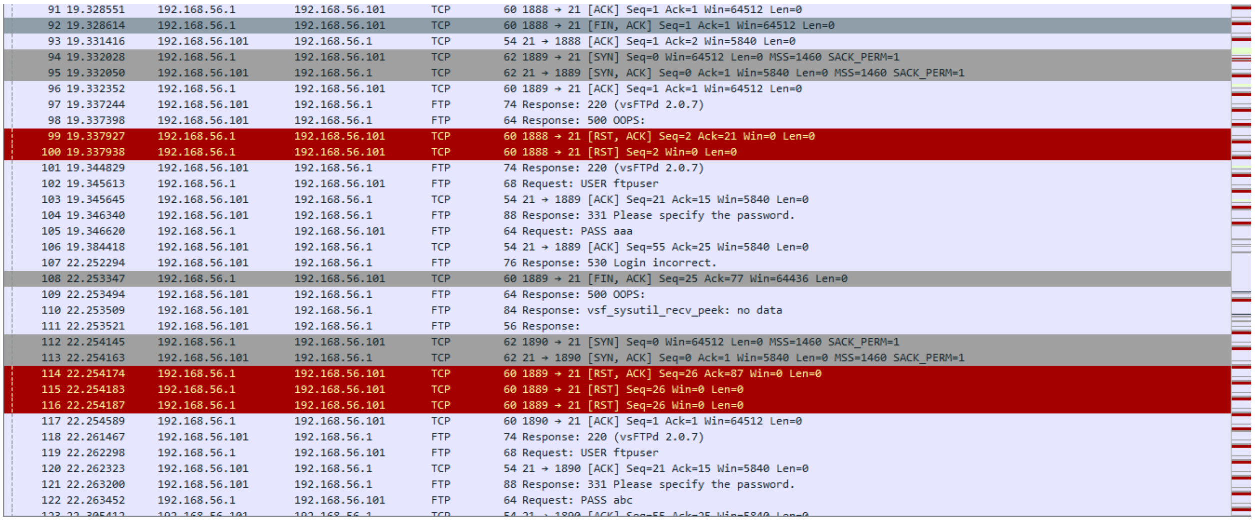
1-Abstract

Summary:

In depth analysis of file Networkcapture2.pcap revealed the signs of **Brute force Attack** on an FTP server with the IP address 192.168.56.101 by the Attacking machine with the IP address 192.168.56.1.

Capture Overview:

In the picture down below it can be seen that the Attacker is trying to login to the FTP server through the use of Brute Force by trying out different combinations of the password.



```
 91 19.328551   192.168.56.1     192.168.56.101   TCP    60 1888 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0
 92 19.328614   192.168.56.1     192.168.56.101   TCP    60 1888 → 21 [FIN, ACK] Seq=1 Ack=1 Win=64512 Len=0
 93 19.331416   192.168.56.101   192.168.56.1     TCP    54 21 → 1888 [ACK] Seq=1 Ack=2 Win=5840 Len=0
 94 19.332028   192.168.56.1     192.168.56.101   TCP    62 1889 → 21 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 SACK_PERM=1
 95 19.332050   192.168.56.101   192.168.56.1     TCP    62 21 → 1889 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
 96 19.332352   192.168.56.1     192.168.56.101   TCP    60 1889 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0
 97 19.337244   192.168.56.101   192.168.56.1     FTP    74 Response: 220 (vsFTPd 2.0.7)
 98 19.337398   192.168.56.101   192.168.56.1     FTP    64 Response: 500 OOPS:
 99 19.337927   192.168.56.1     192.168.56.101   TCP    60 1888 → 21 [RST, ACK] Seq=2 Ack=21 Win=0 Len=0
100 19.337938   192.168.56.1     192.168.56.101   TCP    60 1888 → 21 [RST] Seq=2 Win=0 Len=0
101 19.344829   192.168.56.101   192.168.56.1     FTP    74 Response: 220 (vsFTPd 2.0.7)
102 19.345613   192.168.56.1     192.168.56.101   FTP    68 Request: USER ftpuser
103 19.345645   192.168.56.101   192.168.56.1     TCP    54 21 → 1889 [ACK] Seq=21 Ack=15 Win=5840 Len=0
104 19.346340   192.168.56.101   192.168.56.1     FTP    88 Response: 331 Please specify the password.
105 19.346620   192.168.56.1     192.168.56.101   FTP    64 Request: PASS aaa
106 19.384418   192.168.56.101   192.168.56.1     TCP    54 21 → 1889 [ACK] Seq=55 Ack=25 Win=5840 Len=0
107 22.252294   192.168.56.101   192.168.56.1     FTP    76 Response: 530 Login incorrect.
108 22.253347   192.168.56.1     192.168.56.101   TCP    60 1889 → 21 [FIN, ACK] Seq=25 Ack=77 Win=64436 Len=0
109 22.253494   192.168.56.101   192.168.56.1     FTP    64 Response: 500 OOPS:
110 22.253509   192.168.56.101   192.168.56.1     FTP    84 Response: vsf_sysutil_recv_peek: no data
111 22.253521   192.168.56.101   192.168.56.1     FTP    56 Response:
112 22.254145   192.168.56.1     192.168.56.101   TCP    62 1890 → 21 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 SACK_PERM=1
113 22.254163   192.168.56.101   192.168.56.1     TCP    62 21 → 1890 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
114 22.254174   192.168.56.1     192.168.56.101   TCP    60 1889 → 21 [RST, ACK] Seq=26 Ack=87 Win=0 Len=0
115 22.254183   192.168.56.1     192.168.56.101   TCP    60 1889 → 21 [RST] Seq=26 Win=0 Len=0
116 22.254187   192.168.56.1     192.168.56.101   TCP    60 1889 → 21 [RST] Seq=26 Win=0 Len=0
117 22.254589   192.168.56.1     192.168.56.101   TCP    60 1890 → 21 [ACK] Seq=1 Ack=1 Win=64512 Len=0
118 22.261467   192.168.56.101   192.168.56.1     FTP    74 Response: 220 (vsFTPd 2.0.7)
119 22.262298   192.168.56.1     192.168.56.101   FTP    68 Request: USER ftpuser
120 22.262323   192.168.56.101   192.168.56.1     TCP    54 21 → 1890 [ACK] Seq=21 Ack=15 Win=5840 Len=0
121 22.263200   192.168.56.101   192.168.56.1     FTP    88 Response: 331 Please specify the password.
122 22.263452   192.168.56.1     192.168.56.101   FTP    64 Request: PASS abc
123 22.305412   192.168.56.101   192.168.56.1     TCP    54 21 → 1890 [ACK] Seq=55 Ack=25 Win=5840 Len=0
```

Analysis Tool Used:

The PCAP file was analyzed using **Wireshark** desktop application.

2-Findings

Protocol Breakdown:

The protocols used in the file are the following:

HTTP (Hypertext transfer Protocol): HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

TCP (Transmission Control Protocol): TCP (Transmission Control Protocol) is an important network protocol that is used in the transmission of data over networks. A protocol, in the context of networks, is a set of rules and procedures that govern how the transmission of data is carried out so that everyone in the whole world, independent of the location, software or hardware used, does the thing the same way. TCP works together with IP (Internet Protocol) in a well-known duo called TCP/IP.

ARP (Address Resolution Protocol): Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

FTP (File transfer Protocol): The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture using separate control and data connections between the client and the server.

Actors Involved:

Victim: 192.168.56.1(FTP server), 192.168.56.102(Indirect Victim)

Attacker: 192.168.56.1

Timeline of Events:

1. 192.168.56.102 uploads a Confidential Information.docs file on to the FTP server.
2. Attacker starts Brute force attacking after establishing a connection with ARP protocol.
3. Eventually the attacker is successful in the attack and the Confidential Information.docs is compromised by the attacker.

Malicious Behavior:

Indicators of Compromise	**Indicators of Attack**
Compromisation of file named Confidential Information.docs can be seen.	The attacker was using Brute Force Attack to crack the password.
	The intention of attack seemed to be getting a hold of some files.

3-Mitigation

- There are a number of techniques for preventing brute force attacks. The first is to implement an account lockout policy. For example, after three failed login attempts, the account is locked out until an administrator unlocks it. The disadvantage of this method is that multiple accounts can be locked out by one malicious user, causing a denial of service for the victims and lots of work for the administrator.
- A better, more complicated technique is progressive delays. With progressive delays, user accounts are locked out for a set period of time after a few failed login attempts. The lock-out time increases with each subsequent failed attempt. This prevents automated tools from performing a brute force attack and effectively makes it impractical to perform such an attack.
- Another technique is to use a challenge-response test to prevent automated submissions of the login page. Tools such as the free CAPTCHA can be used to require the user to enter a word or solve a simple math problem to ensure the user is, in fact, a person. This technique is effective, but has accessibility concerns and affects usability of the site.
- Any Web application should enforce the use of strong passwords. At a minimum, requiring users to choose passwords of eight letters or more with some complexity (letters and numbers, or requiring one special character) is an excellent defence against brute force attacks when combined with one of the techniques outlined above.

4-Appendix

Table of carved files:

S.No	Filename
1.	Networkcapture2.pcap

Wireshark Filter Used:

FTP