Department of
Bachelor of Computer Applications

Ethical Hacking Fundamentals

Lab File – CA 07

Subject Code: 19BCA4C02L
Class: IInd Year IInd Semester

Prepared By:
Suman Garai
20BCAR0246

Aim :

Perform Network Scan for UDP & TCP Packet Crafting techniques using hping3 tool in Kali Linux

Requirements :

- Virtualisation Software
- Kali Linux 2022.1
- Basics of hping3
- Internet Connection

Objectives :

To Run different scans :

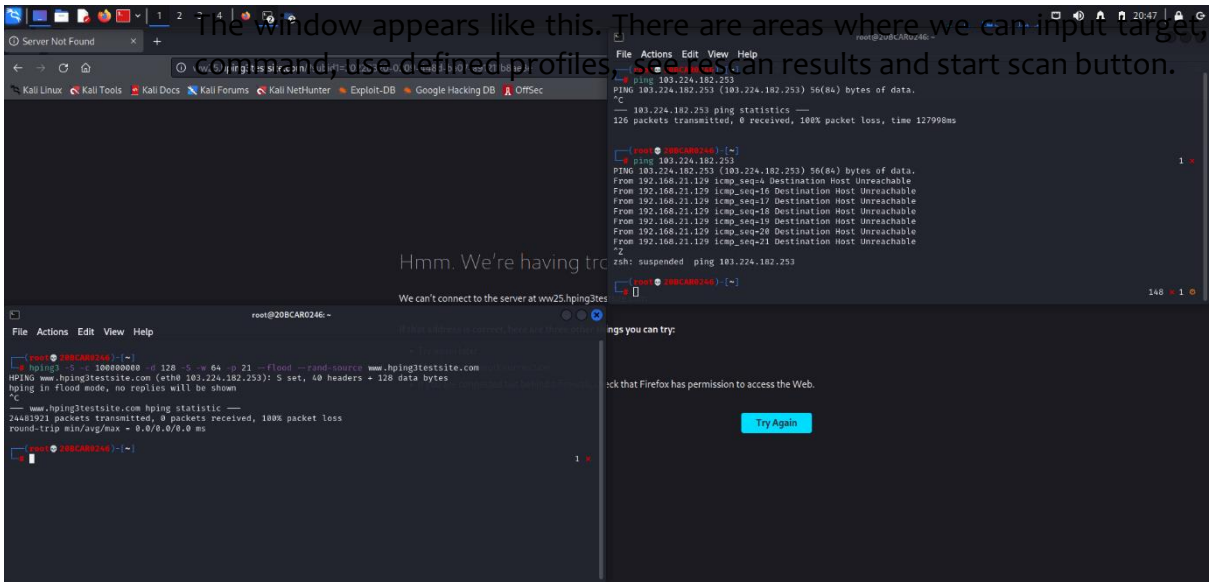
- ✓ Random IP DOS Attack
- ✓ TCP SYN Scan
- ✓ TCP ACK Scan

Procedure :

Random IP DOS Attack

Let me explain the syntax's used in this command:

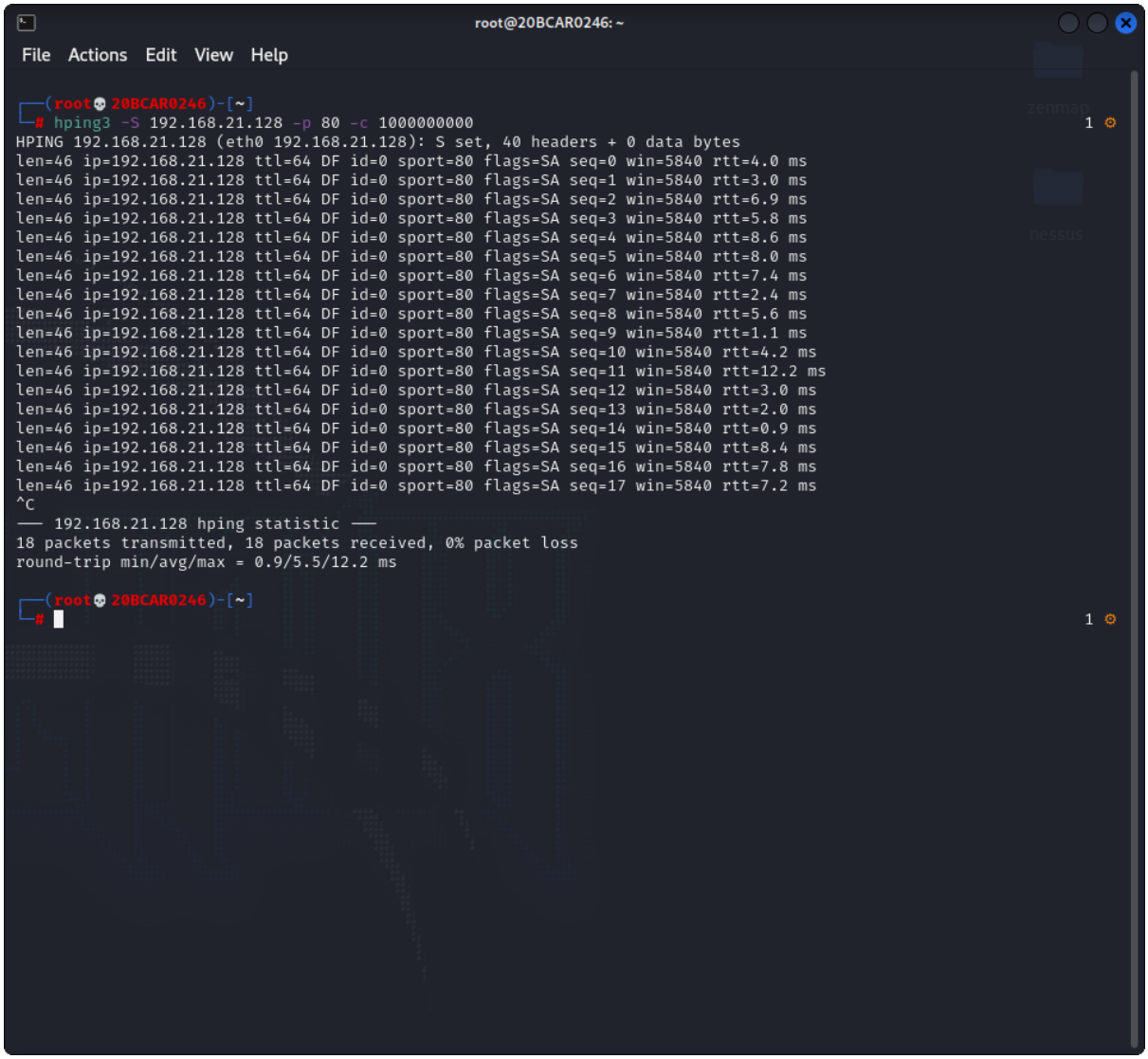
- `hping3`: Name of the application binary.
- `-c 100000000`: Number of packets to send.
- `-d 128`: Size of each packet that was sent to target machine.
- `-S`: I am sending SYN packets only.
- `-w 64`: TCP window size.
- `-p 21`: Destination port (21 being FTP port).
- `--flood`: Sending packets as fast as possible, without taking care to show incoming replies. Flood mode.
- `--rand-source`: Using Random Source IP Addresses.
- `www.hping3testsite.com`: Destination IP address or website name.



The window appears like this. There are areas where we can input target, command, use defined profiles, scan results and start scan button.

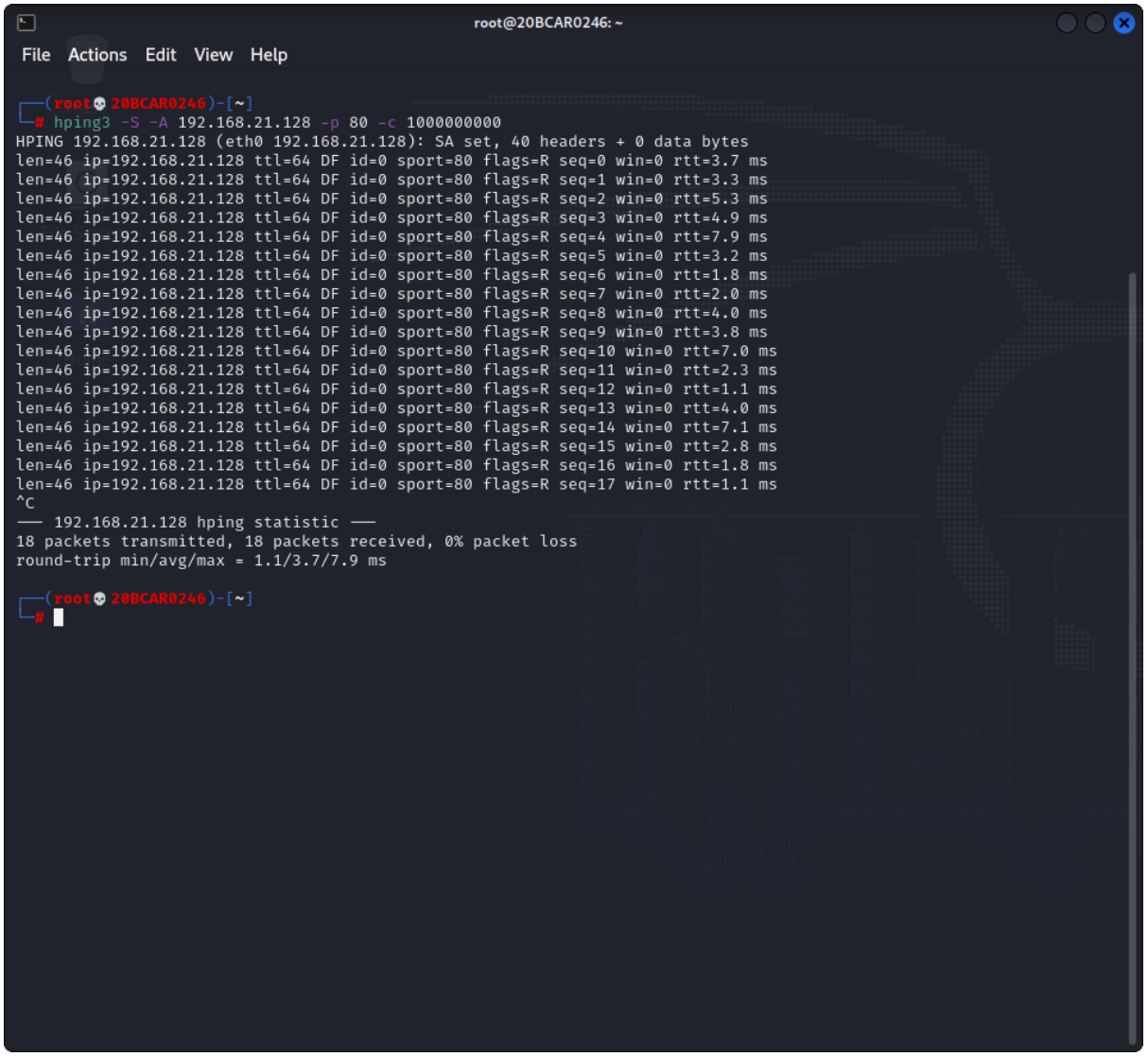
TCP SYN Scan

Command: `hping3 -S 192.168.21.128 -p 80 -c 1000000000`



TCP ACK Scan

Command: `hping3 -A 192.168.21.128 -p 80 -c 1000000000`



Conclusion :

Hping3 is a scriptable program that uses the TCL language, whereby packets can be sent or reveived via a binary string representation describing the packets. It can be used for DOS attack, for TCP ACK & SYN Scan etc.