Writeup

DFIR

Overview – FTP DoS Incident Investigation

This task focuses on investigating a **Denial-of-Service (DoS) attack** targeting an **FTP server (192.168.56.1)** after abnormal spikes in FTP traffic were detected. The incident resulted in the FTP service becoming unavailable, indicating a potential service disruption caused by malicious activity.

Captured network traffic reveals sustained communication between an **attacking host (192.168.56.101)** and the FTP server prior to the outage. The primary objective of this investigation is to analyze the events leading up to the attack, identify the techniques used against the FTP service, and assess the overall impact on the system.

The analysis aims to determine whether the traffic spike was caused by **brute-force attempts, excessive authentication requests, or misuse of FTP commands**, and whether the attacker successfully authenticated to the server. Additionally, the investigation evaluates if any **unauthorized actions** occurred, such as file access, modification, or data exfiltration.

By correlating FTP command activity, authentication attempts, and traffic patterns, this investigation seeks to establish a clear timeline of events and provide insight into how the attack was executed and its consequences on the FTP service.

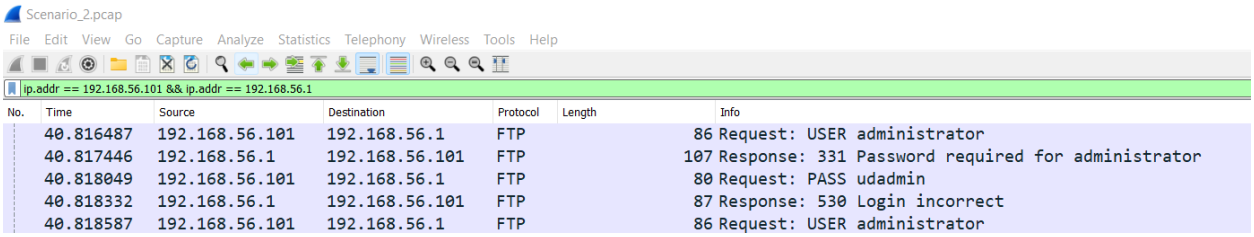
Scope of Investigation

- Analyze FTP traffic spikes preceding the outage
- Review authentication attempts and FTP command usage
- Identify signs of DoS techniques (brute force, connection flooding)
- Assess attacker success and impact on data and service availability

---

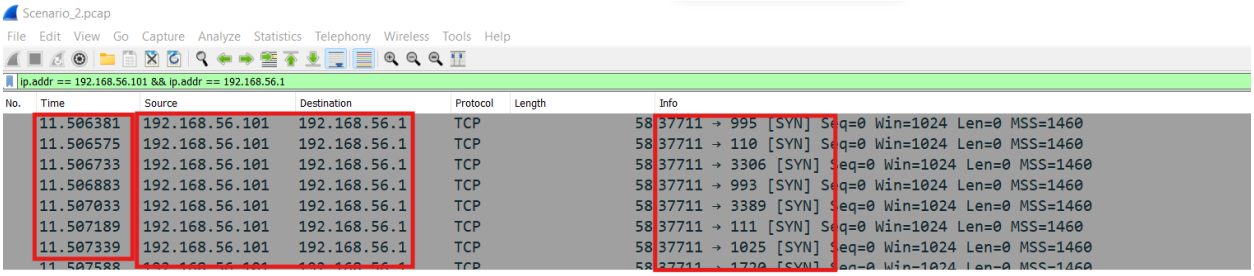
Step 1 – Initial Traffic Analysis

The investigation began by filtering captured network traffic in **Wireshark** using the provided IP addresses of the FTP server (**192.168.56.1**) and the suspected attacking host (**192.168.56.101**).



Early analysis revealed several unusual indicators consistent with a **Denial-of-Service (DoS) attack**:

- The **time intervals between successive packets** from the attacker were extremely short, suggesting rapid-fire requests.



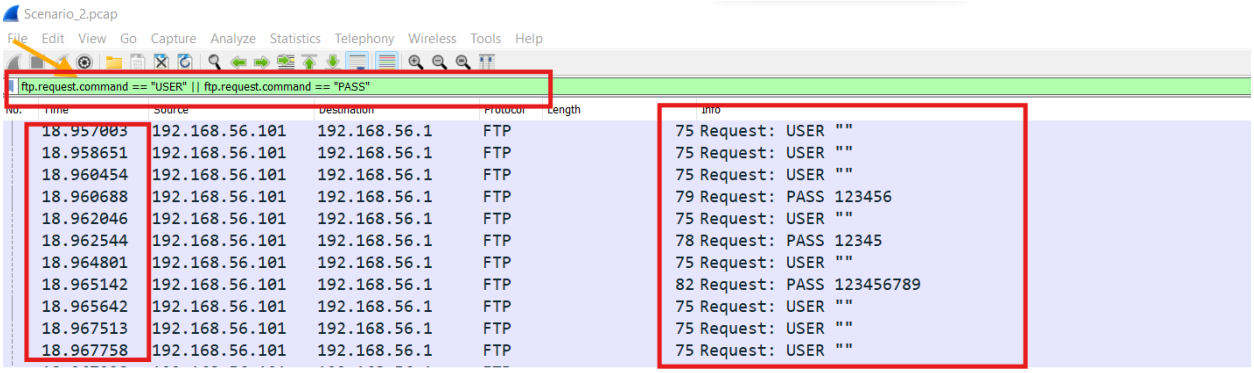
- The **traffic volume between these two IPs** was significantly higher than normal FTP activity, consuming a substantial portion of the overall captured traffic.

- Packet patterns indicated that the server was likely overwhelmed by repeated connection attempts, consistent with **flooding behavior**.

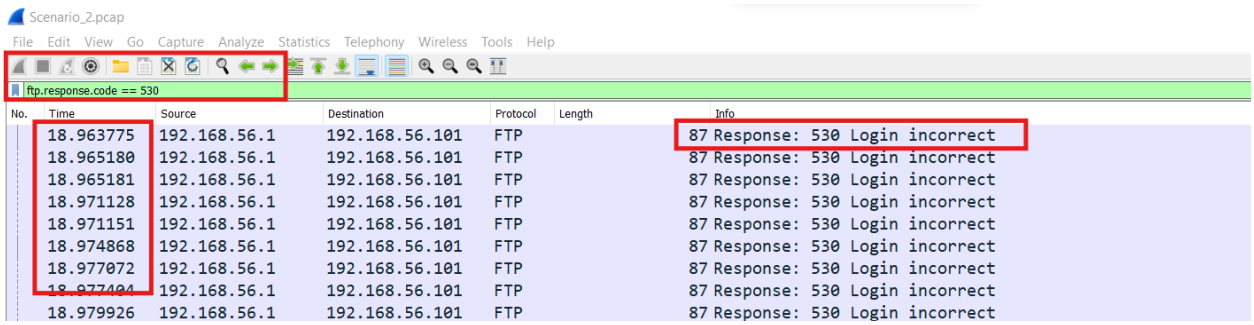
Key Questions

What caused the spike in FTP traffic?

A high volume of FTP USER and PASS commands was observed within a very short time window.(Login Flood)

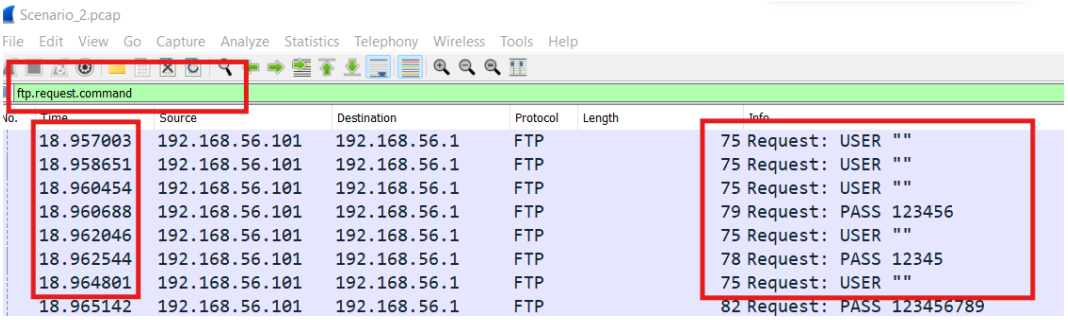


Repeated 530 Login incorrect responses confirm brute-force authentication attempts.



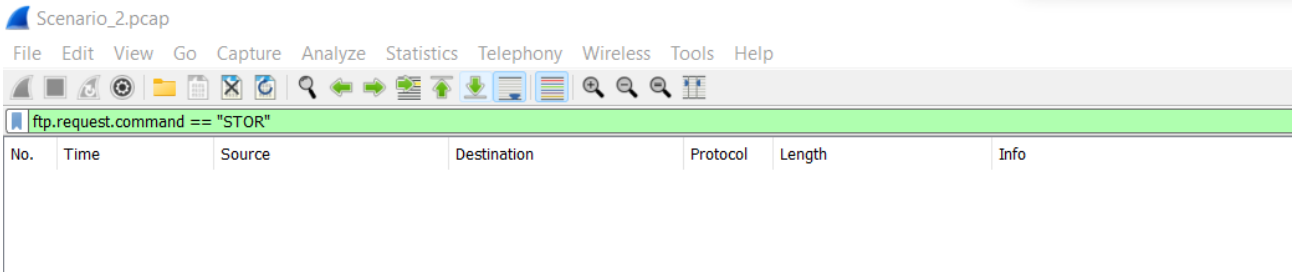
What events occurred immediately before the FTP server was taken offline?

Immediately before the service outage, a high volume of FTP authentication commands was observed Brute Force / Login Flood

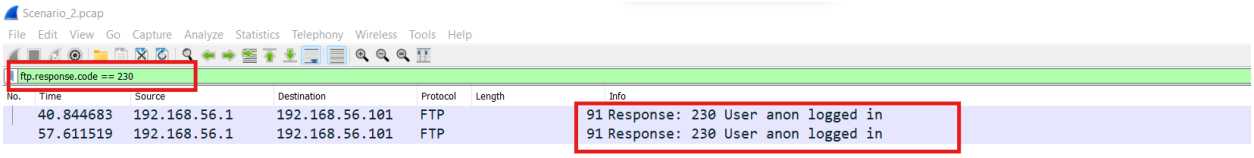


Were any files transferred to or from the server? Were any user accounts compromised?

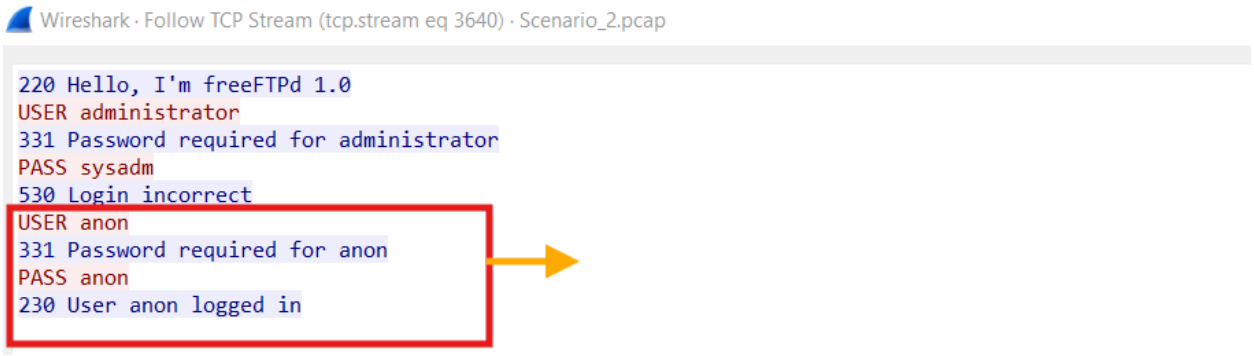
Yes, a file was transferred from the server to the attacker. No files were uploaded to the server.



No legitimate user accounts were compromised.
All login attempts against privileged accounts failed. Anonymous FTP access was successfully used, which indicates a configuration weakness, not an account compromised

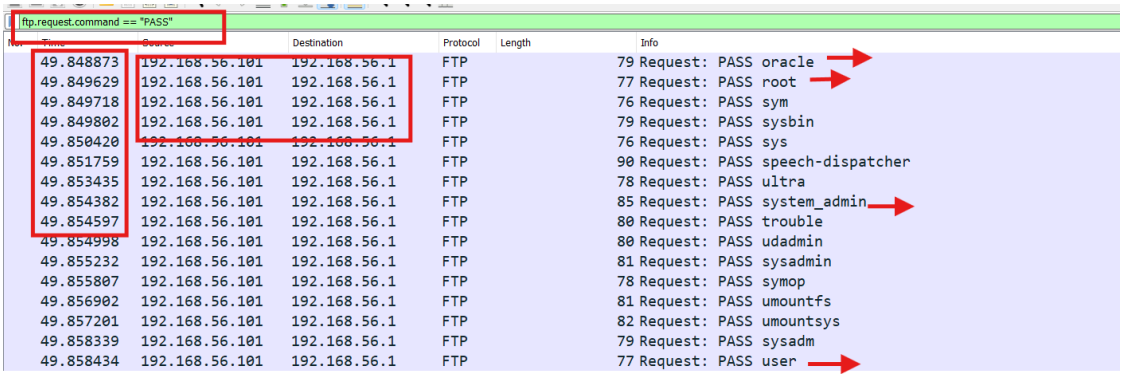


Only anonymous login succeeded



Identify the events leading up to the attack on the FTP server

Before the FTP server became unavailable, it experienced abnormal activity characterized by excessive connection attempts and repeated authentication requests. These events indicate a preparatory phase where the attacker attempted to gain access and exhaust server resources.



- Repeated FTP connection attempts, confirmed by multiple 220 Service Ready responses.

- Most login attempts failed with 530 Login incorrect, indicating brute-force behavior.

- Successful authentication using the anonymous FTP account (230 User anon logged in).

- Execution of FTP commands after authentication, including a file download:

Determine what types of attacks were performed on the FTP service.

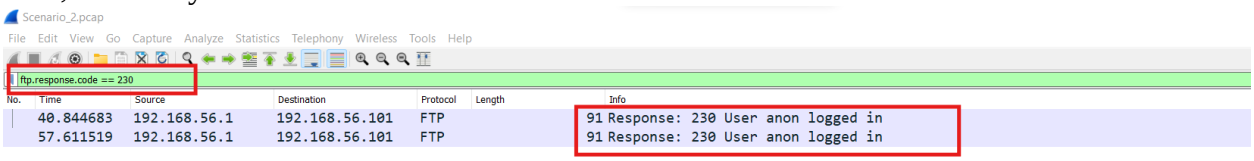
1. **Brute-Force / Password Spraying Attack**
    - High volume of `USER` and `PASS` commands.
    - Multiple 530 Login incorrect responses.
2. **Unauthorized Access via Anonymous FTP**
    - Successful anonymous login (230 response).
3. **Unauthorized File Access**
    - File downloaded using the `RETR` command.
4. **Application-Layer Denial-of-Service (DoS)**
    - Sudden spike in FTP traffic.

Assess the impact of those attacks:

- No legitimate user accounts were compromised.
- One file was downloaded via anonymous FTP access.
- No files were uploaded or modified.
- The FTP service became unavailable due to a denial-of-service attack.

Did the attacker authenticate?

Yes , but anonymous user not admin user

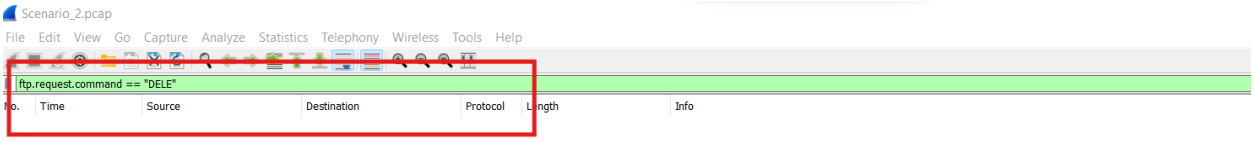


What actions did they perform?

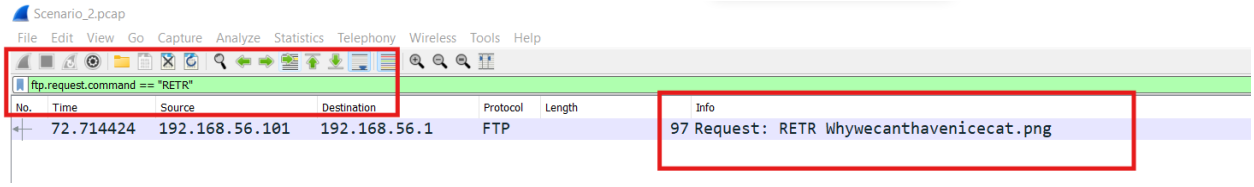
- Attempted login with administrator → failed (530 Login incorrect).
- Logged in as anon → succeeded (230 User anon logged in).
- Executed RETR command→ unauthorized read access (whywecanhavenicecat.png).
- Main impact: high-volume requests caused the FTP server to go offline (DoS effect).

Were any files accessed, modified, or stolen?

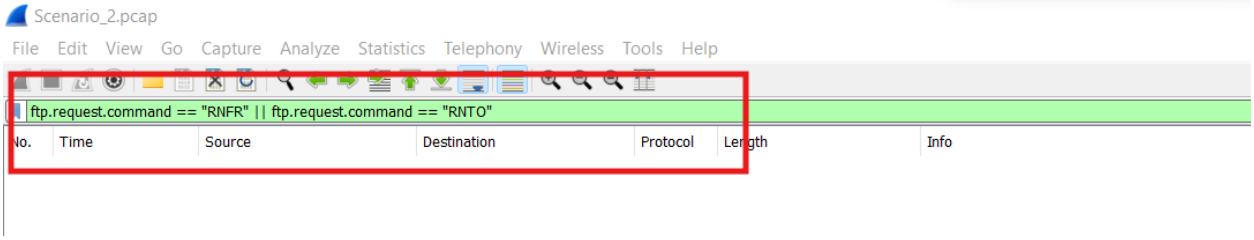
The attacker accessed one file (whywecanhavenicecat.png) using the RETR command. No files were modified, deleted, or stolen, as confirmed by Wireshark analysis of all FTP commands (STOR, DELE, RNFR, RNTO) which showed no activity. This indicates read-only access with no impact on file integrity or confidentiality beyond the accessed file.



No files deleted



No files stolen



No files modified (rename)

read-only access