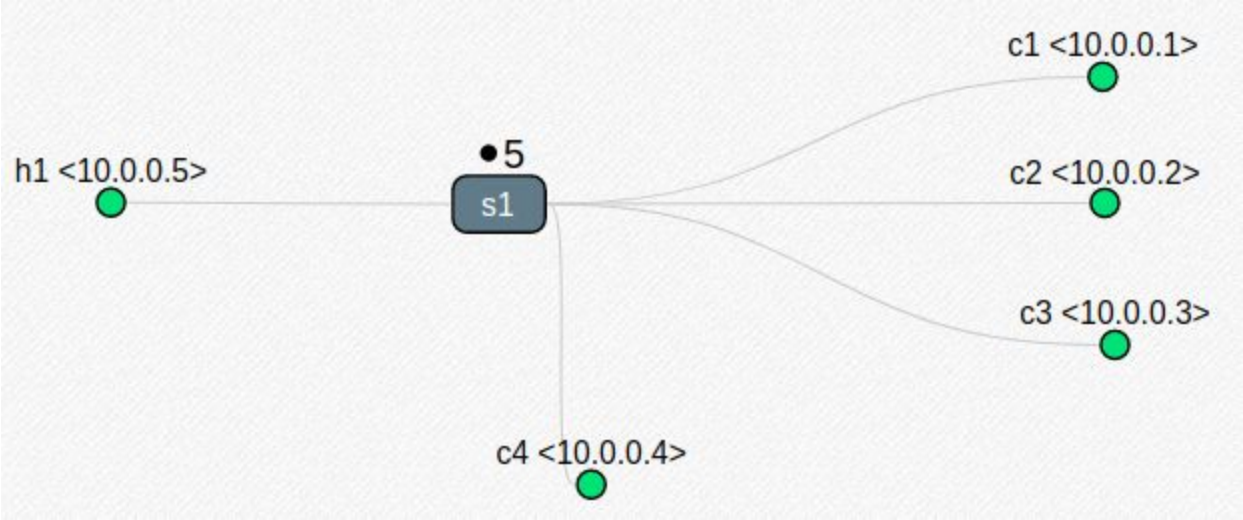
Lab 5: Snort-based Firewall for Intrusion Detection

M Uday Theja
CS14B044

TOPOLOGY:



- Server - h1 <10.0.0.5>
- Gateway Node - s1
- Client1 - c1 <10.0.0.1>
- Client2 - c2 <10.0.0.2>
- Client3 - c3 <10.0.0.3>
- Client4 - c4 <10.0.0.4>

LEGITIMATE TRAFFIC:

- Client **c1** initiates **ping** command sending **ICMP** packets every 3 seconds to server **h1**
- Client **c2** initiates **iperf** command sending **TCP** packets every 5 seconds to server **h1**
- Client **c3** initiates **iperf -u** command sending **UDP** packets every 7 seconds to server **h1**
- *Used Threads for each client for simultaneous communication*

ATTACK TRAFFIC:

- **Denial Of Service (DOS):**
    - Client **c4** uses **hping3** command with **-S --flood** options to initiate **TCP SYN Flood** to server **h1**
- **Distributed Denial Of Service (DDOS):**
    - Client **c4** uses **hping3** command with **-S --flood --rand-source** options to initiate **TCP SYN Flood** to server **h1** with spoofed IP

SNORT RULES:

DOS / DDOS

- **alert tcp $HOME_NET any -> $HOME_NET any (flags: S; msg: "Possible DOS or DDOS Detected"; flow: stateless; detection_filter: track by_dst, count 100, seconds 5; sid: 1000001; rev:001;)**
- Tracks the number of packets at destination and triggers alert if more than 100 packets arrive in 5 seconds
- The rule works well based on the input count and seconds

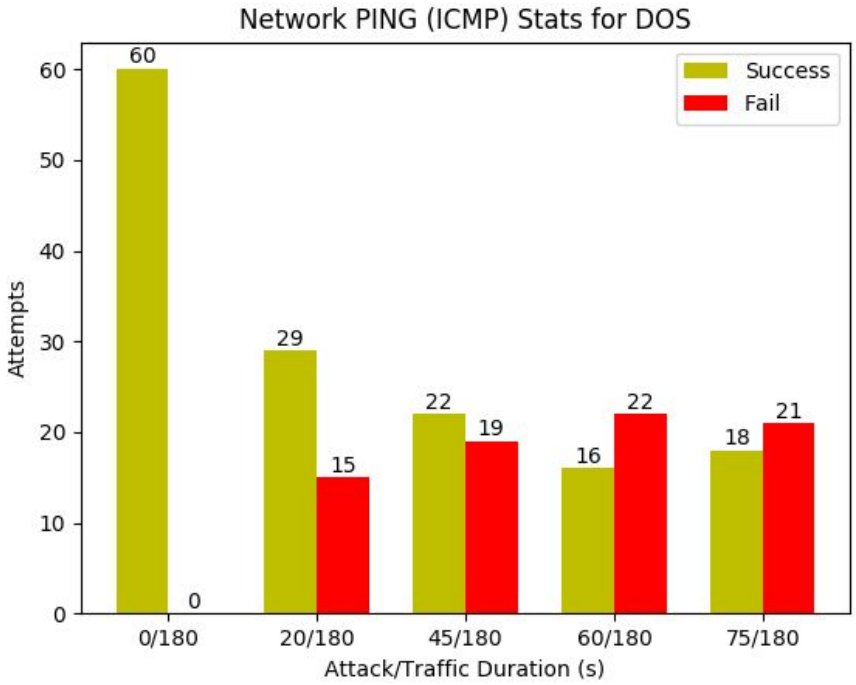
DOS

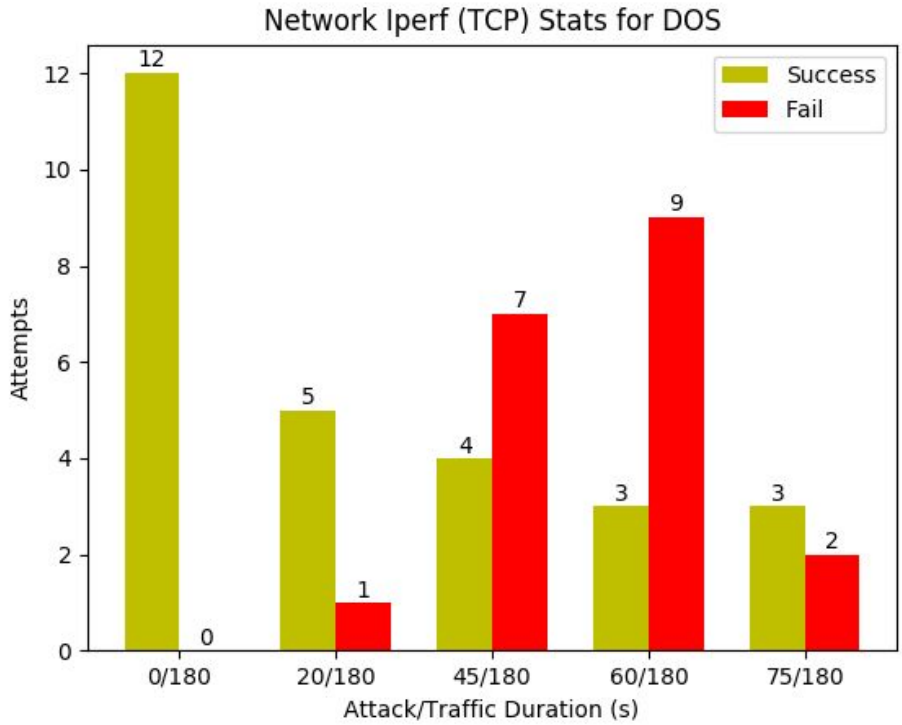
- **alert tcp $HOME_NET any -> $HOME_NET any (flags: S; msg: "DOS Attack"; flow: stateless; detection_filter: track by_src, count 100, seconds 5; sid: 1000002; rev:001;)**
- Tracks the number of packets at source and triggers alert if more than 100 packets arrive in 5 seconds
- The rule works well based on the input count and seconds

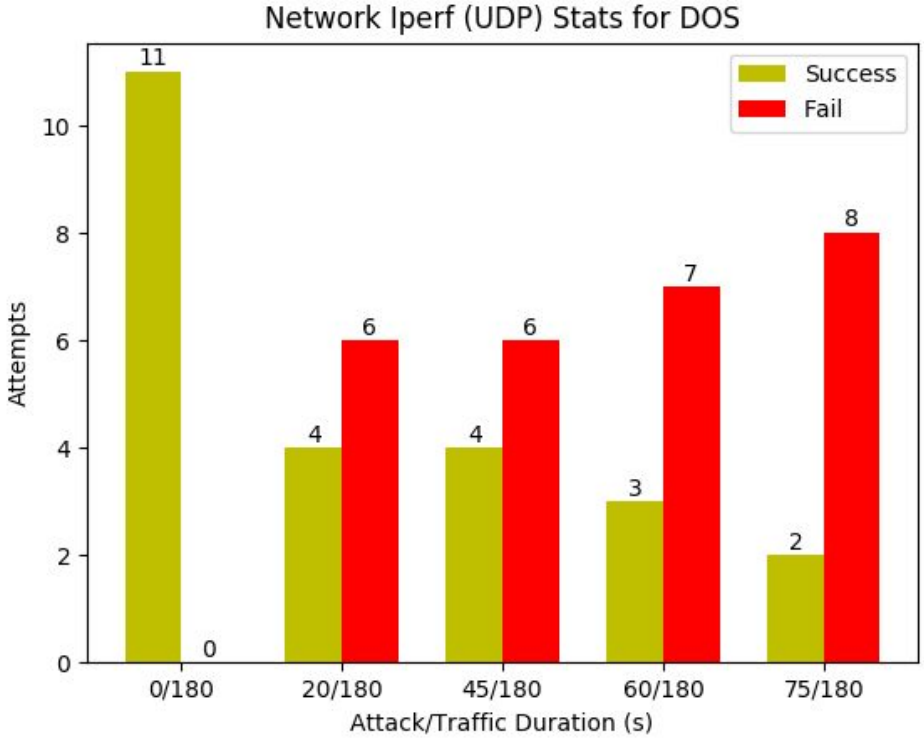
SPOOFING ATTACK

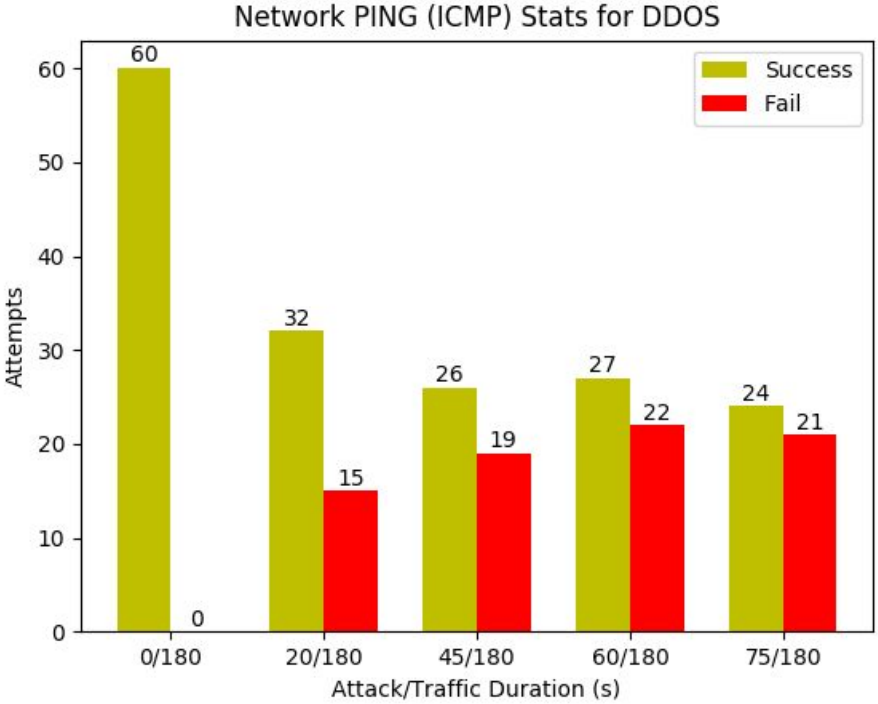
- Added **172.16.0.0/12** subnet under blacklist
- Enabled **scan_local** for preprocessor
- **alert (msg: "REPUTATION_EVENT_BLACKLIST"; sid: 1; gid: 136; rev: 1; metadata: rule-type preproc ; classtype:bad-unknown;)**
- If any packet from the blacklisted subnet arrives then an alert is triggered

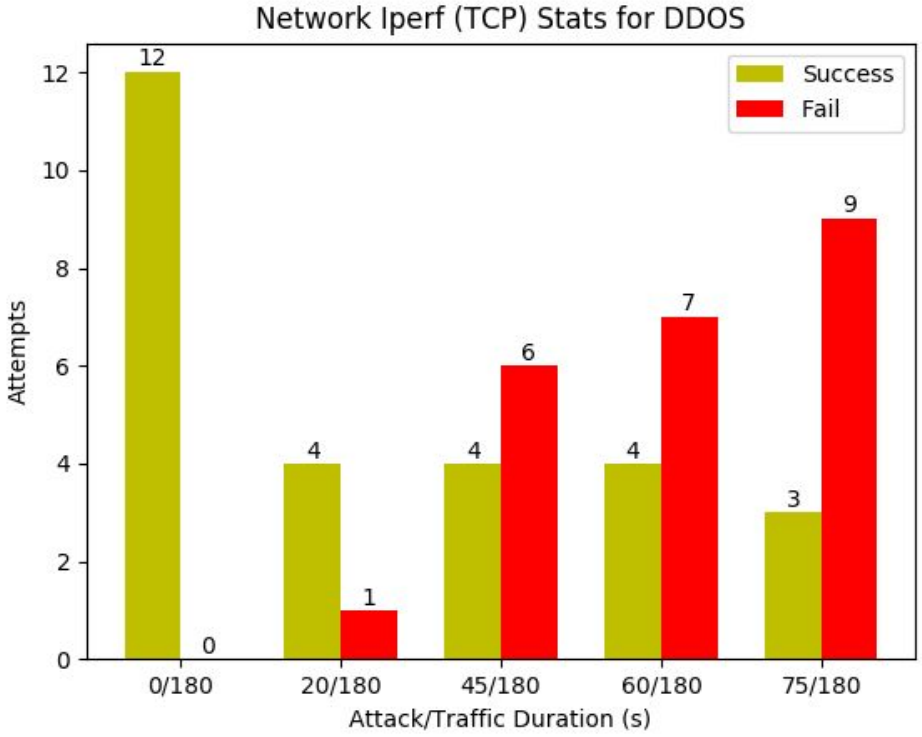
RESULTS:

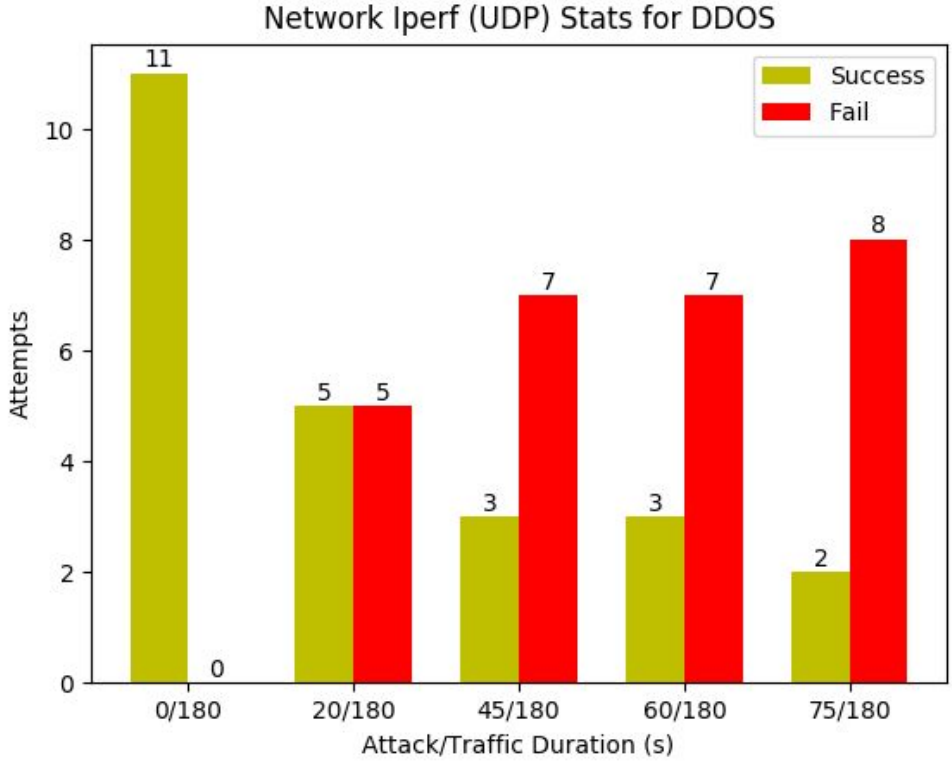

Network PING (ICMP) Stats for DOS
Success
Fail
Attempts
Attack/Traffic Duration (s)
0/180
20/180
45/180
60/180
75/180
60
0
29
15
22
19
16
22
18
21


Network Iperf (TCP) Stats for DOS
Success
Fail
Attempts
Attack/Traffic Duration (s)
0/180
20/180
45/180
60/180
75/180
12
0
5
1
4
7
3
9
3
2


Network Iperf (UDP) Stats for DOS
Success
Fail
Attempts
Attack/Traffic Duration (s)
0/180
20/180
45/180
60/180
75/180
11
0
4
6
4
6
3
7
2
8


Network PING (ICMP) Stats for DDOS
Success
Fail
Attempts
Attack/Traffic Duration (s)
0/180
20/180
45/180
60/180
75/180
60
0
32
15
26
19
27
22
24
21


Network Iperf (TCP) Stats for DDOS
Success
Fail
Attempts
Attack/Traffic Duration (s)
0/180
20/180
45/180
60/180
75/180
12
0
4
1
4
6
4
7
3
9


Network Iperf (UDP) Stats for DDOS
Success
Fail
Attempts
Attack/Traffic Duration (s)
0/180
20/180
45/180
60/180
75/180
11
0
5
5
3
7
3
7
2
8