Wireshark analysis of a Brute Force Attack

Cho Maddic
Jan 18, 2021 12:00 EST

Table of Contents

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.

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 analyze 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.

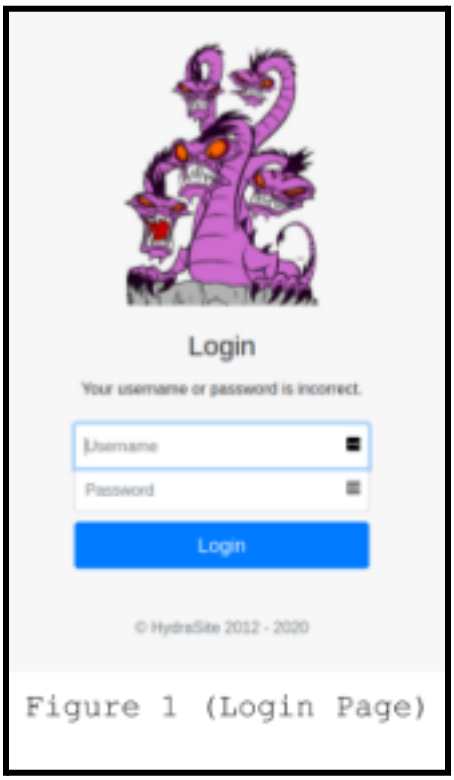

Figure 1 (Login Page)

Brute Force Attack: 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." -l -V”*

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

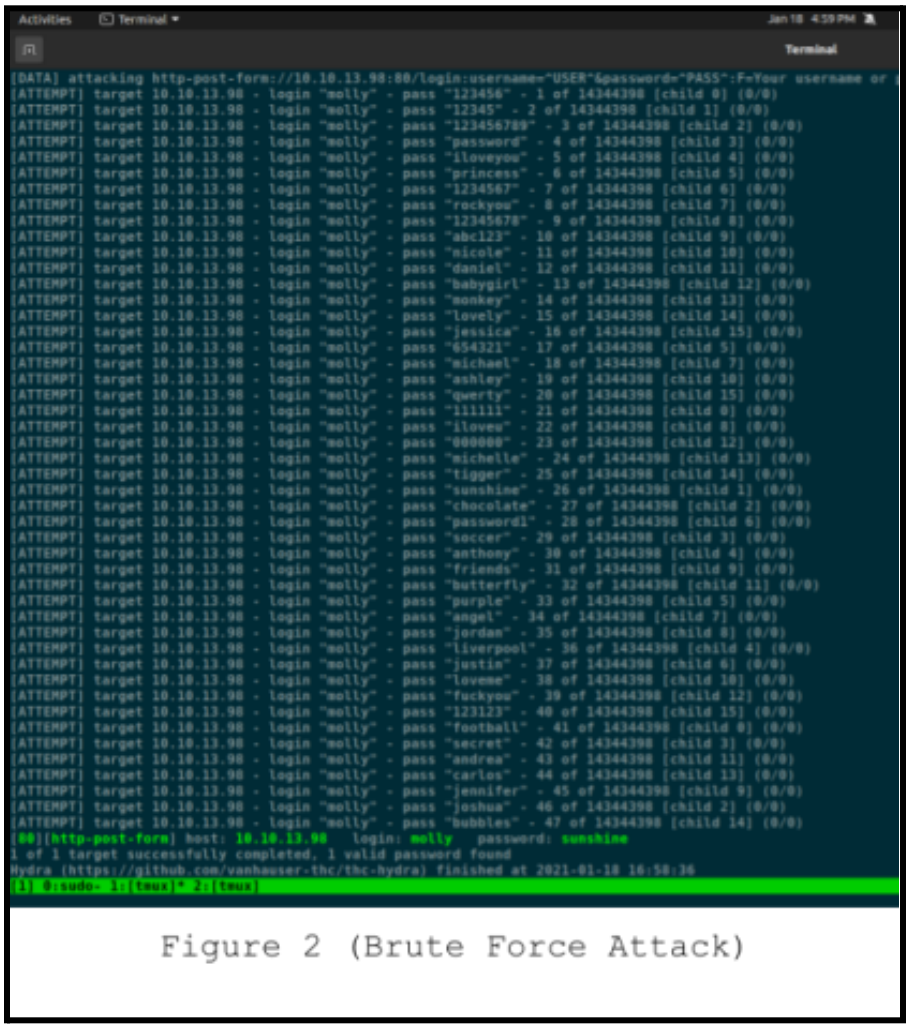

Figure 2 (Brute Force Attack)

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 its 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.

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 percent of them were “HTML Form URL Encoded” consisting of the passwords being sent to the login page from the attacking machine.

Conclusion

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.