Detect DOS and DDOS Attacks with Wireshark

@mmar

Wireshark

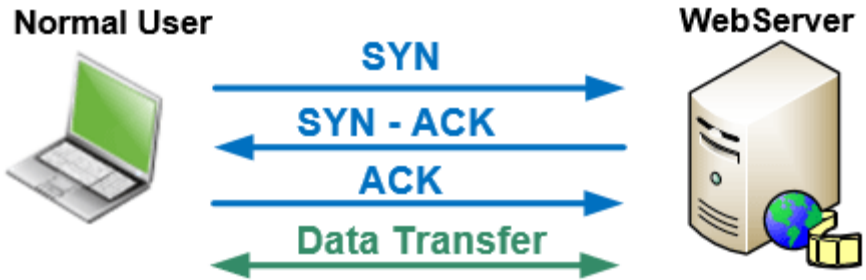
Few tools are as useful to the IT professional as Wireshark, the go-to network packet capture tool. Wireshark will help you capture network packets and display them at a granular level. Once these packets are broken down, you can use them for real-time or offline analysis. This tool lets you put your network traffic under a microscope, and then filter and drill down into it, zooming in on the root cause of problems, assisting with network analysis and ultimately network security

https://t.me/learningnets

Threeway Handshake

3- way Handhake

- When a client attempts to connect to a server using the TCP protocol e.g. (HTTP or HTTPS), it is first required to perform a three-way handshake before any data is exchanged between the two. Since the three-way TCP handshake is always initiated by the client it sends a SYN packet to the server.



- The server next replies acknowledging the request and at the same time sends its own SYN request – this is the SYN-ACK packet. Finally, the client sends an ACK packet which confirms both two hosts agree to create a connection. The connection is therefore established and data can be transferred between them.

https://t.me/learningnets

DOS Detection

Wireshark provides an easy interface to detect DOS and DDOS attacks and detect malicious IPs

Manual Inspection

https://t.me/learningnets

DOS Detection

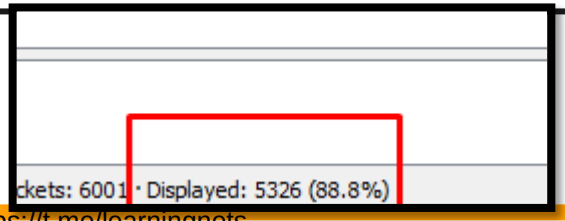
- You can detect a DOS attack by simply viewing a pcap file, a large no of packets from a source to the target within a short span of time indicate a DOS attack
- Whereas in DDOS, you will see, a number of IP addresses (Mostly spoofed) sending packets to a single target

https://t.me/learningnets

Detecting DDOS

- A big giveaway is a large number of SYN packets being sent to a single PC. We are able to note the start of the attack by a huge flood of TCP traffic. We can check the number of syn packets with the following flags

```
tcp.flags.syn == 1 and tcp.flags.ack == 0
tcp.flags.syn == 1
```

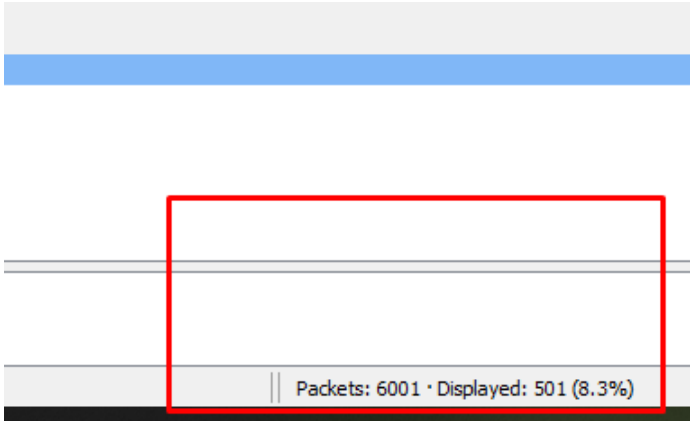


https://t.me/learningnets

Detecting DDOS

- Moreover, If we use the following display filter to display syn/ack packets there will be a huge discrepancy between them and the previous filter packets

```
tcp.flags.syn == 1 and tcp.flags.ack == 1
```



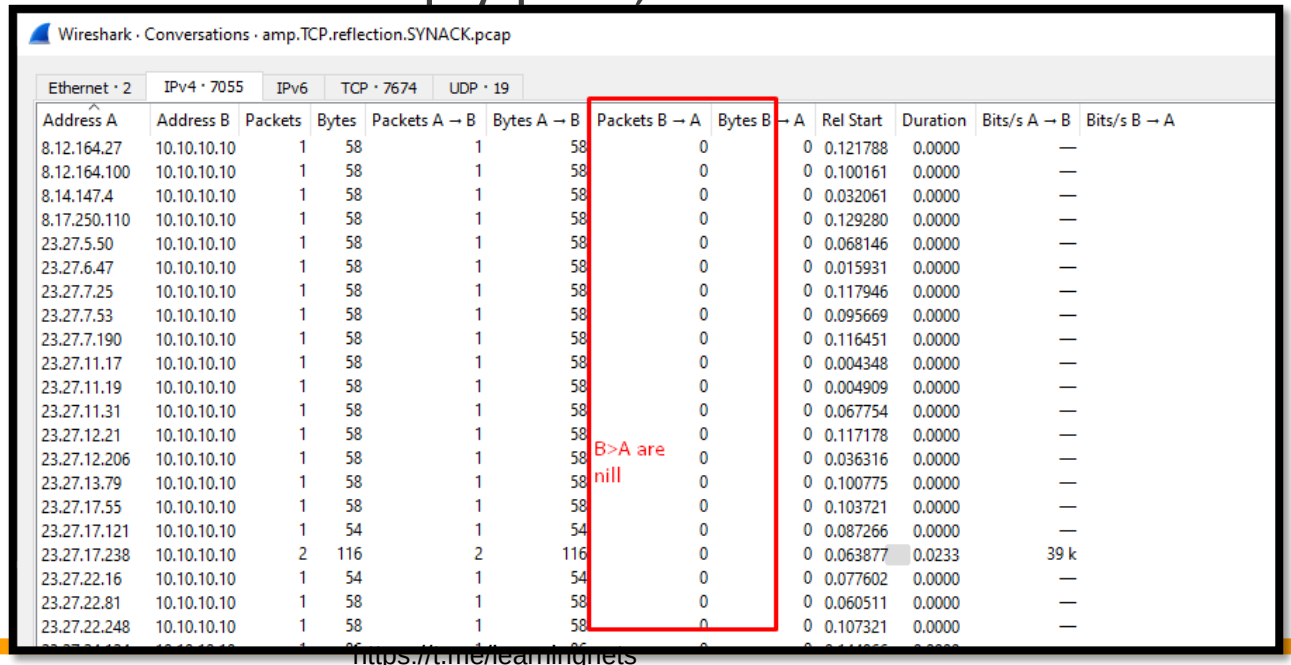
https://t.me/learningnets

Detection with Conversations

https://t.me/learningnets

Detecting DDOS

- Go to statistics and select conversations. If there are a number of packets targeted on one IP from different Source Addresses and no reply pack, it indicates DDOS



Address A	Address 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
8.12.164.27	10.10.10.10	1	58	1	58	0	0	0.121788	0.0000	—	
8.12.164.100	10.10.10.10	1	58	1	58	0	0	0.100161	0.0000	—	
8.14.147.4	10.10.10.10	1	58	1	58	0	0	0.032061	0.0000	—	
8.17.250.110	10.10.10.10	1	58	1	58	0	0	0.129280	0.0000	—	
23.27.5.50	10.10.10.10	1	58	1	58	0	0	0.068146	0.0000	—	
23.27.6.47	10.10.10.10	1	58	1	58	0	0	0.015931	0.0000	—	
23.27.7.25	10.10.10.10	1	58	1	58	0	0	0.117946	0.0000	—	
23.27.7.53	10.10.10.10	1	58	1	58	0	0	0.095669	0.0000	—	
23.27.7.190	10.10.10.10	1	58	1	58	0	0	0.116451	0.0000	—	
23.27.11.17	10.10.10.10	1	58	1	58	0	0	0.004348	0.0000	—	
23.27.11.19	10.10.10.10	1	58	1	58	0	0	0.004909	0.0000	—	
23.27.11.31	10.10.10.10	1	58	1	58	0	0	0.067754	0.0000	—	
23.27.12.21	10.10.10.10	1	58	1	58	0	0	0.117178	0.0000	—	
23.27.12.206	10.10.10.10	1	58	1	58	0	0	0.036316	0.0000	—	
23.27.13.79	10.10.10.10	1	58	1	58	0	0	0.100775	0.0000	—	
23.27.17.55	10.10.10.10	1	58	1	58	0	0	0.103721	0.0000	—	
23.27.17.121	10.10.10.10	1	54	1	54	0	0	0.087266	0.0000	—	
23.27.17.238	10.10.10.10	2	116	2	116	0	0	0.063877	0.0233	39 k	
23.27.22.16	10.10.10.10	1	54	1	54	0	0	0.077602	0.0000	—	
23.27.22.81	10.10.10.10	1	58	1	58	0	0	0.060511	0.0000	—	
23.27.22.248	10.10.10.10	1	58	1	58	0	0	0.107321	0.0000	—	

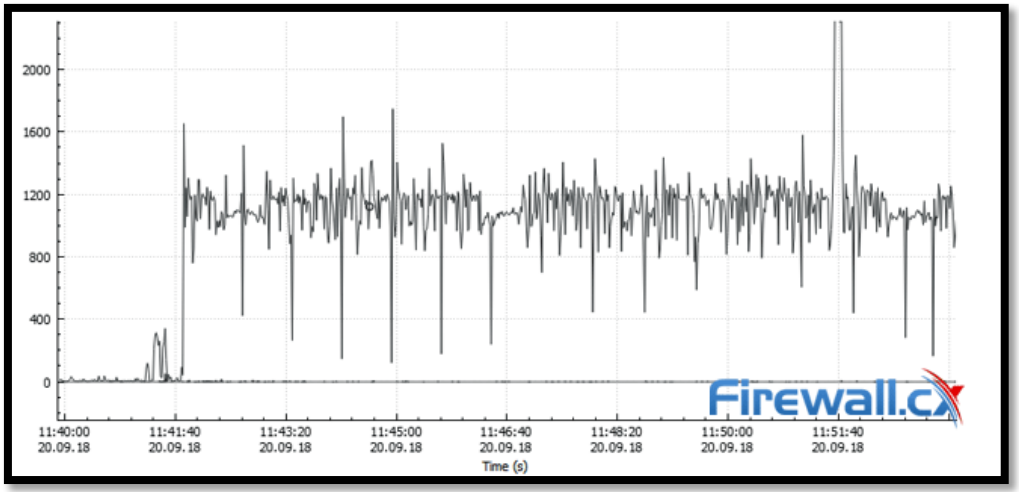
https://t.me/learninghets

Detection with Graphs

https://t.me/learningnets

Detecting DOS/ DDOS

- We can also view Wireshark's graphs for a visual representation of the uptick in traffic. The I/O graph can be found via the Statistics>I/O Graph menu. It shows a massive spike in overall packets from near 0 to up to 2400 packets a second.



https://t.me/learningnets

DEMO

https://t.me/learningnets

THANKS

https://t.me/learningnets