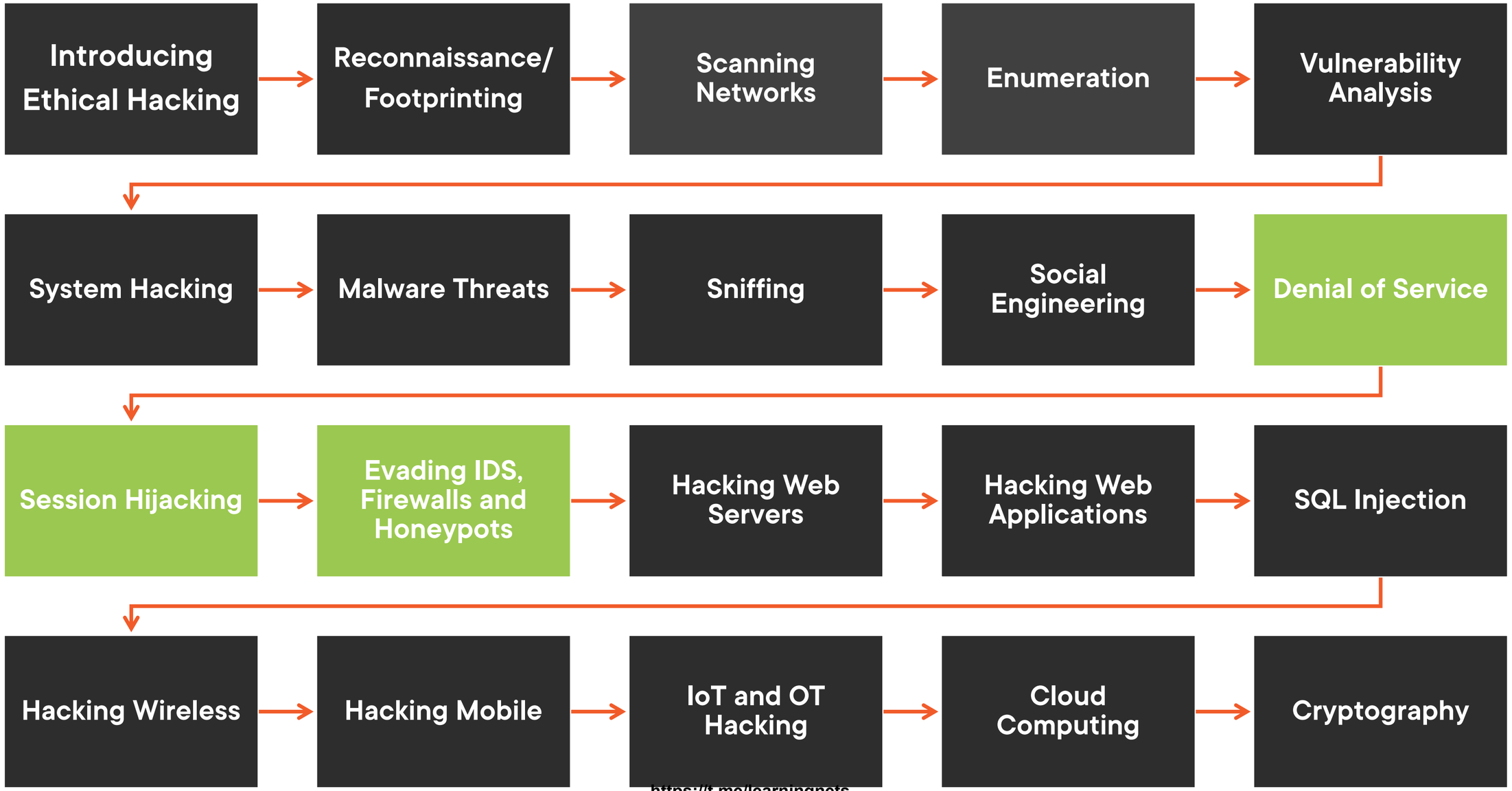
Ethical Hacking: Network and Perimeter Hacking

Denial of Service

Michael J. Teske
Principal Staff Author-Pluralsight

LinkedIn: /teskemj

Ethical Hacking



Course Overview

Denial of Service (DoS)

- Concepts
- Tactics & Techniques
- Countermeasures

Session Hijacking

- Concepts
- Tactics & Techniques
- Countermeasures

Course Overview

IDS, Firewalls and Honeypots

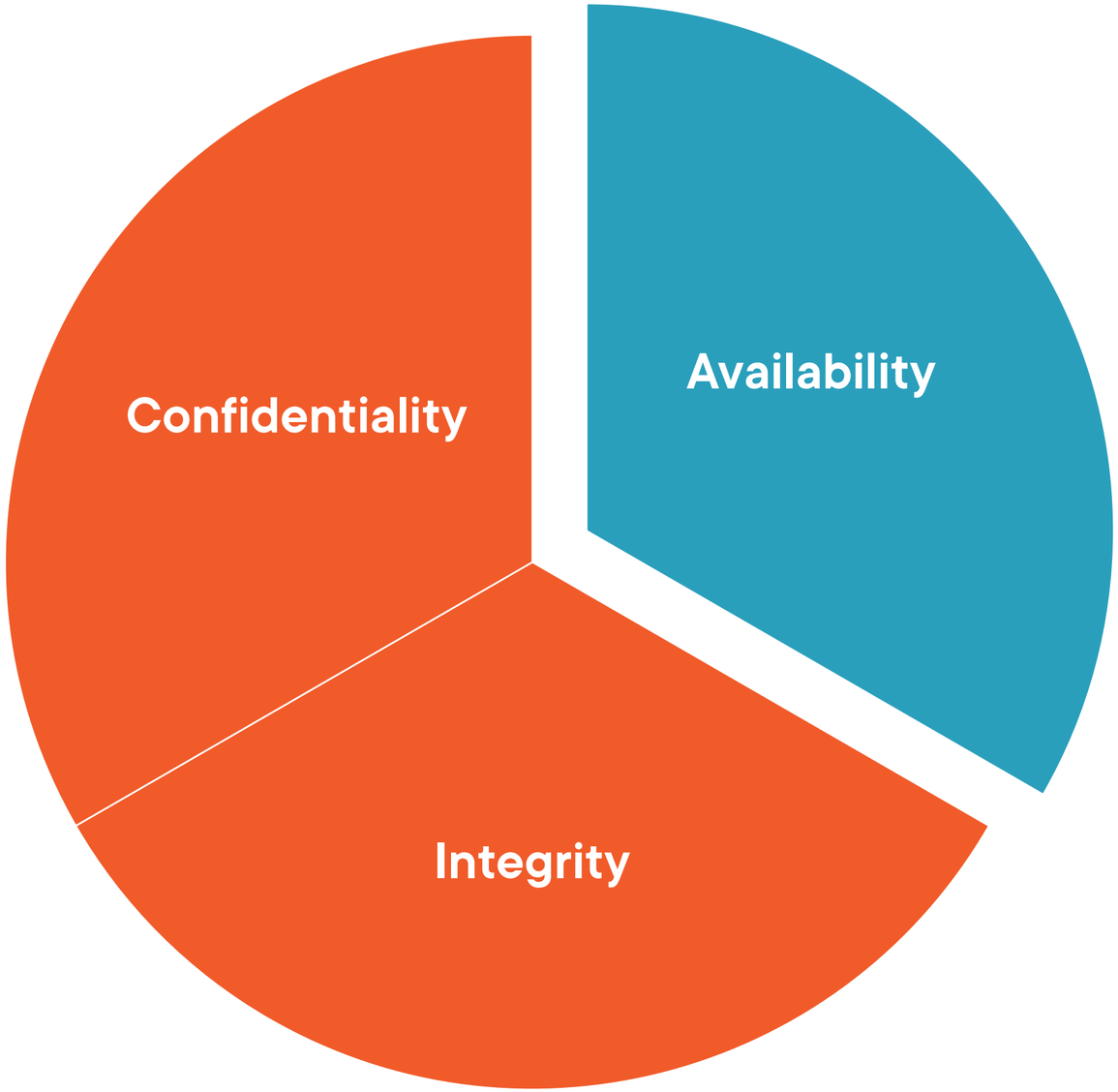
- Concepts
- Tactics & Techniques
- Countermeasures

Course Review

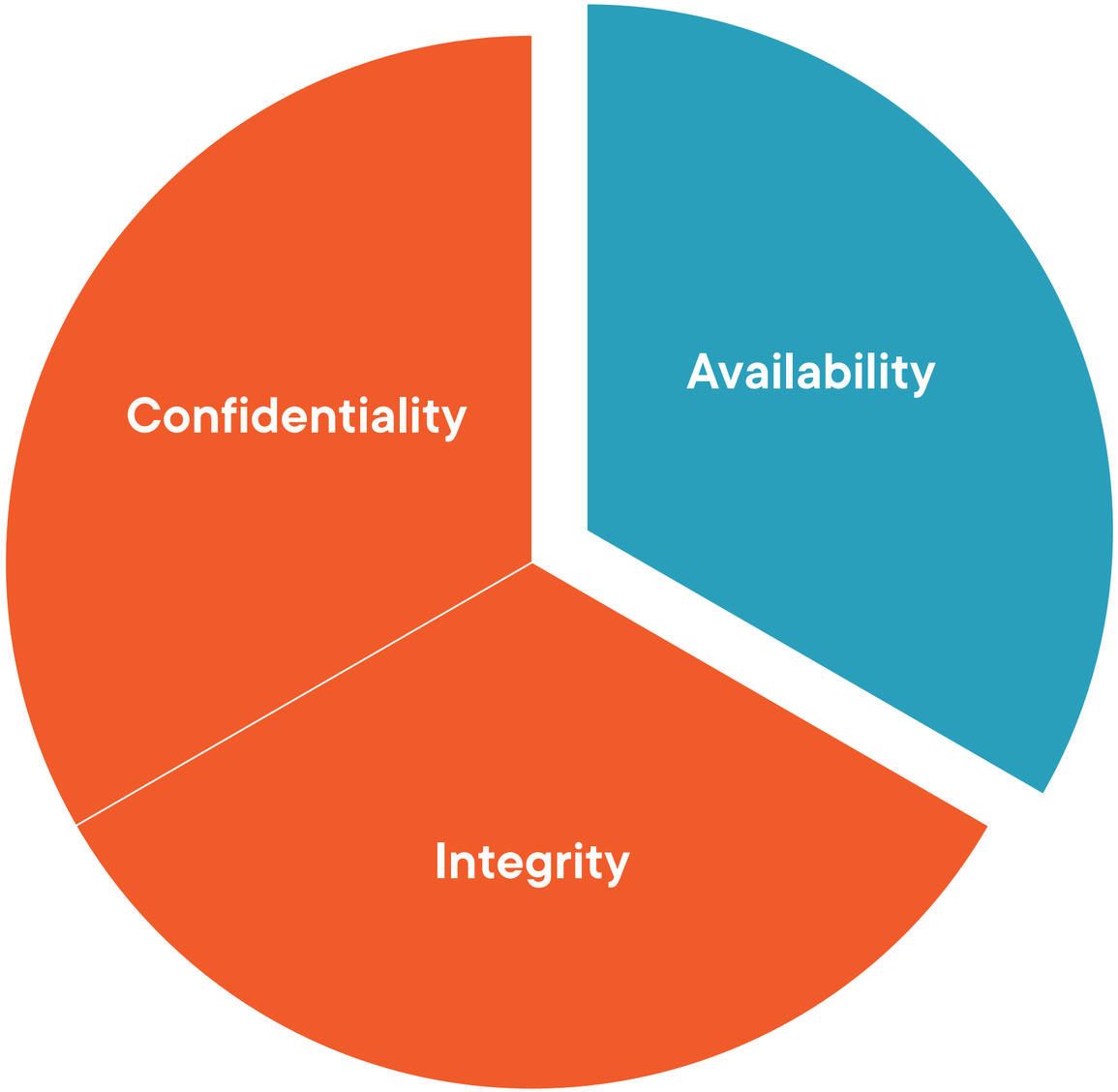
Denial of Service Concepts

Denial Of Service

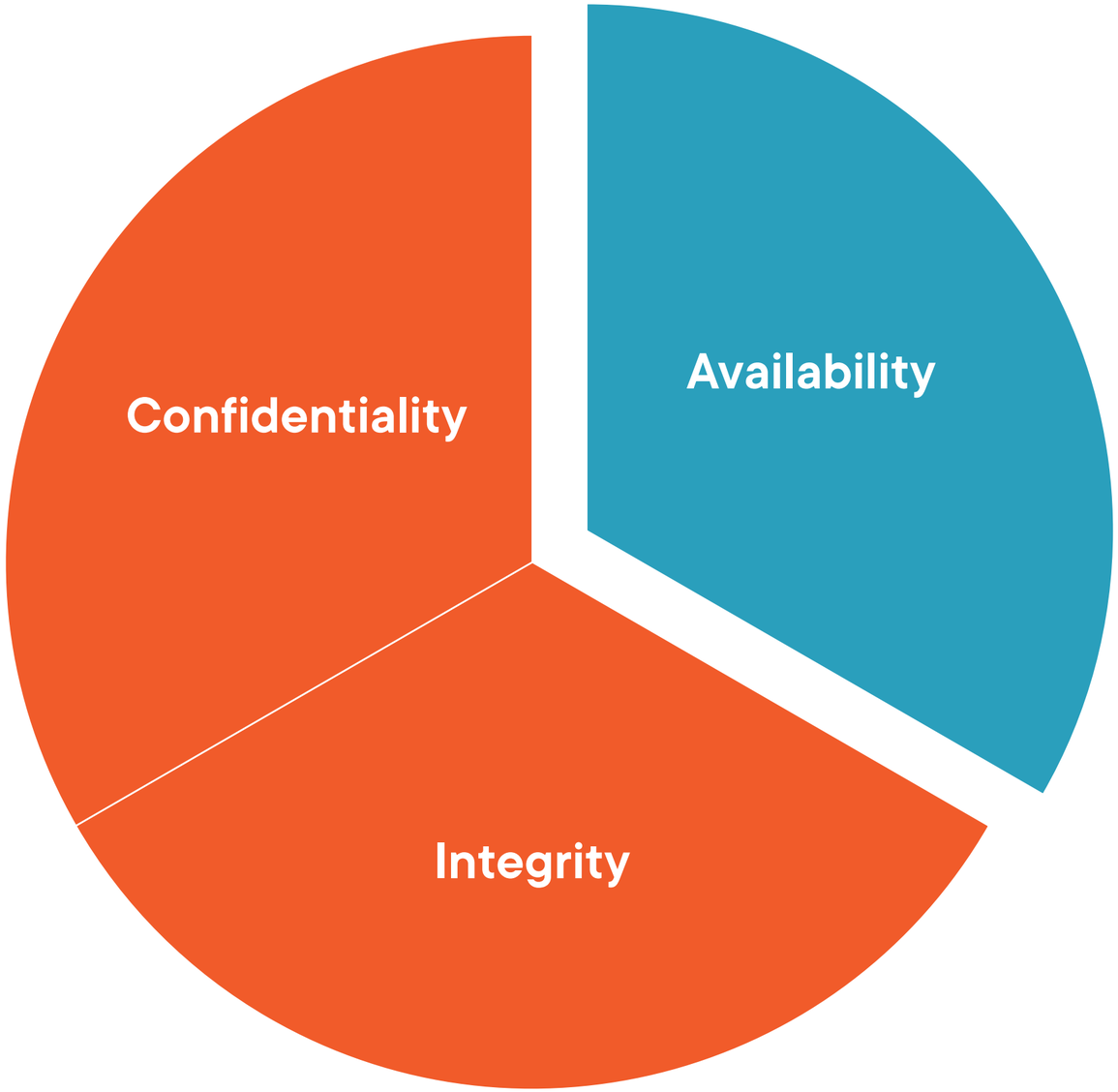
Denial Of Service



Denial Of Service



Denial Of Service



Denial of Service (DoS)

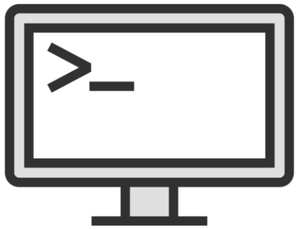
Attack is designed to prevent the use or availability of a service/resource

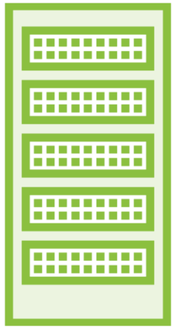
DoS uses a single connection while Distributed Denial of Service (DDoS) uses many sources of traffic

The *"many sources of traffic"* typically come from a botnet, a.k.a. "*distributed reflection denial-of-service*"

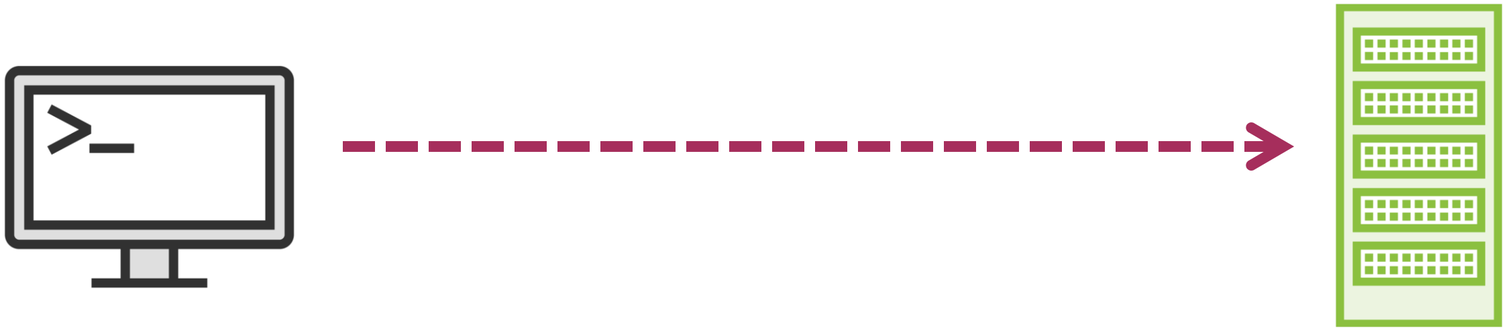
Botnets are a collection of infected computers controlled by the attacker

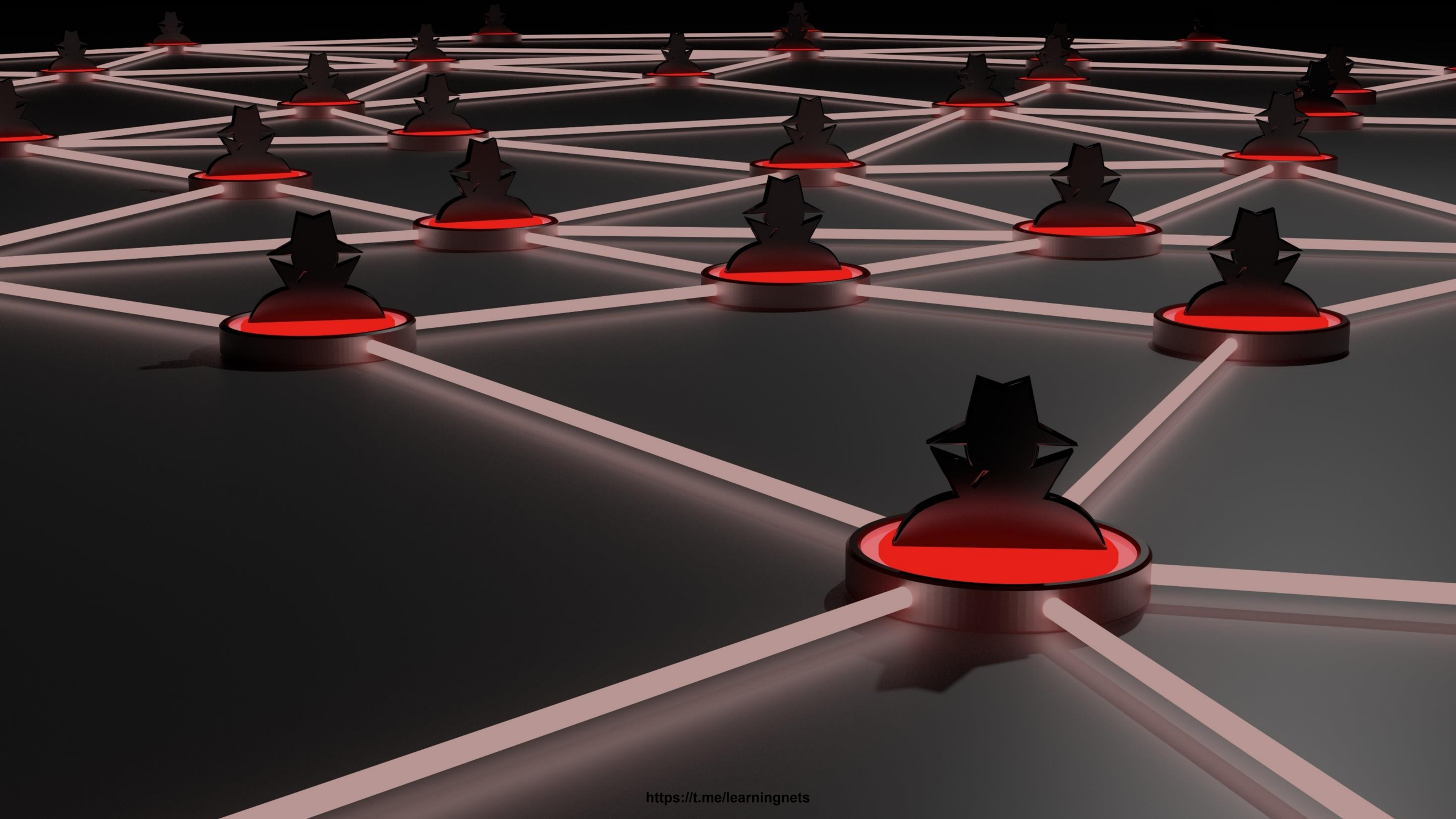
Denial of Service Attack



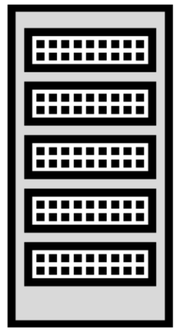


Denial of Service Attack

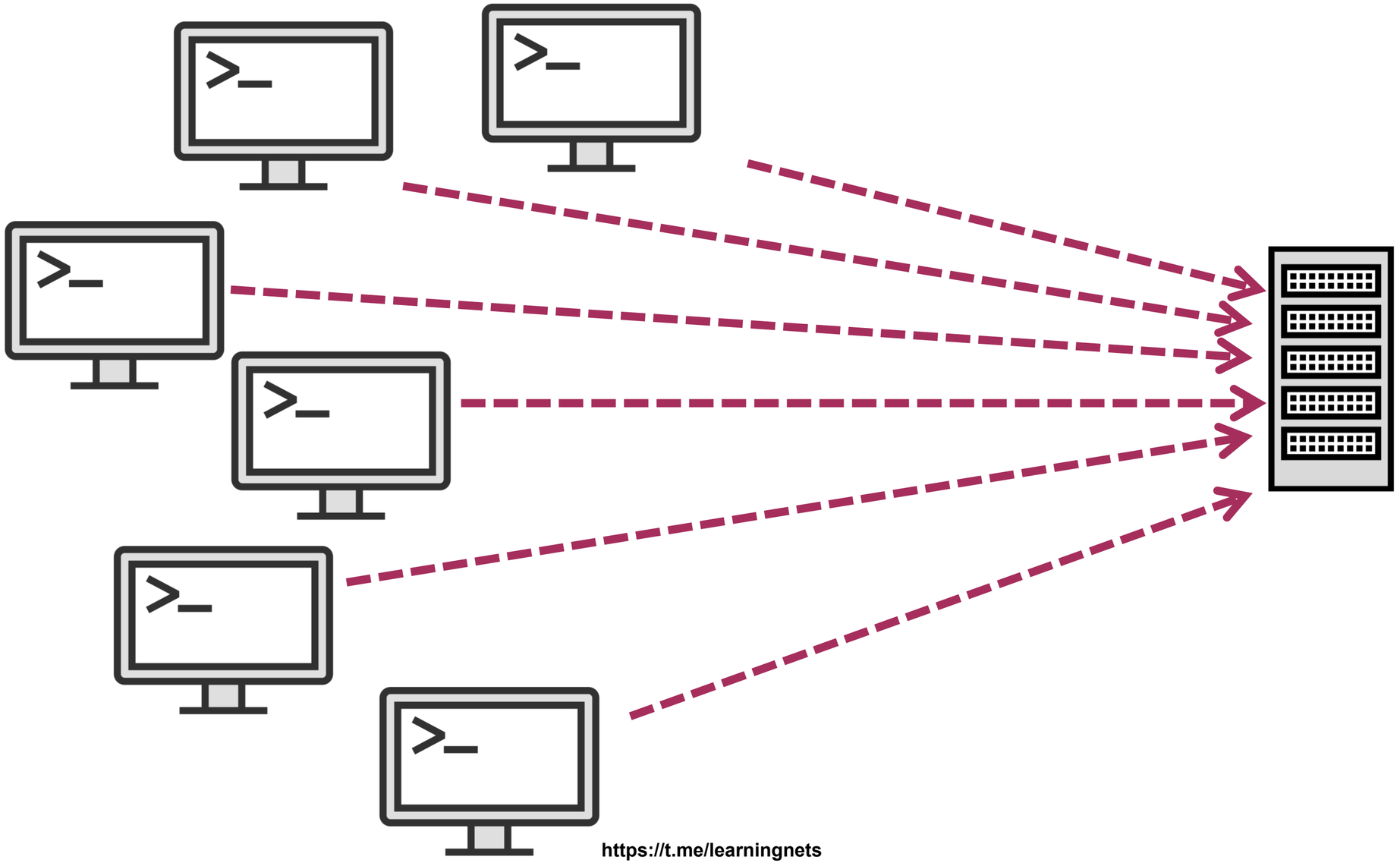




Distributed Denial of Service Attack (DDoS)



Distributed Denial of Service Attack (DDoS)



Tactics and Techniques

Denial of Service Attack Categories

Application Layer Attack

Protocol Attacks

Volumetric Attacks

Denial of Service Attack Categories

Application Layer Attack

Protocol Attacks

Volumetric Attacks

Denial of Service Attack Categories

Application Layer Attack

Protocol Attacks

Volumetric Attacks

Denial of Service Attack Categories

Application Layer Attack

Protocol Attacks

Volumetric Attacks

Denial of Service Attack Categories

Application Layer Attack

Protocol Attacks

Volumetric Attacks

Denial of Service Attack Categories

Application Layer Attack

Protocol Attacks

Volumetric Attacks

Denial of Service Attack Categories

Application Layer Attack

Protocol Attacks

Volumetric Attacks

DoS/DDoS Attacks

DoS/DDoS Attacks

TCP

state-exhaustion

DoS/DDoS Attacks

TCP

state-exhaustion

DoS/DDoS Attacks

TCP

state-exhaustion

UDP/SYN/ICMP flood

DoS/DDoS Attacks

TCP

state-exhaustion

UDP/SYN/ICMP flood

DoS/DDoS Attacks

TCP

state-exhaustion

UDP/SYN/ICMP flood

SYN attack

DoS/DDoS Attacks

TCP state-exhaustion	**UDP/SYN/ICMP flood**	**SYN attack**
Smurf		

DoS/DDoS Attacks

TCP state-exhaustion	**UDP/SYN/ICMP flood**	**SYN attack**
Smurf		

DoS/DDoS Attacks

TCP state-exhaustion	**UDP/SYN/ICMP flood**	**SYN attack**
Smurf	**Ping of death**	

DoS/DDoS Attacks

TCP state-exhaustion	**UDP/SYN/ICMP flood**	**SYN attack**
Smurf	**Ping of death**	**Zero day**

Dos/DDoS Tools

Slowloris

High Orbit Ion Cannon (HOIC)

Low Orbit Ion Cannon (LOIC)

R.U.D.Y

hping3

Dos/DDoS Tools

Slowloris

High Orbit Ion Cannon (HOIC)

Low Orbit Ion Cannon (LOIC)

R.U.D.Y

hping3

Dos/DDoS Tools

High Orbit Ion Cannon (HOIC)

Low Orbit Ion Cannon (LOIC)

R.U.D.Y

hping3

Dos/DDoS Tools

High Orbit Ion Cannon (HOIC)

Low Orbit Ion Cannon (LOIC)

R.U.D.Y

hping3

Dos/DDoS Tools

R.U.D.Y

hping3

Dos/DDoS Tools

R.U.D.Y

hping3

Dos/DDoS Tools

R.U.D.Y

hping3

Dos/DDoS Tools

[redacted]

[redacted]

[redacted]

hping3

Dos/DDoS Tools

[redacted]

[redacted]

[redacted]

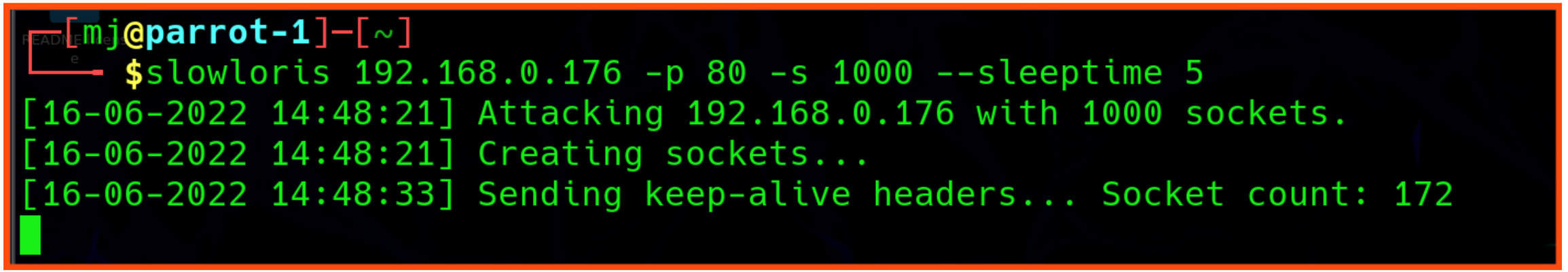
hping3

Dos/DDoS Tools

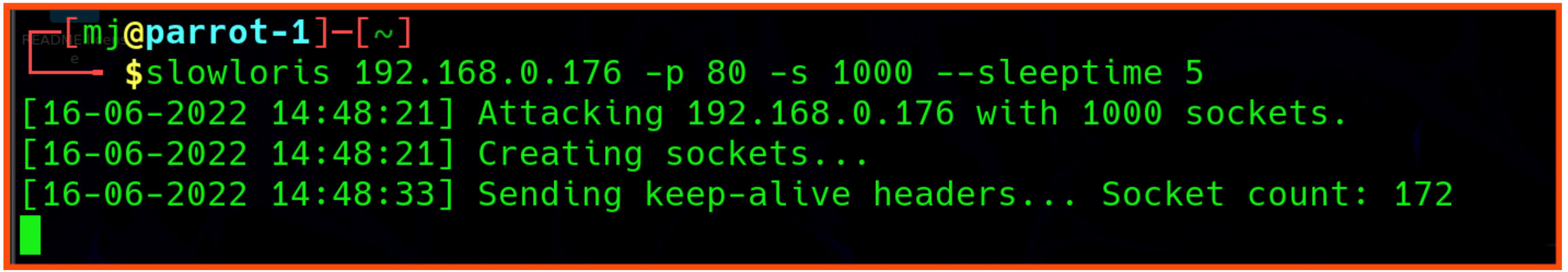
Slowloris and Hping3

Slowloris and Hping3

Slowloris and Hping3



Slowloris and Hping3



Slowloris and Hping3

```
┌──[mj@parrot-1]─[~]
└──╼ $slowloris 192.168.0.176 -p 80 -s 1000 --sleeptime 5
[16-06-2022 14:48:21] Attacking 192.168.0.176 with 1000 sockets.
[16-06-2022 14:48:21] Creating sockets...
[16-06-2022 14:48:33] Sending keep-alive headers... Socket count: 172
```

```
┌──[✗]─[mj@parrot-1]─[~]
└──╼ $sudo hping3 -c 1000000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.0.176
HPING 192.168.0.176 (ens33 192.168.0.176): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

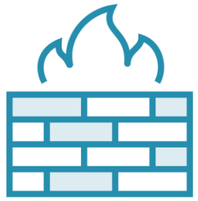
Demo

Denial-of-Service using:

- SYN Flood using Hping3
- Application layer attack using Slowloris

Countermeasures

Countermeasures



Properly configured perimeter security devices

Disable unnecessary services, ensure systems are up to date

Harden web servers

Use reverse proxy servers, ensure ISP has controls in place

Learning Check

Learning Check

Syn flood/attack

Learning Check

- **Syn flood/attack**
- **Application layer attack**

Learning Check

- **Syn flood/attack**
- **Application layer attack**

Learning Check

- **Syn flood/attack**
- **Application layer attack**
- **Volumetric attack**

Learning Check

- **Syn flood/attack**
- **Application layer attack**
- **Volumetric attack**

Learning Check

- Syn flood/attack
- Application layer attack
- Volumetric attack
- Botnets/Zombies

Module Review

Key Learnings

DDoS/DoS attack types

Tactics, techniques and tools

Countermeasures

Up Next:
Session Hijacking