Université Saint-Joseph de Beyrouth
Faculté d'ingénierie
Institut national des télécommunications et de l'informatique

Assessing the Potential of Suricata Under Multi-Layer Denial-of-Service Attacks

Michaela EL RIF and Andrew ZGHEIB

Supervisor: **Prof. Gerard CHALHOUB**

May 29, 2026

Introduction

Problematic

What are the limitations of Suricata in detecting DoS attacks?

Background

Denial-of-Service (DoS) attacks:

- Volumetric attacks
- Protocol attacks
- Application-layer attacks

Intrusion Detection System (IDS):

- Security solution
- Real-time detection
- Alert based on rules

Objectives

Evaluation of Suricata's performance under two scenarios:

- Individual DoS attacks
- Combined distinct DoS attacks

Scope & Constraints

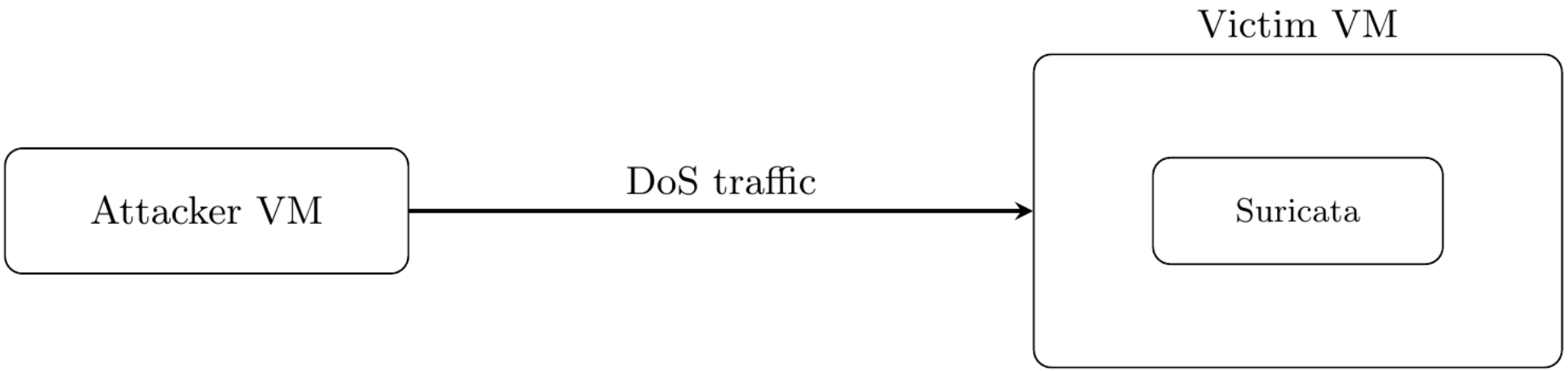
- Virtual Environment
- Normal traffic vs Real-world traffic
- No external connectivity
- Thresholds based on DoS scenarios

Related Work

- Suricata's effectiveness as a Network IDS (NIDS)
- Detection of UDP flood attacks

Methodology

System Architecture



VM Specifications

Specification	Attacker VM	Victim VM
Operating System	Kali Linux 2026.1	Ubuntu Desktop 26.04 LTS
vCPU Cores	8 vCPUs	2 vCPUs
Memory	8 GB	4 GB
Disk Space	80 GB	20 GB

Suricata Pipeline

DoS Attacks

- UDP Flood
- ICMP Flood
- SYN Flood

Individual DoS Attacks

Measured traffic (1/2)

Each attack was simulated from one terminal

Attack	Min. (pps)	Max. (pps)	Mean (pps)	Std Dev
UDP Flood	3404	3644	3518	79
ICMP Flood	2937	3932	3489	364
SYN Flood	4004	4390	4213	110

CPU consumption less than 35%

Measured traffic (2/2)

Each attack was simulated from two terminals

Attack	Min. (pps)	Max. (pps)	Mean (pps)	Std Dev
UDP Flood	8334	9849	9117	577
ICMP Flood	7181	8538	8070	399
SYN Flood	8435	9676	9022	357

CPU consumption above 45%

Ruleset Configuration (1/3)

```
alert udp any any -> $HOME_NET any (
        msg:"Possible UDP Flood";  flow: stateless;
        threshold: type threshold, track by_rule, count 6000, seconds 1;
        sid:1000001;  rev:2;
)
```

Ruleset Configuration (2/3)

```
alert icmp any any -> $HOME_NET any (
        msg:"Possible ICMP Flood";  itype: 8;
        threshold: type threshold, track by_rule, count 6000, seconds 1;
        sid:1000002;  rev:2;
)
```

Ruleset Configuration (3/3)

```
alert tcp any any -> $HOME_NET any (
        msg:"Possible SYN Flood";  flags: S;  flow: stateless;
        threshold: type threshold, track by_rule, count 6000, seconds 1;
        sid:1000003;  rev:2;
)
```

Combined DoS Attacks

Ruleset Configuration

Above the threshold:

- Separate detection per attack
- Same individual ruleset

Below the threshold:

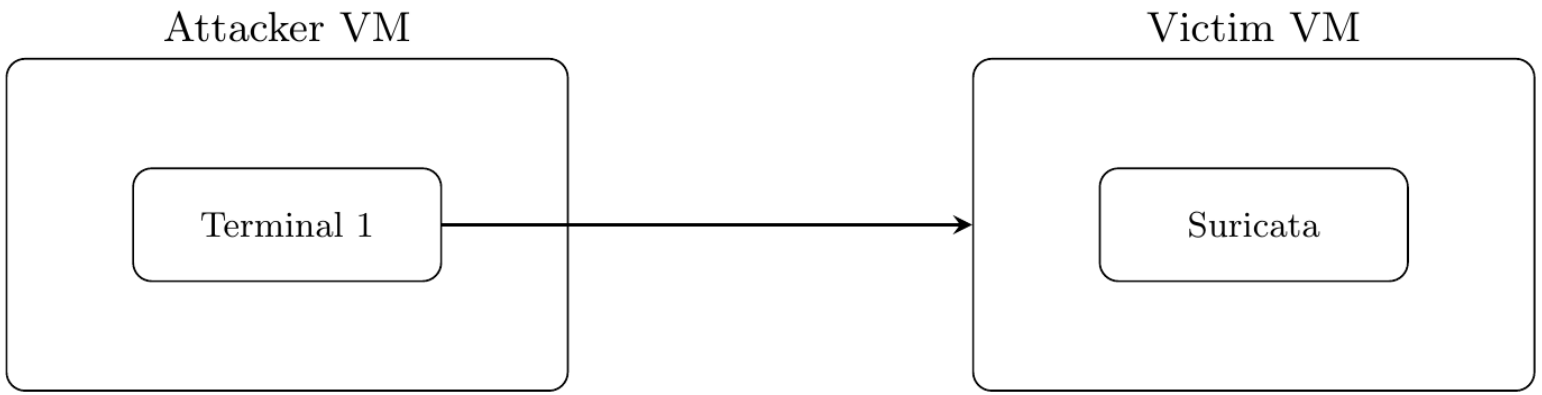
- Test detection by existing rules
- Test impact on victim CPU

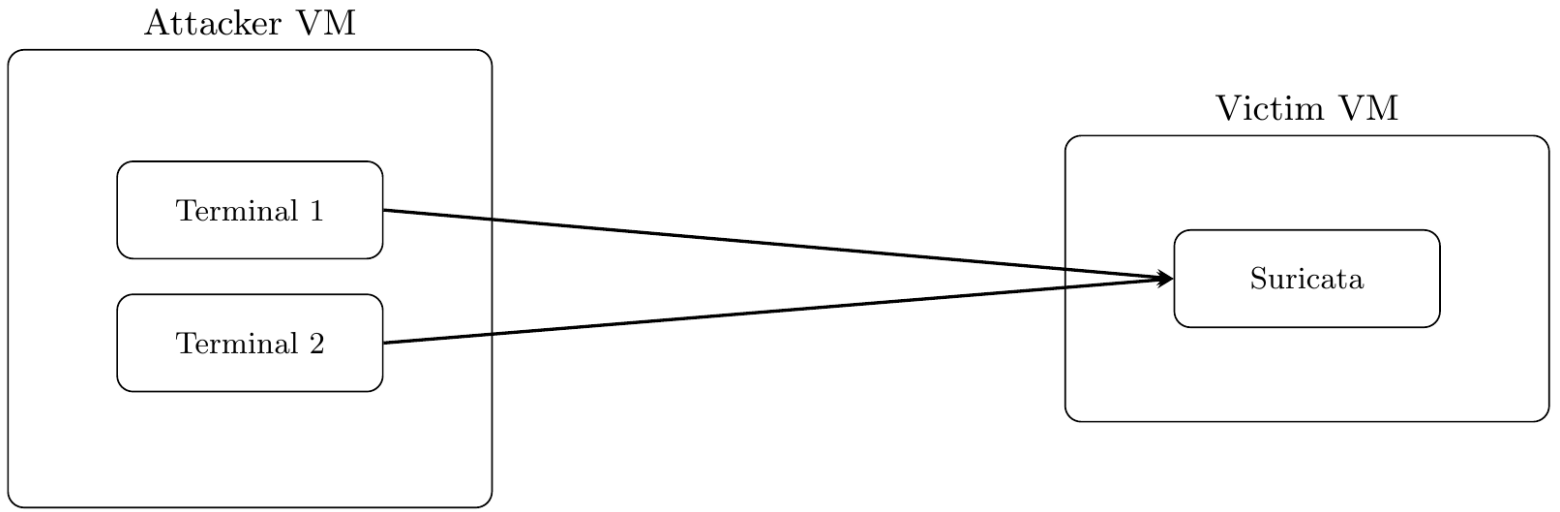
Attack Scenarios

Attack Scenarios

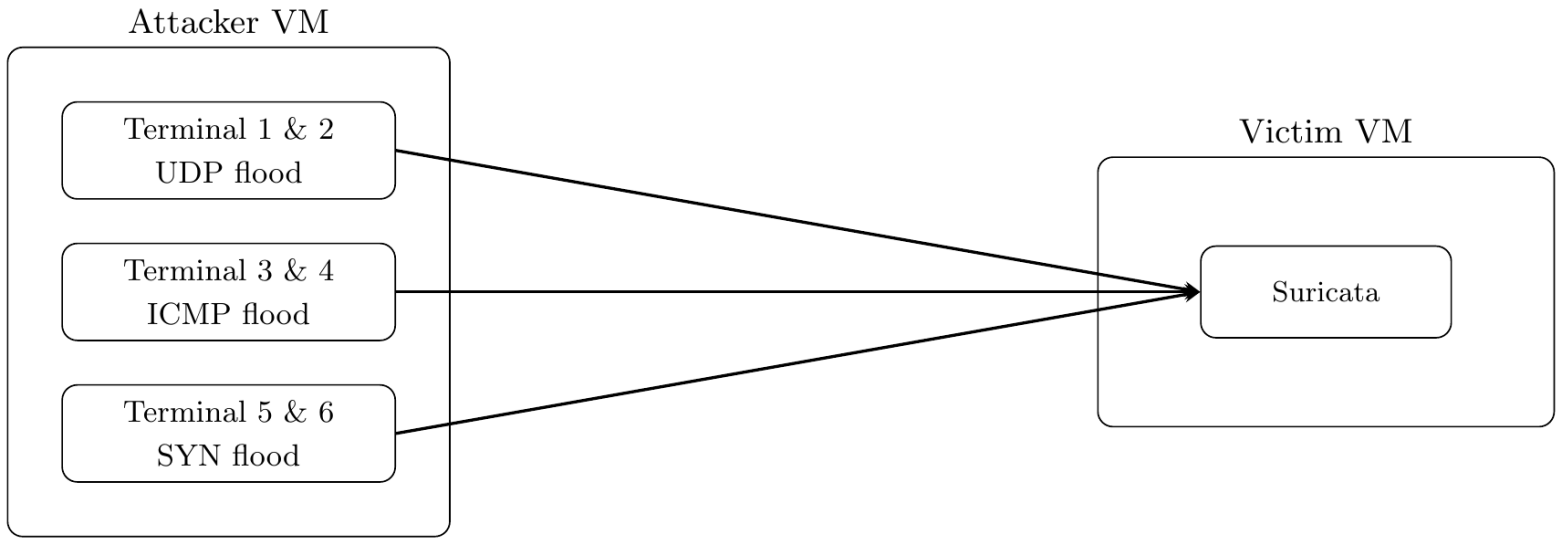
- **Scenario 1:** Individual DoS attacks
- **Scenario 2:** Combined distinct DoS attacks
- hping3 -a <spoofed_ip> --<proto> --flood <victim_ip>

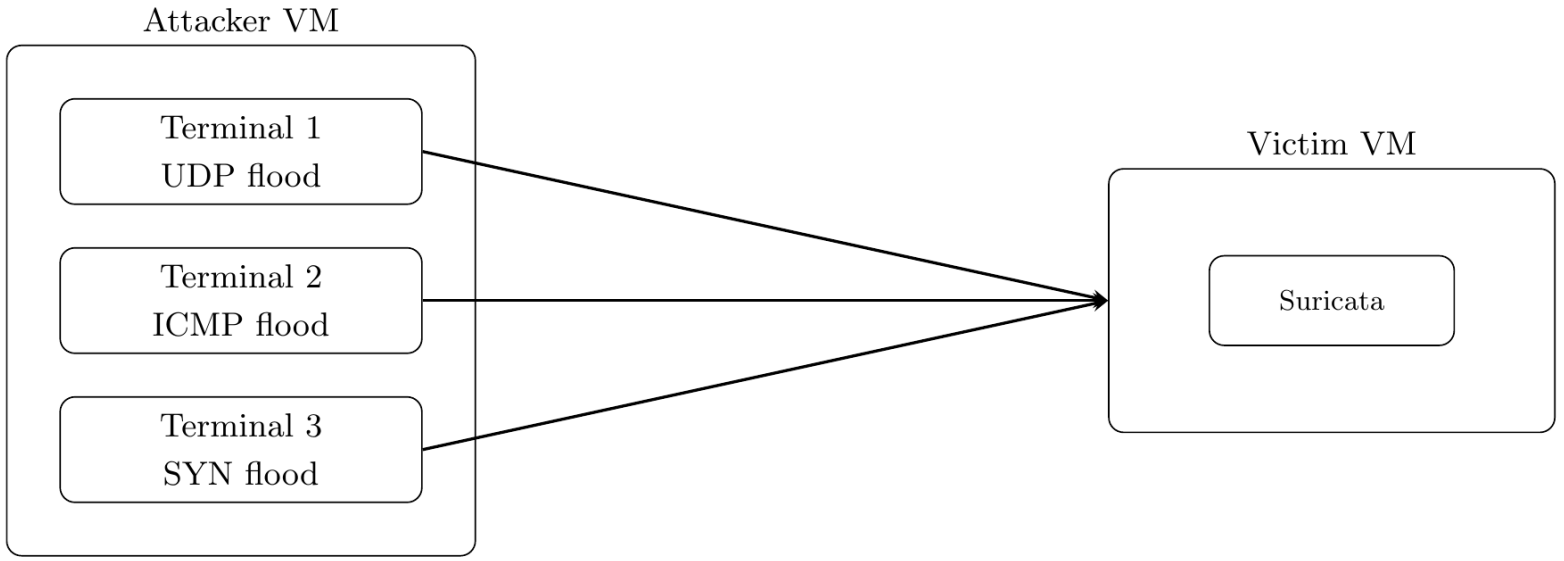
Scenario 1


Attacker VM
Terminal 1
Victim VM
Suricata


Attacker VM
Terminal 1
Terminal 2
Victim VM
Suricata

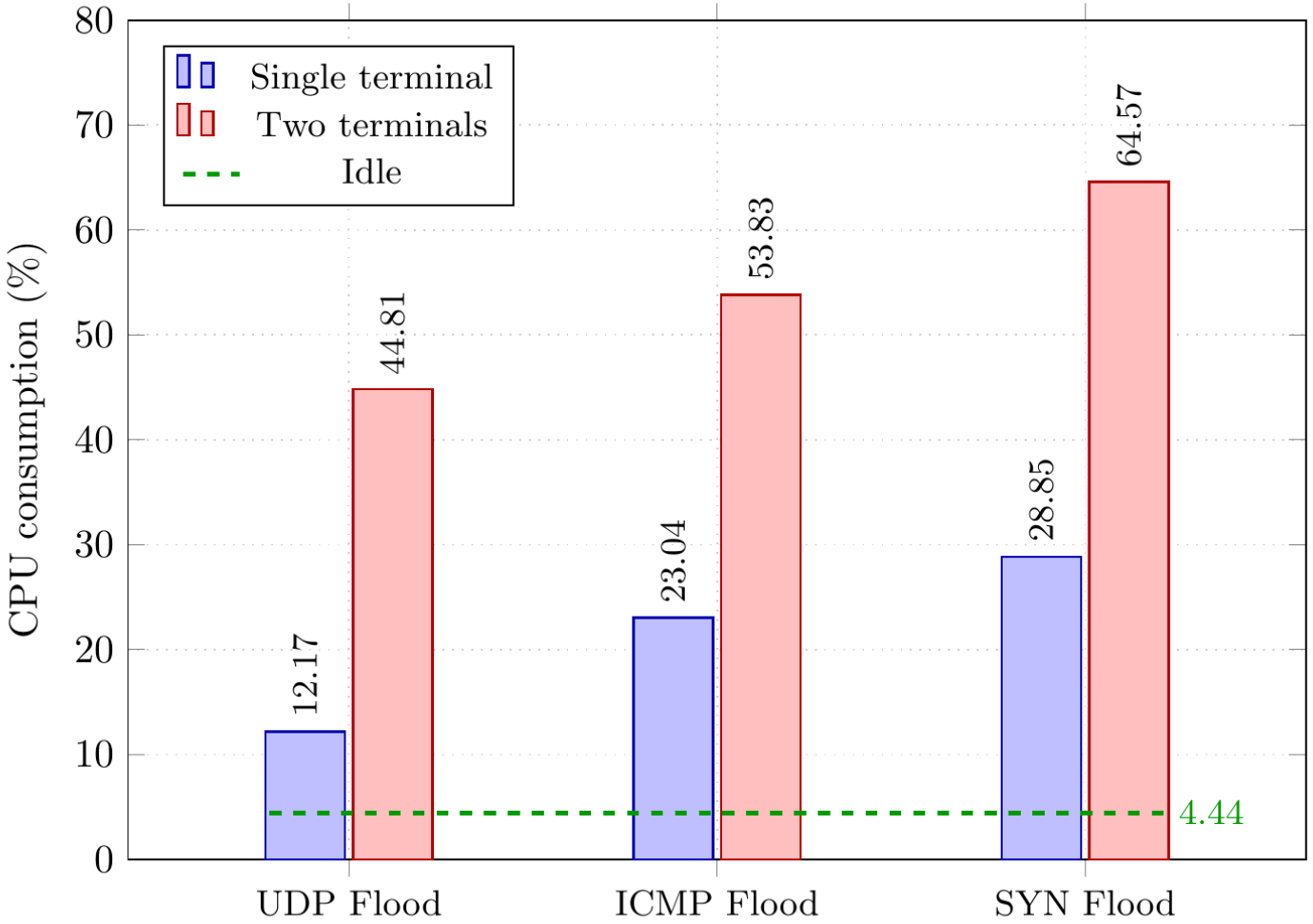
Scenario 2


Attacker VM
Terminal 1 & 2
UDP flood
Terminal 3 & 4
ICMP flood
Terminal 5 & 6
SYN flood
Victim VM
Suricata

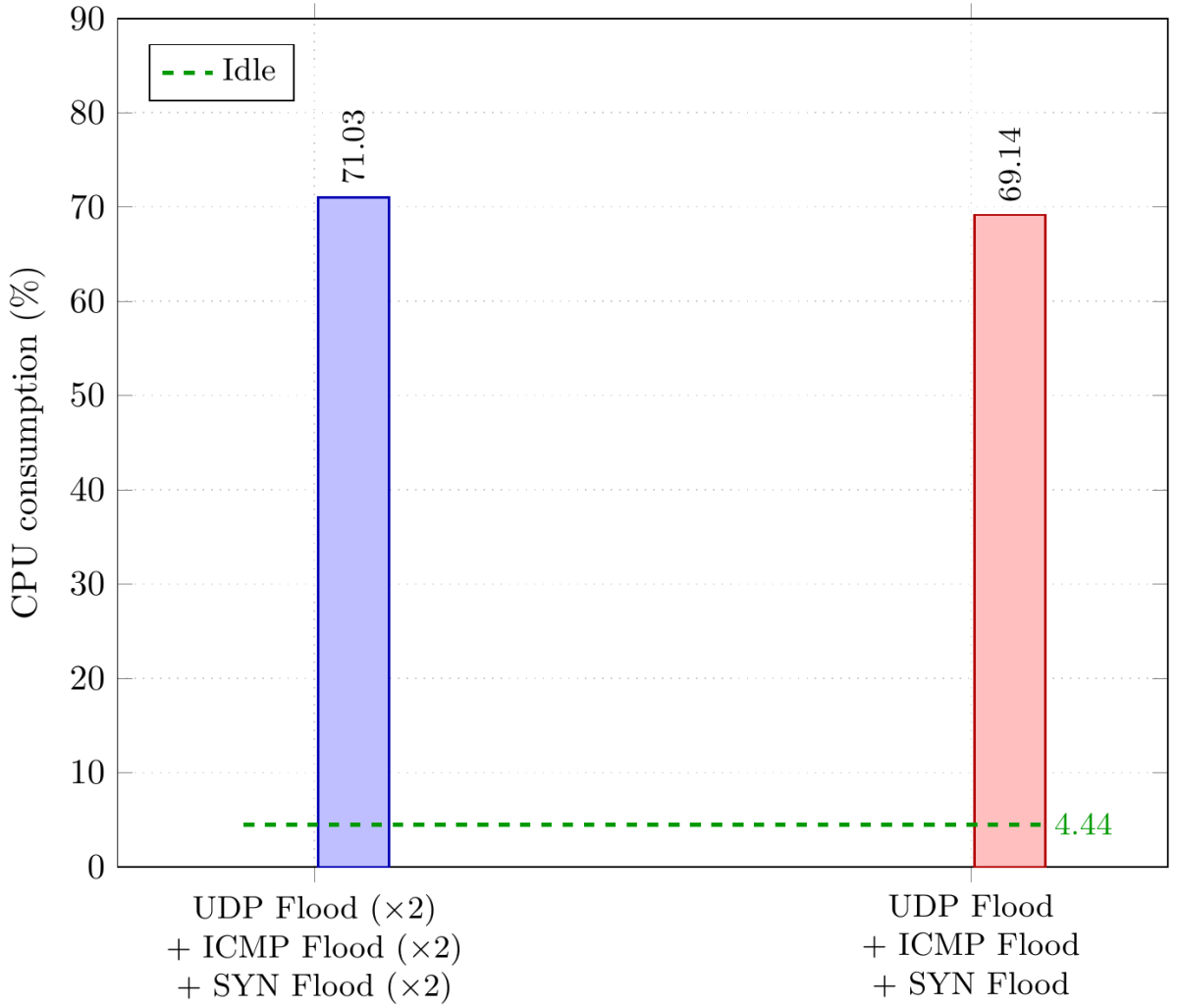

Attacker VM
Terminal 1
UDP flood
Terminal 2
ICMP flood
Terminal 3
SYN flood
Victim VM
Suricata

Results

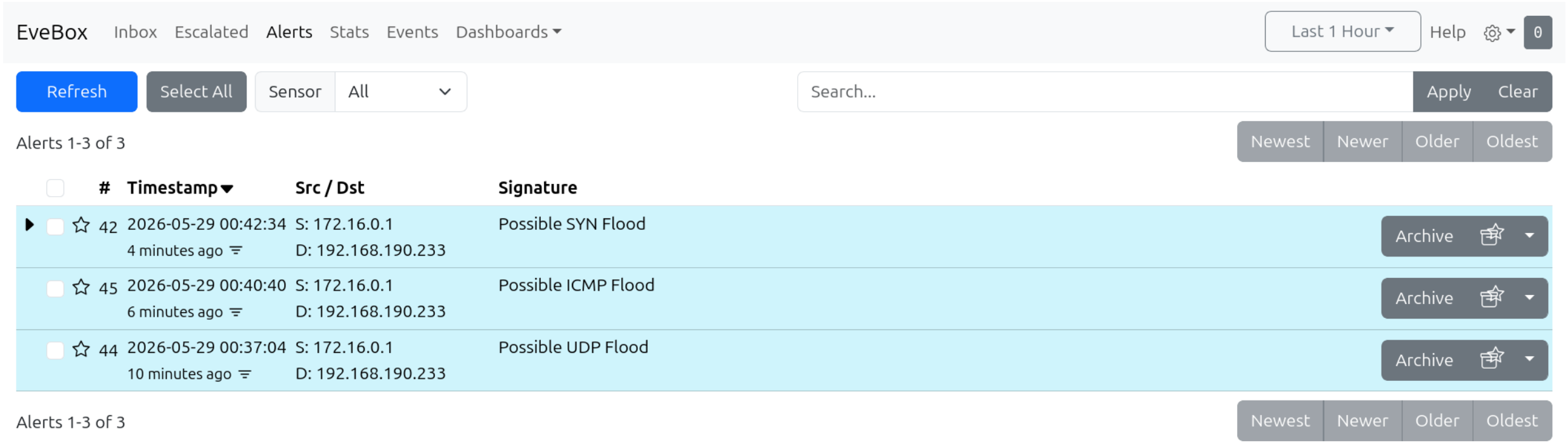
Results (1/3)


Single terminal
Two terminals
Idle
CPU consumption (%)
0
10
20
30
40
50
60
70
80
12.17
44.81
23.04
53.83
28.85
64.57
4.44
UDP Flood
ICMP Flood
SYN Flood

Results (2/3)


Idle
71.03
69.14
4.44
CPU consumption (%)
0
10
20
30
40
50
60
70
80
90
UDP Flood (×2)
+ ICMP Flood (×2)
+ SYN Flood (×2)
UDP Flood
+ ICMP Flood
+ SYN Flood

Results (3/3)


EveBox
Inbox
Escalated
Alerts
Stats
Events
Dashboards
Last 1 Hour
Help
0
Refresh
Select All
Sensor
All
Search...
Apply
Clear
Alerts 1-3 of 3
Newest
Newer
Older
Oldest
Timestamp
Src / Dst
Signature
42 2026-05-29 00:42:34
4 minutes ago
S: 172.16.0.1
D: 192.168.190.233
Possible SYN Flood
Archive
45 2026-05-29 00:40:40
6 minutes ago
S: 172.16.0.1
D: 192.168.190.233
Possible ICMP Flood
Archive
44 2026-05-29 00:37:04
10 minutes ago
S: 172.16.0.1
D: 192.168.190.233
Possible UDP Flood
Archive
Alerts 1-3 of 3
Newest
Newer
Older
Oldest

Recommendations & Conclusion

Investigation

- Global rule using ip as protocol
- Lua scripting
- xbits keyword

Recommendations

- Security Information and Event Management (SIEM)
- Anomaly-Based IDS

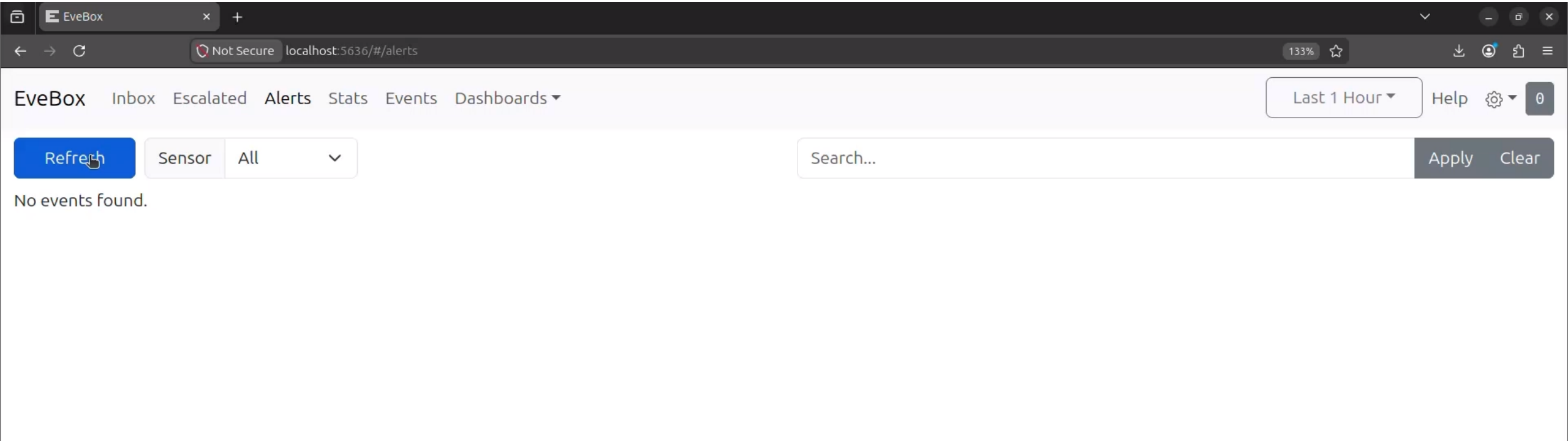
Université Saint-Joseph de Beyrouth
Faculté d'ingénierie
Institut national des télécommunications et de l'informatique

Conclusion

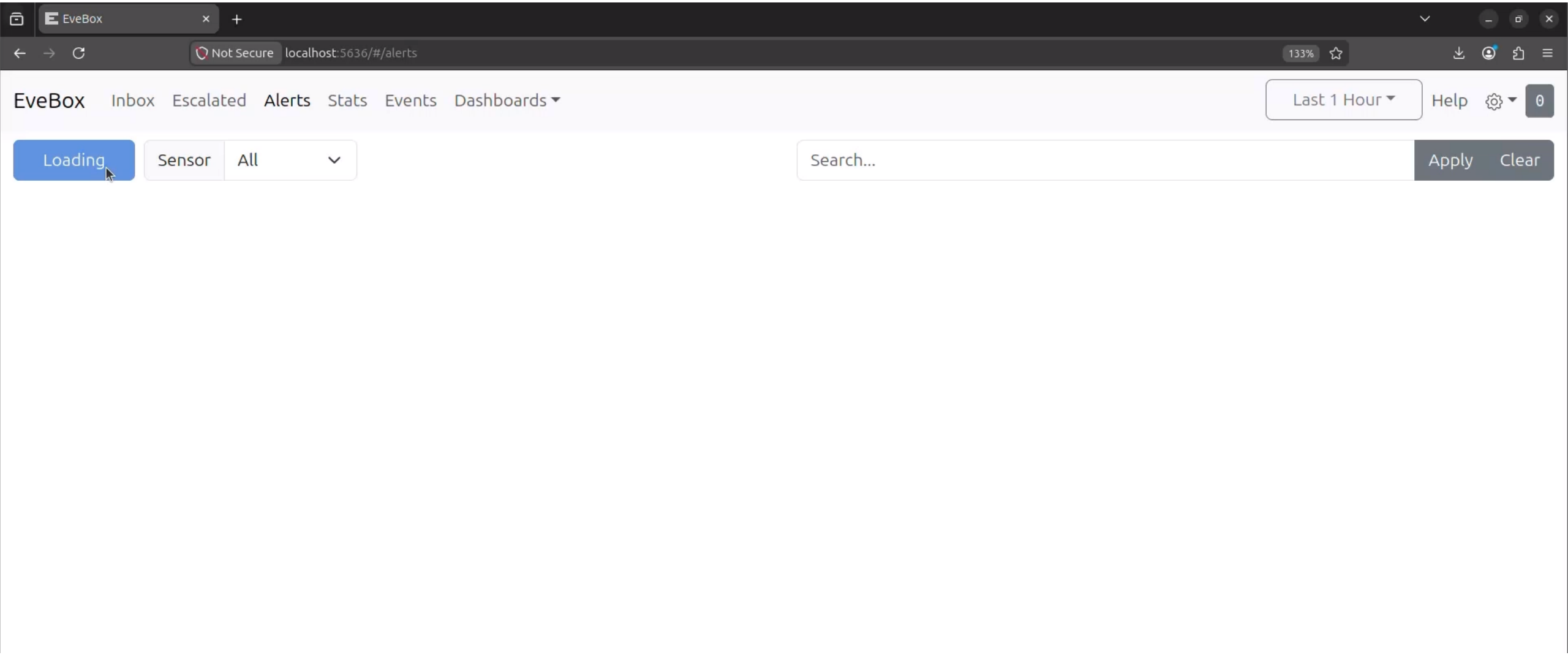
- VMware testbed (Kali attacker, Ubuntu victim)
- UDP, ICMP, SYN floods (single + combined)
- High victim CPU consumption
- Attacks detection for ≥6000 pps
- Low-rate combined attacks missed => limited multi-vector correlation

Demo

Scenario 1


EveBox
Not Secure
localhost:5636/#/alerts
133%
EveBox
Inbox
Escalated
Alerts
Stats
Events
Dashboards
Last 1 Hour
Help
0
Refresh
Sensor
All
Search...
Apply
Clear
No events found.

Scenario 2


EveBox
Not Secure
localhost:5636/#/alerts
133%
EveBox
Inbox
Escalated
Alerts
Stats
Events
Dashboards
Last 1 Hour
Help
0
Loading
Sensor
All
Search...
Apply
Clear