

# Detecting Brute Force Attacks with Scapy

---



**Sean Wilkins**

Network Engineer & Author

[swilkins@infodispersion.com](mailto:swilkins@infodispersion.com)

[www.infodispersion.com](http://www.infodispersion.com)



There are multiple ways to monitor for brute force attacks.



# Overview



- **FTP Brute Force Attack Detection**
- **Concepts Demonstration - FTP Brute Force Detection**
- **SSH Brute Force Attack Detection**
- **Concepts Demonstration - SSH Brute Force Detection**



# Brute Force Attack Detection

**Analyze packets to determine a  
brute force attack attempt**

**Focus on analysis of FTP sessions**

**Commonly used and doesn't  
use encrypted communications**



# Brute Force Attack



**Why is this knowledge useful?**

**Systems need to be kept secure**

**Brute force method is a low knowledge attack**

**Attempts to find credentials**

**Detection generally left to automated appliances**

**In-depth hands-on approach may be needed**



Code will be based on the  
capture of a saved attack.



# FTP Traffic Analysis

**Monitor user and password  
process**

**Helps to differentiate  
between normal and nefarious  
logins**



# FTP

**Basic knowledge of FTP is required**

**Uses USER and PASS**

**Matches the traffic that relays the commands**

**How does the server respond?**





# Server Response

**Two main responses**

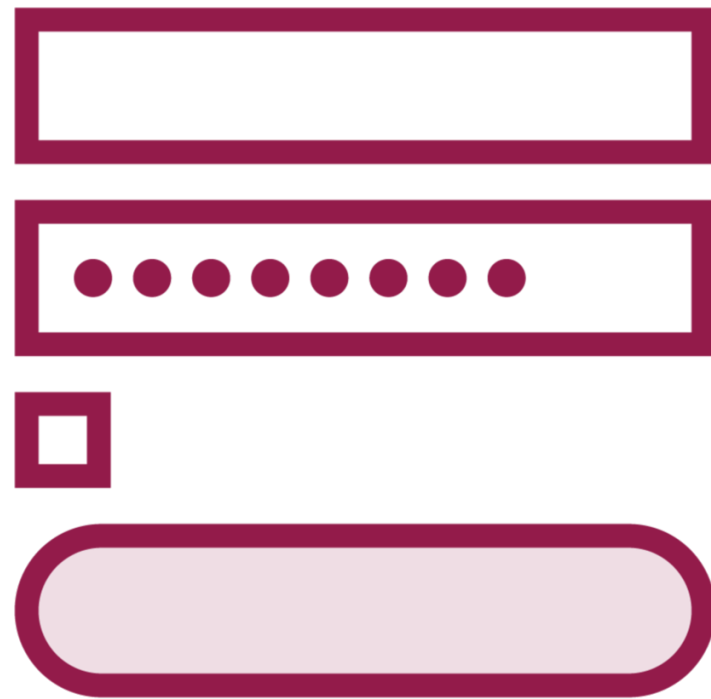
**230 Login  
Successful**

**530 Login Incorrect**

**Sent when  
credentials are  
correct**

**Sent when  
credentials are  
invalid**





**Collect sessions that include successful and unsuccessful login attempts**

**View individually – hard to determine if there is a problem**

**Important to analyze multiple sessions**



# Demo



## FTP Brute Force Detection



# SSH



**Utilizes encryption**

**Makes it harder to determine an attack**

**Doesn't have access to command level knowledge**

**Need to utilize a more creative solution**

# SSH Login Failure

Wireshark · Conversations · sshfails.pcap

Ethernet · 14IPv4 · 9IPv6 · 4TCP · 65UDP · 32

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.10.10.105	60624	10.10.10.103	22	38	2683	15.923287	0.0311	591 k	690 k				
10.10.10.105	60640	10.10.10.103	22	48	3753	16.167247	16.3824	1439	1832				
10.10.10.105	60650	10.10.10.103	22	30	3753	16.167335	16.4045	1502	1830				
10.10.10.105	60664	10.10.10.103	22	30	3753	16.167337	16.3933	1503	1831				
10.10.10.105	60672	10.10.10.103	22	48	3753	16.167592	16.4151	1436	1829				
10.10.10.105	54420	10.10.10.103	22	30	3753	62.533936	14.3263	1719	2095				
10.10.10.105	54430	10.10.10.103	22	30	3753	62.545631	14.3273	1719	2095				
10.10.10.105	54444	10.10.10.103	22	30	3753	62.553837	14.3301	1719	2095				
10.10.10.105	54456	10.10.10.103	22	30	3753	62.565776	14.3293	1719	2095				
10.10.10.105	37910	10.10.10.103	22	48	3753	106.845447	18.3753	1283	1633				
10.10.10.105	37916	10.10.10.103	22	48	3753	106.858005	18.3769	1283	1633				
10.10.10.105	37926	10.10.10.103	22	48	3753	106.869965	18.3770	1283	1633				
10.10.10.105	37940	10.10.10.103	22	48	3753	106.881422	18.3799	1283	1633				
10.10.10.105	52926	10.10.10.103	22	30	3753	155.186058	18.4537	1335	1626				
10.10.10.105	52928	10.10.10.103	22	30	3753	155.201998	18.4478	1335	1627				
10.10.10.105	52940	10.10.10.103	22	30	3753	155.237972	18.4307	1336	1629				
10.10.10.105	52948	10.10.10.103	22	30	3753	155.250156	18.4304	1336	1629				
10.10.10.105	54988	10.10.10.103	22	48	3753	201.561969	20.4643	1152	1467				
10.10.10.105	54990	10.10.10.103	22	48	3753	201.562084	20.4744	1151	1466				
10.10.10.105	55008	10.10.10.103	22	30	3753	201.607771	20.4680	1203	1466				
10.10.10.105	55020	10.10.10.103	22	48	3753	201.617960	20.4689	1152	1466				
10.10.10.105	45652	10.10.10.103	22	30	3753	249.965943	22.4833	1095	1335				
10.10.10.105	45664	10.10.10.103	22	30	3753	249.977753	22.4817	1096	1335				
10.10.10.105	45678	10.10.10.103	22	30	3753	250.013970	22.4772	1096	1335				
10.10.10.105	45682	10.10.10.103	22	30	3753	250.025888	22.4765	1096	1335				
10.10.10.105	44262	10.10.10.103	22	48	3753	300.389966	18.3817	1283	1633				
10.10.10.105	44276	10.10.10.103	22	48	3753	300.402034	18.3806	1283	1633				
10.10.10.105	44284	10.10.10.103	22	30	3753	300.434028	18.3748	1340	1633				
10.10.10.105	44290	10.10.10.103	22	14	3753	300.446107	18.3754	1312	1633				

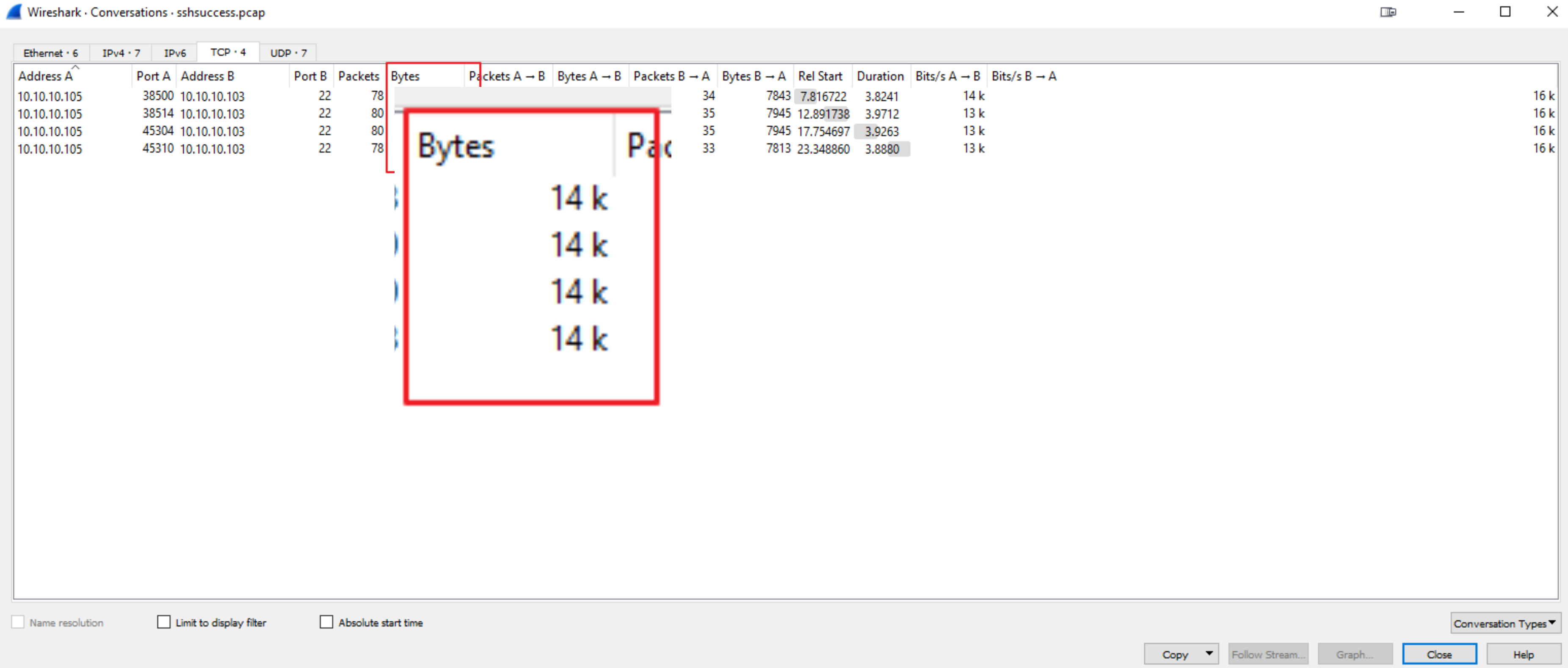
☐ Name resolution☐ Limit to display filter

Conversation Types

CopyFollow Stream...Graph...CloseHelp



# SSH Login Success





**What is done with this information?**

**Multiple failed attempts can be determined**

**Successful attempts screened out**



# Demonstration Strategy

**Track the number of bytes  
exchanged**

**Flag sessions inside a specific  
threshold**





# Demo



## SSH Brute Force Detection



# Summary



- **FTP Brute Force Attack Detection**
- **Concepts Demonstration - FTP Brute Force Detection**
- **SSH Brute Force Attack Detection**
- **Concepts Demonstration - SSH Brute Force Detection**

