# SCENARIO: THE "UNAUTHORIZED ACCESS" ALERT

**Company:** *CYBERCORP Solutions* (a small fintech startup).
**The Incident:** An automated alert was triggered at 11:45 PM on a Tuesday. The alert reported a high volume of traffic hitting the company's **internal file server**, which usually has zero traffic after business hours.

**Your Task:** Analyze the following tcpdump raw output and answer the assessment questions to generate your report.

---

## THE RAW TCPDUMP LOG DATA

```
1. 23:45:01.102341 IP 192.168.1.15.54221 > 10.0.0.5.22: Flags [S], seq 10234567, win 65535, length 0

2. 23:45:01.102554 IP 10.0.0.5.22 > 192.168.1.15.54221: Flags [S.], seq 98765432, ack 10234568, win 28960, length 0

3. 23:45:01.102661 IP 192.168.1.15.54221 > 10.0.0.5.22: Flags [.], ack 1, win 65535, length 0

4. 23:45:05.221342 IP 192.168.1.15.54221 > 10.0.0.5.22: Flags [P.], seq 1:150, ack 1, win 65535, length 149

5. 23:45:06.110443 IP 10.0.0.5.22 > 192.168.1.15.54221: Flags [P.], seq 1:3000, ack 150, win 28960, length 2999

6. 23:45:10.554210 IP 10.0.0.5.22 > 192.168.1.15.54221: Flags [F.], seq 3001, ack 150, win 28960, length 0
```

---

## PRACTICE ASSESSMENT QUESTIONS

**Q1: Identify the Source and Destination.**

- What is the IP address of the **Source**?
- What is the IP address of the **Destination**?

**Q2: Identify the Service/Protocol.**

- What is the **Port Number**?
- What **Service** uses this port?

**Q3: Analyze the "Three-Way Handshake."**

- In lines 1, 2, and 3, you see the [S], [S.], and [.] flags. Did the connection successfully establish?

**Q4: Observe the Data Payload.**

- In line 5, look at the length. It says **2999**.
- In line 4, the source sent a length of **149**.

- Does this look like the source is *sending* information to the server, or *downloading* (extracting) a large amount of information from the server?

**Q5: Incident Status.**

- In line 6, the flag [F.] appears. What does the F flag (FIN) mean happened to the connection?

---

# My Cybersecurity Incident Report:
# CyberCorp Solutions Network Traffic Analysis

## INCIDENT REPORT: UNAUTHORIZED ACCESS & DATA EXFILTRATION

### EXECUTIVE SUMMARY

At 11:45 PM on Tuesday, an automated security alert flagged unusual after-hours traffic on our internal file server. An investigation confirmed a successful TCP SSH connection and the subsequent unauthorized download of approximately 3,000 bytes of data from the server to an internal source IP address.

The business impact is significant, as this incident indicates a potential breach of data confidentiality and integrity, which could lead to regulatory penalties and reputational damage. Immediate actions were taken to contain the threat and notify relevant stakeholders.

### FINDINGS & ANALYSIS

The following key indicators were identified from the tcpdump log data:

- **Incident Timeline:** The activity occurred between 11:45:01pm and 11:45:10pm.
- **Source IP Address:** 192.168.1.15
- **Destination Server:** 10.0.0.5
- **Protocol Used:** TCP SSH (Port 22).
- **Connection Status:** A successful three-way handshake was established.
- **Data Transfer:** A file transfer of **2,999 bytes** was observed moving from the destination server *back* to the source IP. This indicates data was downloaded from our server, not uploaded to it.

## RECOMMENDATIONS

1. **Investigate Source User:** The Security Team will determine if the user of IP 192.168.1.15 was authorized to access the file server via SSH at that hour.
2. **Account Status:** If unauthorized (a malicious actor), the user account associated with the connection will be immediately disabled or reset to prevent further access.
3. **Implement MFA:** I recommend the enforcement of Multi-Factor Authentication (MFA) for all internal file server access to mitigate future credential compromise risks.