

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**).

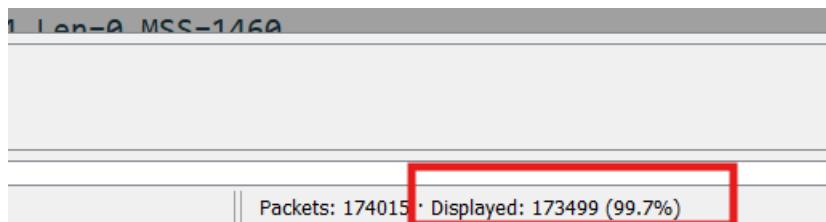
No.	Time	Source	Destination	Protocol	Length	Info
40.816487		192.168.56.101	192.168.56.1	FTP	86	Request: USER administrator
40.817446		192.168.56.1	192.168.56.101	FTP	107	Response: 331 Password required for administrator
40.818049		192.168.56.101	192.168.56.1	FTP	80	Request: PASS udadmin
40.818332		192.168.56.1	192.168.56.101	FTP	87	Response: 530 Login incorrect
40.818587		192.168.56.101	192.168.56.1	FTP	86	Request: USER administrator

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.

No.	Time	Source	Destination	Protocol	Length	Info
11.506381		192.168.56.101	192.168.56.1	TCP	58	37711 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11.506575		192.168.56.101	192.168.56.1	TCP	58	37711 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11.506733		192.168.56.101	192.168.56.1	TCP	58	37711 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11.506883		192.168.56.101	192.168.56.1	TCP	58	37711 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11.507033		192.168.56.101	192.168.56.1	TCP	58	37711 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11.507189		192.168.56.101	192.168.56.1	TCP	58	37711 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11.507339		192.168.56.101	192.168.56.1	TCP	58	37711 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11.507588		192.168.56.101	192.168.56.1	TCP	58	37711 → 1729 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

- 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)

No.	Time	Source	Destination	Protocol	Length	Info
18.957003		192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.958651		192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.960454		192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.960688		192.168.56.101	192.168.56.1	FTP		79 Request: PASS 123456
18.962046		192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.962544		192.168.56.101	192.168.56.1	FTP		78 Request: PASS 12345
18.964801		192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.965142		192.168.56.101	192.168.56.1	FTP		82 Request: PASS 123456789
18.965642		192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.967513		192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.967758		192.168.56.101	192.168.56.1	FTP		75 Request: USER ""

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

No.	Time	Source	Destination	Protocol	Length	Info
18.963775		192.168.56.1	192.168.56.101	FTP		87 Response: 530 Login incorrect
18.965180		192.168.56.1	192.168.56.101	FTP		87 Response: 530 Login incorrect
18.965181		192.168.56.1	192.168.56.101	FTP		87 Response: 530 Login incorrect
18.971128		192.168.56.1	192.168.56.101	FTP		87 Response: 530 Login incorrect
18.971151		192.168.56.1	192.168.56.101	FTP		87 Response: 530 Login incorrect
18.974868		192.168.56.1	192.168.56.101	FTP		87 Response: 530 Login incorrect
18.977072		192.168.56.1	192.168.56.101	FTP		87 Response: 530 Login incorrect
18.977494		192.168.56.1	192.168.56.101	FTP		87 Response: 530 Login incorrect
18.979926		192.168.56.1	192.168.56.101	FTP		87 Response: 530 Login incorrect

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

Scenario_2.pcap

No.	Time	Source	Destination	Protocol	Length	Info
18.957003	18.957003	192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.958651	18.958651	192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.960454	18.960454	192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.960688	18.960688	192.168.56.101	192.168.56.1	FTP		79 Request: PASS 123456
18.962046	18.962046	192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.962544	18.962544	192.168.56.101	192.168.56.1	FTP		78 Request: PASS 12345
18.964801	18.964801	192.168.56.101	192.168.56.1	FTP		75 Request: USER ""
18.965142	18.965142	192.168.56.101	192.168.56.1	FTP		82 Request: PASS 123456789

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.

Scenario_2.pcap

No.	Time	Source	Destination	Protocol	Length	Info
72.714424	72.714424	192.168.56.101	192.168.56.1	FTP		97 Request: RETR Whywecanthavenicecat.png

Scenario_2.pcap

No.	Time	Source	Destination	Protocol	Length	Info

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

Scenario_2.pcap

No.	Time	Source	Destination	Protocol	Length	Info
40.844683	40.844683	192.168.56.1	192.168.56.101	FTP		91 Response: 230 User anon logged in
57.611519	57.611519	192.168.56.1	192.168.56.101	FTP		91 Response: 230 User anon logged in

Only anonymous login succeeded

Wireshark · Follow TCP Stream (tcp.stream eq 3640) · Scenario_2.pcap

```

220 Hello, I'm freeFTPd 1.0
USER administrator
331 Password required for administrator
PASS sysadm
530 Login incorrect
USER anon
331 Password required for anon
PASS anon
230 User anon logged in

```

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.

No	Time	Source	Destination	Protocol	Length	Info
49.848873		192.168.56.101	192.168.56.1	FTP		79 Request: PASS oracle →
49.849629		192.168.56.101	192.168.56.1	FTP		77 Request: PASS root →
49.849718		192.168.56.101	192.168.56.1	FTP		76 Request: PASS sym
49.849802		192.168.56.101	192.168.56.1	FTP		79 Request: PASS sysbin
49.850420		192.168.56.101	192.168.56.1	FTP		76 Request: PASS sys
49.851759		192.168.56.101	192.168.56.1	FTP		90 Request: PASS speech-dispatcher
49.853435		192.168.56.101	192.168.56.1	FTP		78 Request: PASS ultra →
49.854382		192.168.56.101	192.168.56.1	FTP		85 Request: PASS system_admin →
49.854597		192.168.56.101	192.168.56.1	FTP		80 Request: PASS trouble
49.854998		192.168.56.101	192.168.56.1	FTP		80 Request: PASS udadmin
49.855232		192.168.56.101	192.168.56.1	FTP		81 Request: PASS sysadmin
49.855807		192.168.56.101	192.168.56.1	FTP		78 Request: PASS sysop
49.856902		192.168.56.101	192.168.56.1	FTP		81 Request: PASS umountfs
49.857201		192.168.56.101	192.168.56.1	FTP		82 Request: PASS umountsys
49.858339		192.168.56.101	192.168.56.1	FTP		79 Request: PASS sysadm
49.858434		192.168.56.101	192.168.56.1	FTP		77 Request: PASS user →

- 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:

No	Time	Source	Destination	Protocol	Length	Info
72.714424		192.168.56.101	192.168.56.1	FTP		97 Request: RETR Whywecanhave nicecat.png

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

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

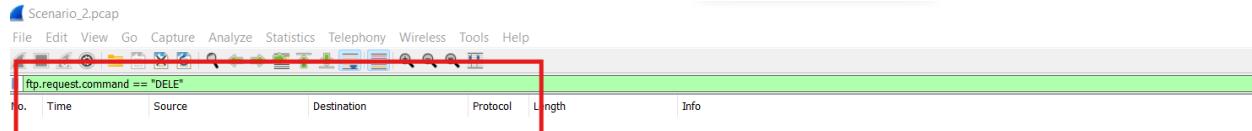


What actions did they perform?

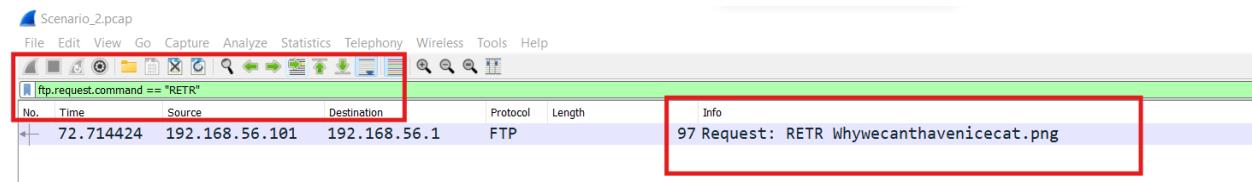
- Attempted login with administrator → failed (530 Login incorrect).
- Logged in as anon → succeeded (230 User anon logged in).
- Executed RETR command→ unauthorized read access (whywecanhave nicecat.png).
- Main impact: high-volume requests caused the FTP server to go offline (DoS effect).

Were any files accessed, modified, or stolen?

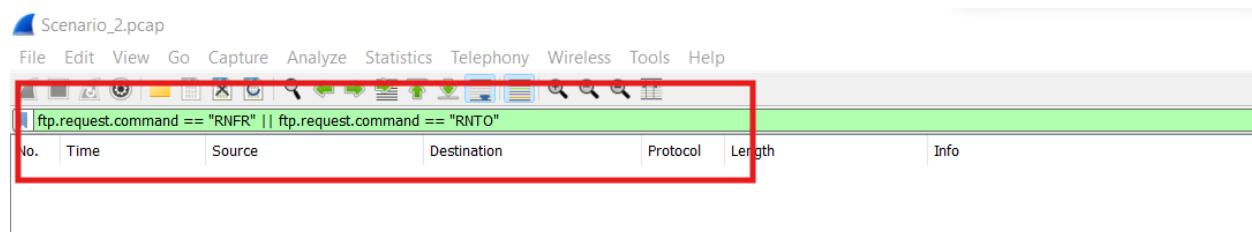
The attacker accessed one file (whywecanhave nicecat.png) using the RETR command. No files were modified, deleted, or stolen, as confirmed by Wireshark analysis of all FTP commands (STOR, DELE, RNFR, RNTO) which showed no activity. This indicates read-only access with no impact on file integrity or confidentiality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



No files deleted



No files stolen



No files modified (rename)



read-only access