



Department of  
**Bachelor of Computer Applications**

**Ethical Hacking Fundamentals**  
Lab File – CA 07

**Subject Code:** 19BCA4C02L  
**Class:** II<sup>nd</sup> Year II<sup>nd</sup> 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 :

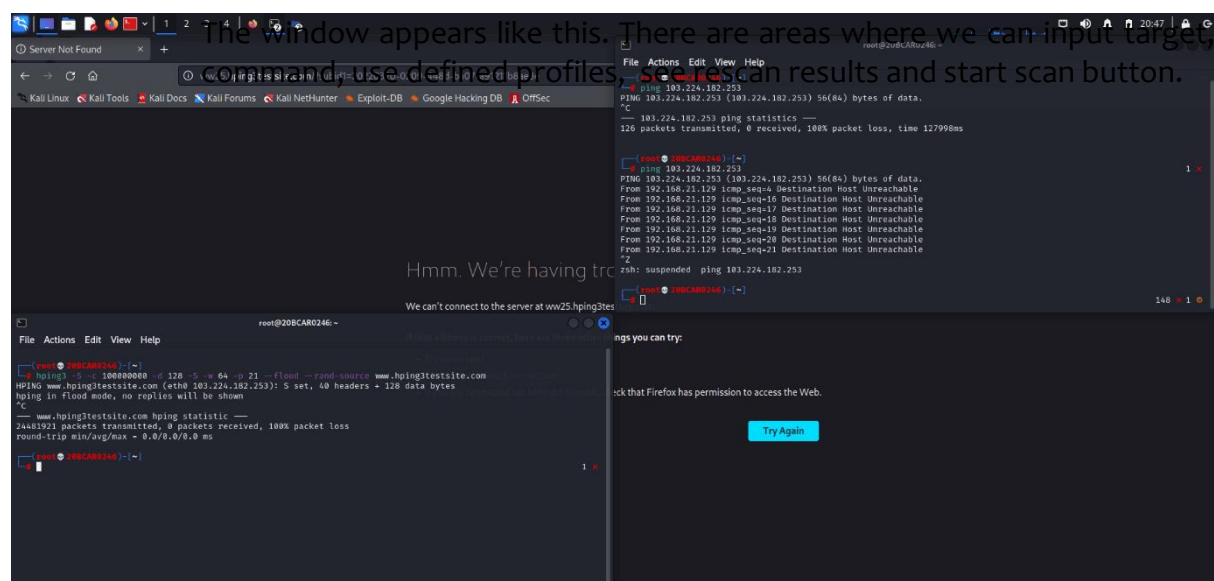
- ✓ Random IP DOS Attack
- ✓ TCP SYN Scan
- ✓ TCP ACK Scan

## 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.



## TCP SYN Scan

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

```
root@20BCAR0246: ~  
File Actions Edit View Help  
(root@20BCAR0246)~  
# hping3 -S 192.168.21.128 -p 80 -c 1000000000  
HPING 192.168.21.128 (eth0 192.168.21.128): S set, 40 headers + 0 data bytes  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=4.0 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=3.0 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=6.9 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5840 rtt=5.8 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5840 rtt=8.6 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=5 win=5840 rtt=8.0 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=5840 rtt=7.4 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=5840 rtt=2.4 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=8 win=5840 rtt=5.6 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=9 win=5840 rtt=1.1 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=10 win=5840 rtt=4.2 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=11 win=5840 rtt=12.2 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=12 win=5840 rtt=3.0 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=13 win=5840 rtt=2.0 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=14 win=5840 rtt=0.9 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=15 win=5840 rtt=8.4 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=16 win=5840 rtt=7.8 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=SA seq=17 win=5840 rtt=7.2 ms  
^C  
— 192.168.21.128 hping statistic —  
18 packets transmitted, 18 packets received, 0% packet loss  
round-trip min/avg/max = 0.9/5.5/12.2 ms  
(root@20BCAR0246)~
```

## TCP ACK Scan

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

```
root@20BCAR0246: ~  
File Actions Edit View Help  
root@20BCAR0246:~# hping3 -S -A 192.168.21.128 -p 80 -c 1000000000  
HPING 192.168.21.128 (eth0 192.168.21.128): SA set, 40 headers + 0 data bytes  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0 rtt=3.7 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=1 win=0 rtt=3.3 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=2 win=0 rtt=5.3 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=3 win=0 rtt=4.9 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=4 win=0 rtt=7.9 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=5 win=0 rtt=3.2 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=6 win=0 rtt=1.8 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=7 win=0 rtt=2.0 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=8 win=0 rtt=4.0 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=9 win=0 rtt=3.8 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=10 win=0 rtt=7.0 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=11 win=0 rtt=2.3 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=12 win=0 rtt=1.1 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=13 win=0 rtt=4.0 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=14 win=0 rtt=7.1 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=15 win=0 rtt=2.8 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=16 win=0 rtt=1.8 ms  
len=46 ip=192.168.21.128 ttl=64 DF id=0 sport=80 flags=R seq=17 win=0 rtt=1.1 ms  
^C  
— 192.168.21.128 hping statistic —  
18 packets transmitted, 18 packets received, 0% packet loss  
round-trip min/avg/max = 1.1/3.7/7.9 ms  
root@20BCAR0246:~#
```

## Conclusion :

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