DDoS Attack, Detection & Mitigation

Name	Roll Number
Sreya Naradasu	CB.EN.U4CSE22059
Prakhyati Kothapalli	CB.EN.U4CSE22209
Mahisri Nagireddy	CB.EN.U4CSE22338
Hansika Sayyad	CB.EN.U4CSE22543
Abhisri Neka	CB.EN.U4CSE22102

Setting Up the Local Web Server (Apache)

What is it?

Create a mini website server on your local machine using **Apache2**, a popular web server software.

Commands:

- **sudo apt update && sudo apt install apache2 -y**: Updates package lists and installs Apache.
- **sudo systemctl start apache2**: Starts the server immediately.
- **sudo systemctl enable apache2**: Starts Apache on boot.
- **curl http://localhost**: Checks if Apache is working.

Why?

Simulate a real-world environment where a server is hosted and attackers target it.

Simulating a DDoS Attack

What is a DDoS?

Distributed Denial of Service floods a server with requests until it crashes.

Tool Used: hping3

sudo apt install hping3 -y: Installs hping3 to send customized packets.

Command:

sudo hping3 -S -p 80 --flood --rand-source 127.0.0.1: Sends SYN packets to port 80, flooding from random sources.

Why?

Mimic real-world DDoS scenarios for testing defenses.

Attack: SYN Flood

A SYN Flood attack is a type of Denial-of-Service (DoS) attack that exploits the TCP handshake process to overwhelm a server with half-open connections, making it unavailable for legitimate users.

Detecting the DDoS Attack: Count Active Connections

Command

netstat -an | grep :80 | wc -l: Lists open connections, filters to port 80, and counts them.

Explanation

netstat -an: Lists all open connections. **grep :80**: Filters connections to port 80. **wc -l**: Counts open connections.

Result

More connections than usual indicate a potential DDoS.

Detecting the DDoS Attack: Find Top Attacker IPs

1

Command

```
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr | head
```

2

Explanation

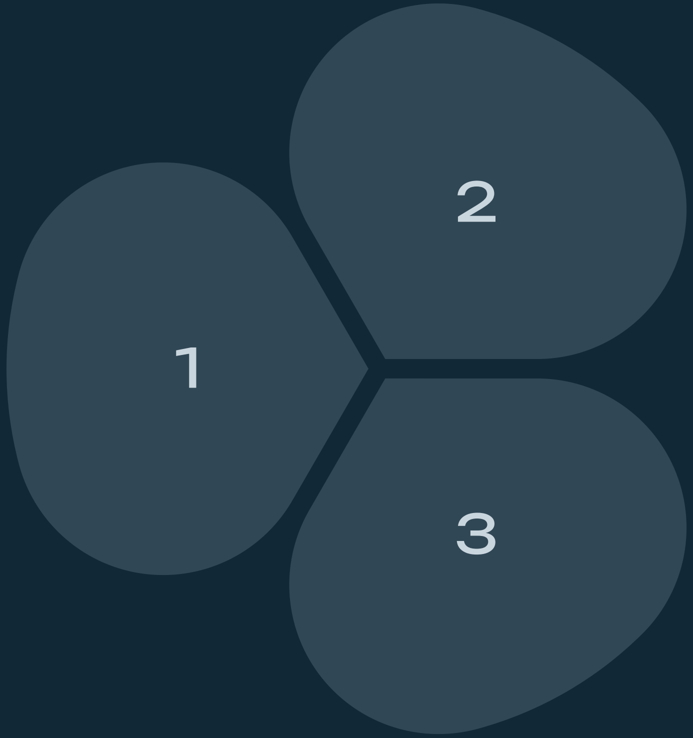
Shows active TCP/UDP connections, grabs IP addresses, removes port numbers, counts IP occurrences, and sorts by frequency.

3

Result

Tells you who is attacking you by listing the top attacking IPs.

Blocking the Attack: Block a Single Attacker IP



Command

```
sudo iptables -A INPUT -s
<ATTACKER_IP> -j DROP
```

Explanation

Adds a rule to the INPUT chain to match packets from the attacker IP and silently drop them.

Result

The attacker is blocked and cannot tell they've been blocked.

Blocking the Attack: Block Multiple IPs at Once

1

Create a file

echo -e "ip1\nip2\n..." > blocked_ips.txt: Creates a file with all malicious IPs.

2

Block IPs

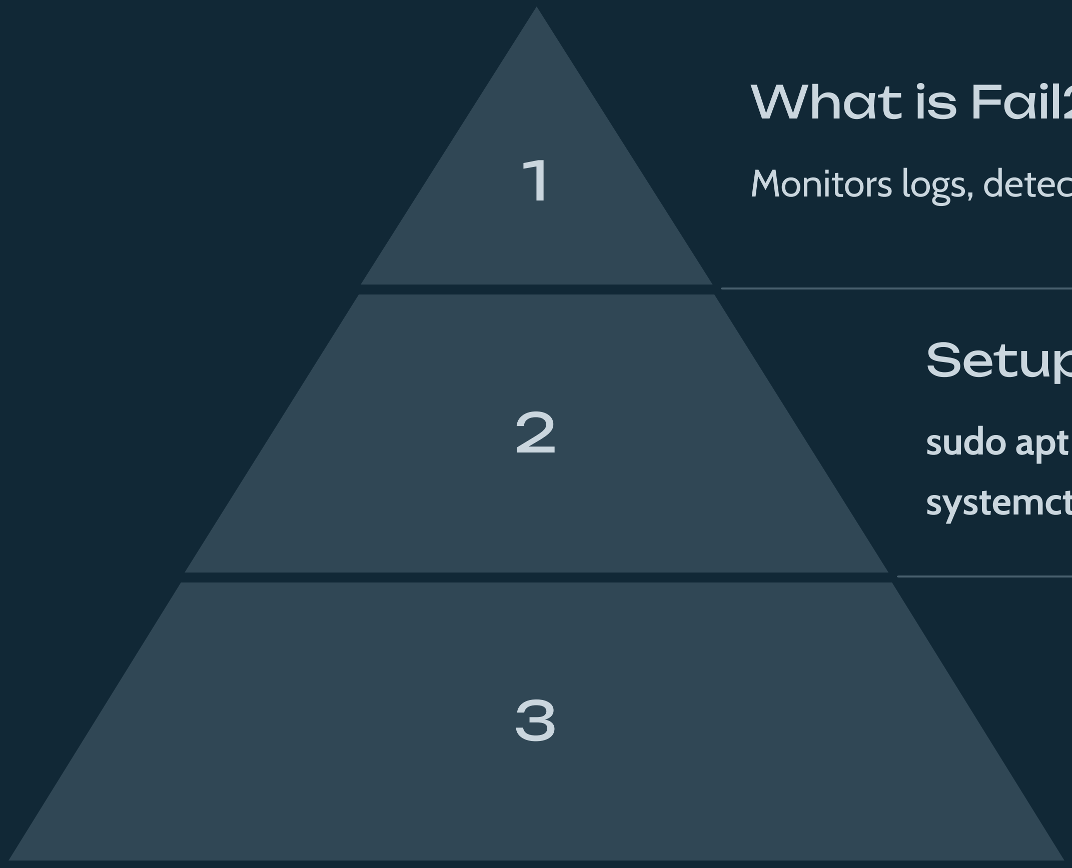
while read ip; do sudo iptables -A INPUT -s "$ip" -j REJECT; done < blocked_ips.txt

3

Explanation

Reads one IP at a time and blocks each one efficiently.

Automatically Detect & Block Using Fail2Ban



What is Fail2Ban?

Monitors logs, detects malicious behavior, and bans IPs.

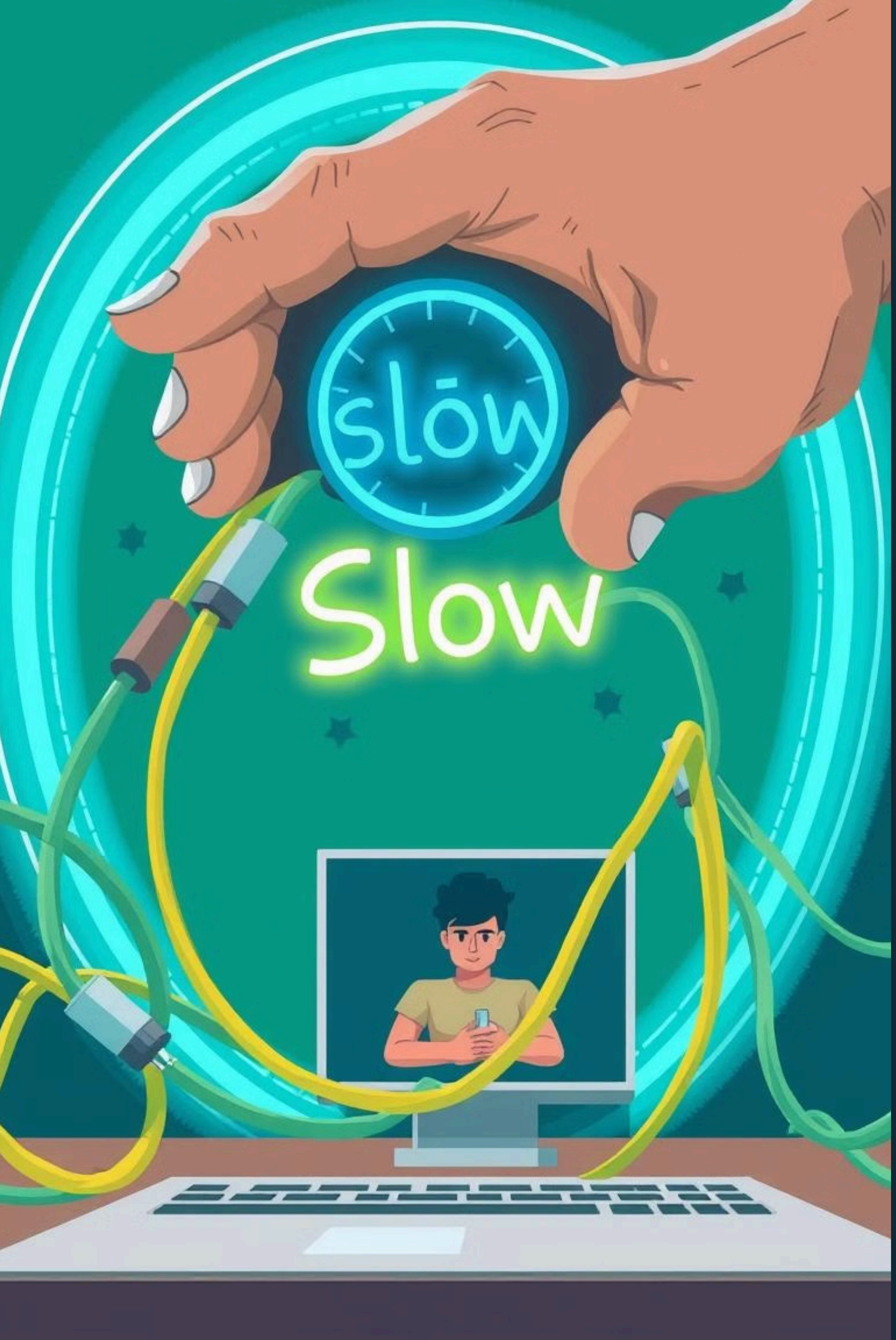
Setup

sudo apt install fail2ban -y, **sudo systemctl enable fail2ban**, **sudo systemctl start fail2ban**

Configuration

Edit **/etc/fail2ban/jail.local** to set log paths and retry limits.

Set it and forget it. Fail2Ban watches and protects like a bodyguard.



Rate Limiting via iptables

Command

```
sudo iptables -A INPUT -p tcp --dport 80 -m limit --limit 10/s --limit-burst 20 -j ACCEPT
```

Explanation

Allows only 10 packets per second per IP, with a burst of 20 before rate limiting.

Result

Stops spamming by any single IP.

Verifying Protection

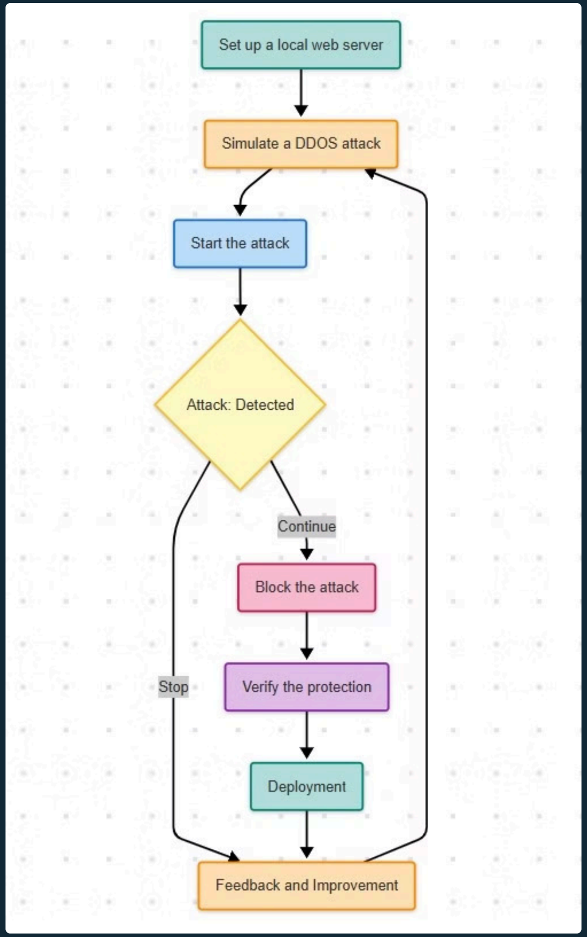
1 **Command**

netstat -an | grep :80 | wc -l: Re-check connection numbers after blocking and rate limiting.

2 **Result**

Connection numbers should drop or stabilize, indicating successful protection.

Block diagram


Set up a local web server
Simulate a DDOS attack
Start the attack
Attack: Detected
Continue
Block the attack
Stop
Verify the protection
Deployment
Feedback and Improvement