

Incident Report: FTP Malicious File Upload Simulation

Prepared by: Ayanloye Olaitan
Date: 15.08.2025
Title: FTP Malicious File Upload Simulation

Incident Summary

This report documents a simulated FTP malicious file upload performed within a controlled cybersecurity lab to assess security vulnerabilities in an Ubuntu-based FTP server. The test involved creating and uploading a malicious file from a Kali Linux attacker machine to the target FTP server.

Systems Involved:

- **Attacker Machine:** Kali Linux (IP: 192.168.56.102)
- **Target Machine:** Ubuntu FTP Server (IP: 192.168.56.103)
- **Service:** vsftpd FTP Server
- **User Account:** ftpusers

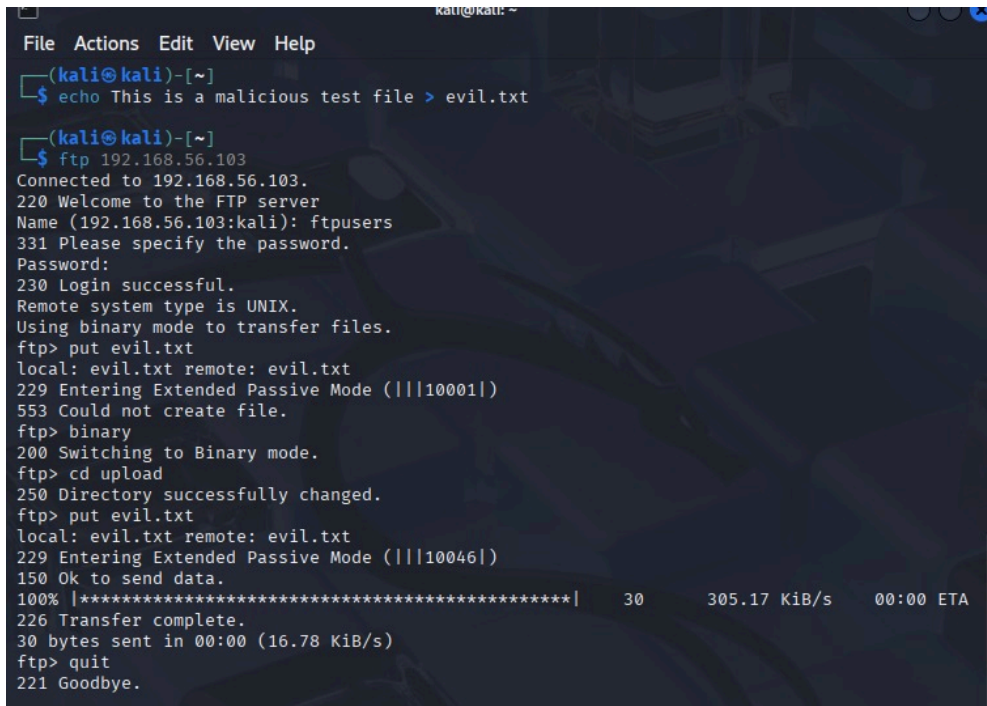
Timeline of Events

Time (UTC)	Event	Details
14:35:21	Connection Initiated	Client 192.168.56.102 connected to FTP server
14:35:23	Login Successful	User ftpusers successfully logged in
14:35:30	Upload Failed	Attempted to create /evil.txt in root FTP directory – permission denied
14:35:39	Upload Successful	File /upload/evil.txt uploaded successfully (30 bytes, 305.17 KB/s)

Log Evidence

```
Tue Aug 15 14:35:21 2025 [pid 2054] CONNECT: Client "192.168.56.102"  
Tue Aug 15 14:35:23 2025 [pid 2054] [ftputers] OK LOGIN: Client  
"192.168.56.102"  
Tue Aug 15 14:35:30 2025 [pid 2054] [ftputers] FAIL CREATE FILE: Client  
"192.168.56.102", "/evil.txt"  
Tue Aug 15 14:35:39 2025 [pid 2054] [ftputers] OK UPLOAD: Client  
"192.168.56.102", "/upload/evil.txt", 30 bytes, 305.17Kbyte/sec
```

Screenshots



```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali)-[~]  
$ echo This is a malicious test file > evil.txt  
~(kali@kali)-[~]  
$ ftp 192.168.56.103  
Connected to 192.168.56.103.  
220 Welcome to the FTP server  
Name (192.168.56.103:kali): ftputers  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> put evil.txt  
local: evil.txt remote: evil.txt  
229 Entering Extended Passive Mode (|||10001|)  
553 Could not create file.  
ftp> binary  
200 Switching to Binary mode.  
ftp> cd upload  
250 Directory successfully changed.  
ftp> put evil.txt  
local: evil.txt remote: evil.txt  
229 Entering Extended Passive Mode (|||10046|)  
150 Ok to send data.  
100% |*****| 30 305.17 KiB/s 00:00 ETA  
226 Transfer complete.  
30 bytes sent in 00:00 (16.78 KiB/s)  
ftp> quit  
221 Goodbye.
```

Screenshot 1: Creation of evil.txt and FTP connection attempt.

```

(kali@kali)-[~]
└─$ ftp 192.168.56.103
Connected to 192.168.56.103.
220 Welcome to the FTP server
Name (192.168.56.103:kali): ftpusers
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 Switching to Binary mode.
ftp> put testfile.txt
local: testfile.txt remote: testfile.txt
229 Entering Extended Passive Mode (|||10056|)
553 Could not create file.
ftp> cd upload
421 Timeout.
ftp> quit

(kali@kali)-[~]
└─$ ftp 192.168.56.103
Connected to 192.168.56.103.
220 Welcome to the FTP server
Name (192.168.56.103:kali): ftpusers
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 Switching to Binary mode.
ftp> cd upload
250 Directory successfully changed.
ftp> put testfile.txt
local: testfile.txt remote: testfile.txt
229 Entering Extended Passive Mode (|||10058|)
150 Ok to send data.
100% |*****| 14 158.97 KiB/s 00:00 ETA
226 Transfer complete.
14 bytes sent in 00:00 (8.20 KiB/s)
ftp> quit
221 Goodbye.

```

Screenshot 2: Failed upload attempt to root directory and successful upload to /upload.

```

ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo systemctl restart vsftpd
ayanloye-olaitan@ayanloye-olaitan-VirtualBox:~$ sudo tail -f /var/log/vsftpd.log
Mon Aug 4 22:55:30 2025 [pid 41987] CONNECT: Client "192.168.56.101"
Mon Aug 4 22:55:39 2025 [pid 41986] [ftp] OK LOGIN: Client "192.168.56.101", anon password "?"
Mon Aug 4 22:55:55 2025 [pid 41988] [ftp] FAIL UPLOAD: Client "192.168.56.101", "/test.txt", 0.0
0Kbyte/sec
Mon Aug 4 22:59:46 2025 [pid 42033] CONNECT: Client "192.168.56.101"
Mon Aug 4 22:59:53 2025 [pid 42032] [ftp] OK LOGIN: Client "192.168.56.101", anon password "?"
Thu Aug 14 17:15:44 2025 1 192.168.56.101 0 /testfile.txt b _ i r ftpusers ftp 0 * i
Fri Aug 15 15:21:07 2025 1 192.168.56.101 0 /testfile.txt b _ i r ftpusers ftp 0 * i
Fri Aug 15 15:29:02 2025 1 192.168.56.101 14 /upload/testfile.txt b _ i r ftpusers ftp 0 * c
Fri Aug 15 15:31:35 2025 1 192.168.56.101 0 /evil.txt b _ i r ftpusers ftp 0 * i
Fri Aug 15 15:32:12 2025 1 192.168.56.101 30 /upload/evil.txt b _ i r ftpusers ftp 0 * c

```

Screenshot 3: Verification of uploaded file on Ubuntu FTP server.

Impact Assessment

The FTP server's /upload directory allows unauthenticated write access for valid users, potentially enabling malicious file uploads.

Recommendations

- Restrict upload permissions to trusted users only.
- Implement antivirus/malware scanning on uploaded files.
- Switch to SFTP with key-based authentication.
- Continuously monitor FTP logs for suspicious patterns.

Conclusion

This simulation confirmed that the FTP server can be used to upload potentially malicious files. While conducted in a lab setting, similar vulnerabilities could be exploited in real-world scenarios if mitigations are not applied.