstation	bryan.acme.local	10.0.0.11
Eric's workstation	eric.acme.local	10.0.0.12
Web Server	intra.acme-corp	10.0.0.100
Database Server	db.acme-corp	10.0.0.101
Mail Server	mail.acme-corp	10.0.0.102
DNS Server	Google DNS	8.8.8.8

By the end of this lab, you should be able to:

- Detect and interpret attack vectors
- Analyze DNS queries and HTTP payloads to identify malware activity.
- Trace unauthorized queries to internal servers (e.g., web or database servers).
- Detect and prove data exfiltration.
- Use Wireshark's **display filters** and **TCP stream reconstruction**

Investigation Tasks & Questions

Part 1: Baseline Traffic Familiarization

- Identify any email traffic sent internally — who sent it and what was the content?

Part 2: Attack Detection

- What attack vector was used? remote code execution, brute-force login, or phishing?
- Which employee was the target (give the IP address of his station)?
- (Hint: focus on the usual suspects HTTP, DNS, SMTP traffic).

Part 3: Malware Execution & Communication

- How did the malware installation take place exactly, what was the source of the malware?
- What was the name of the malware process?

Part 4: Internal Database Reconnaissance

- Which internal servers or services did the malware try to access?
- What data was retrieved by the malware running on the compromised system?

Part 5: Data Exfiltration

- Identify the session where the stolen data is exfiltrated to an external IP.
- Is it the same remote IP/host as the one that was involved in malware installation?
- Capture a screenshot of the exfiltrated credentials or salary data

(Solution in next lecture)