



DIPARTIMENTO  
DI INGEGNERIA  
DELL'INFORMAZIONE

# MSN Project - Group 8

Cosuti Luca - ID. 2057061

De Faveri Francesco L. - ID. 2057069

26/05/2023

# List of Contents

Project Requirements

Network Configuration

Attacks

Defences

## Project Requirements

---

# Network Requirements

## Network Requirements:

- 5 VyOS Routers.
- Network Range  
192.168.220.0/24

## Minimum Attacks:

- 2 Reconnaissance.
- 3 Denial of Service.
- 1 DNS Attack.

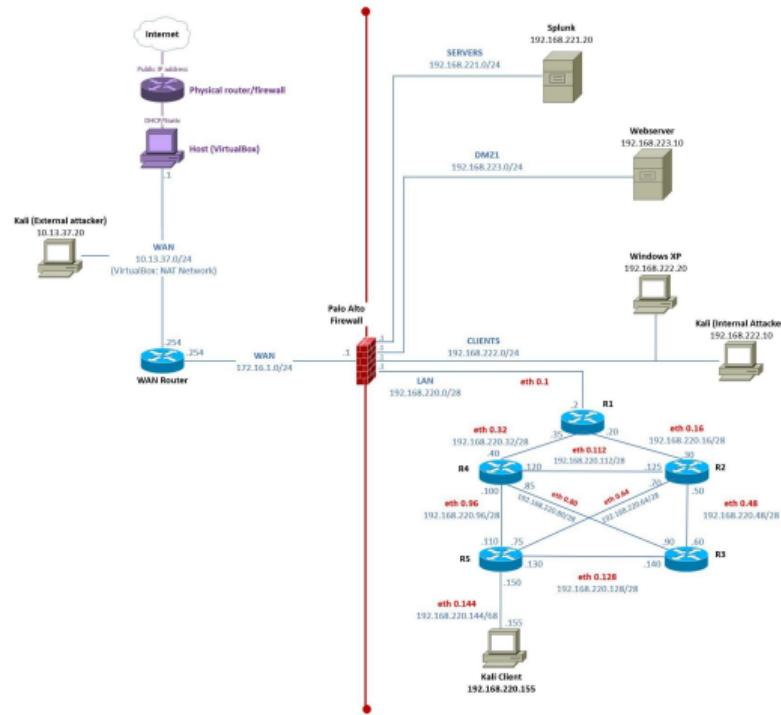
## Minimum Protections:

- Palo Alto NG Firewall.
- SIEM Splunk.
- Splunk MLTK.
- Webserver.

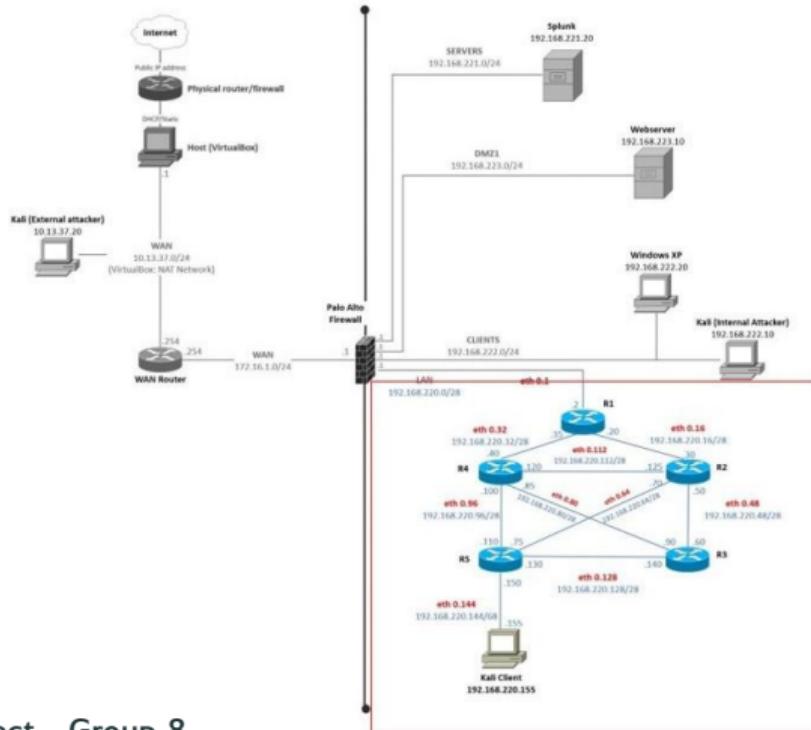
## Network Configuration

---

# Network Topology

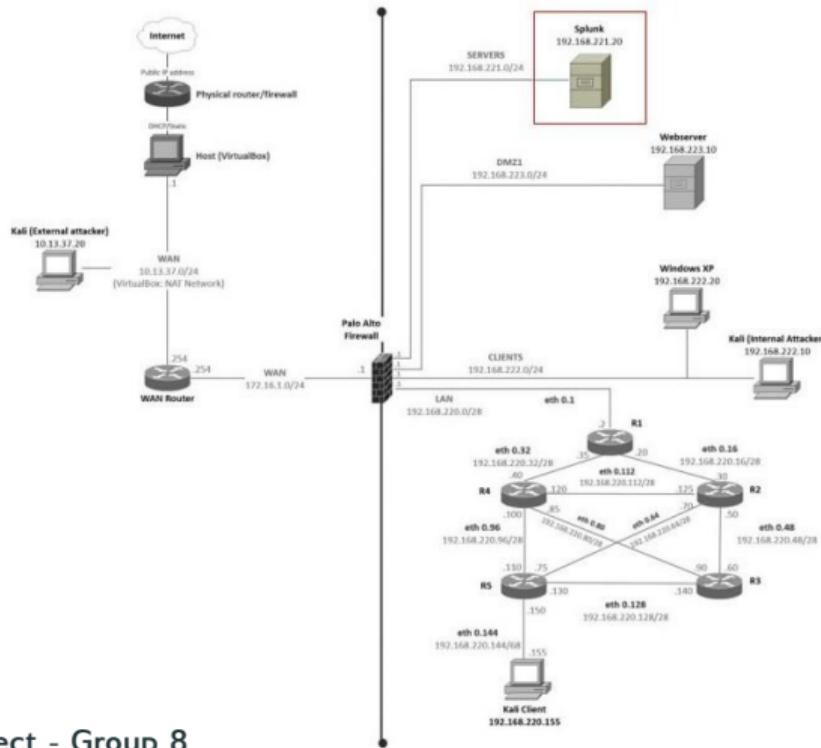


# Network Segmentation - LAN Network



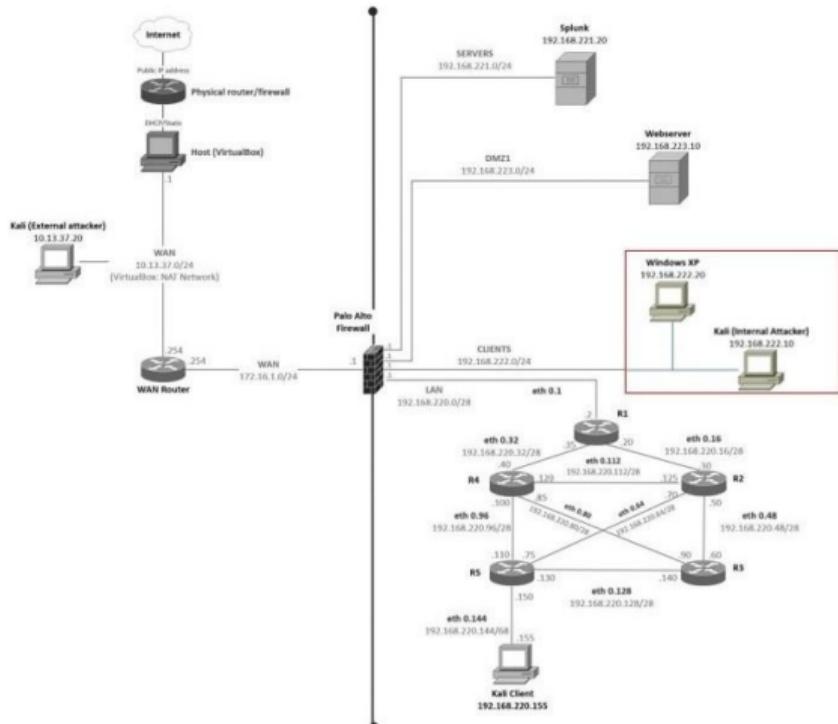
- 192.168.220.0/24;
- 5 Routers and 1 Client;
- **Can** initiate connections with any network

# Network Segmentation - SERVERS Network



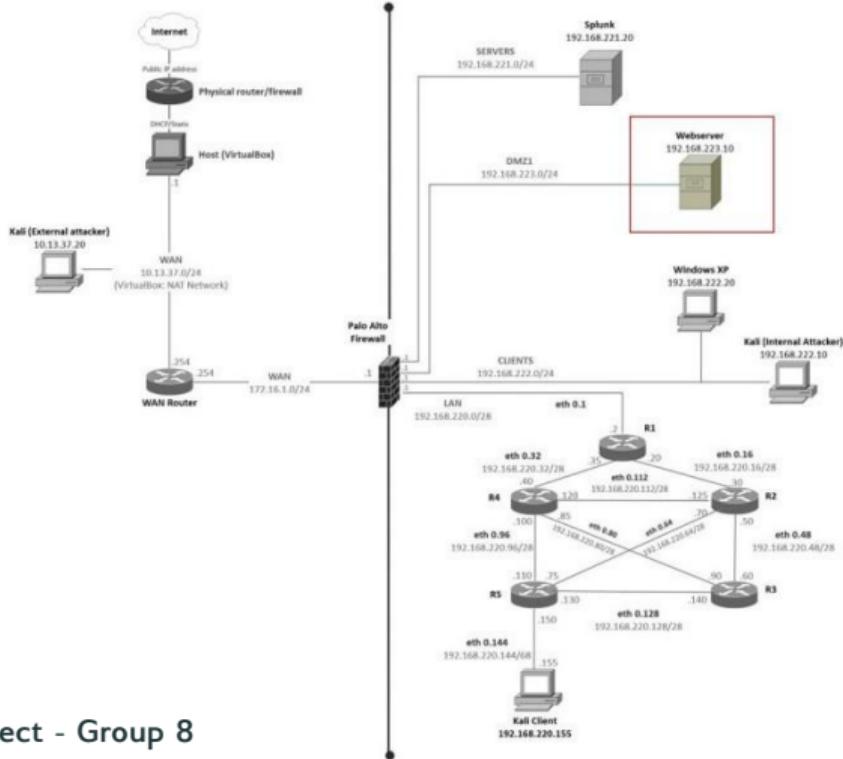
- 192.168.221.0/24
- Splunk Service
- Gets accessed by the CLIENTS network

# Network Segmentation - CLIENTS Network



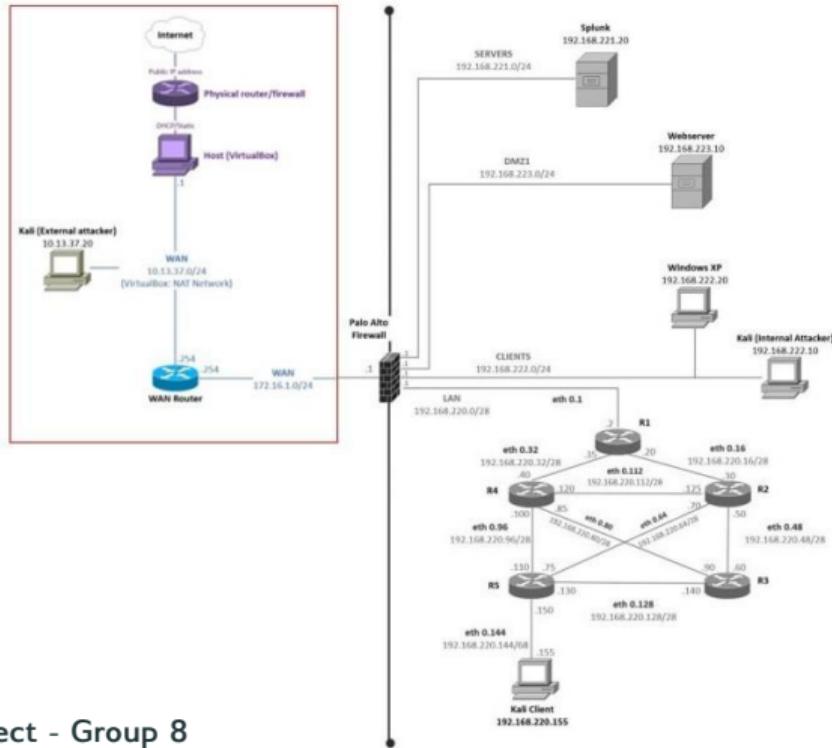
- 192.168.222.0/24
- Kali Internal Attacker & Windows XP
- CAN initiate connections with any network

# Network Segmentation - DMZ Network



- 192.168.223.0/24
- Vulnerable Webserver
- Can be accessed from anywhere, including the WAN segment

# Network Segmentation - WAN Network



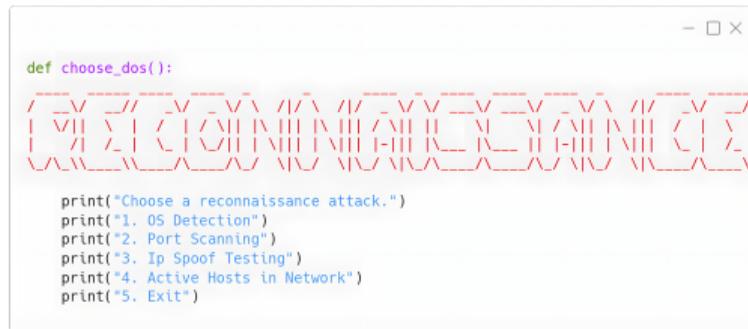
- 10.13.37.0/24
- Kali External Attacker & Internet
- Can access ONLY the DMZ

## Attacks

---

# Reconnaissance

- OS Detection
- Port Scanning
- Ip Spoof Testing
- Active Hosts in Network



```
def choose_dos():
    print("Choose a reconnaissance attack.")
    print("1. OS Detection")
    print("2. Port Scanning")
    print("3. Ip Spoof Testing")
    print("4. Active Hosts in Network")
    print("5. Exit")
```

# LIVE DEMO

# Denial of Service

- Syn Flood
- Spoofed Syn Flood
- ICMP Flood
- Spoofed ICMP Flood
- Spoofed UDP Flood
- Ping of Death

```
- □ ×  
  
def choose_dos():  
  
    print("Choose a denial of service attack.")  
    print("1. SYN Flood")  
    print("2. Spoofed SYN Flood")  
    print("3. ICMP Flood")  
    print("4. Spoofed ICMP Flood")  
    print("5. Spoofed UDP Flood")  
    print("6. Ping of Death")  
    print("7. Exit")
```

# LIVE DEMO

# Special Attacks

- DNS Amplification
- SQL Injection

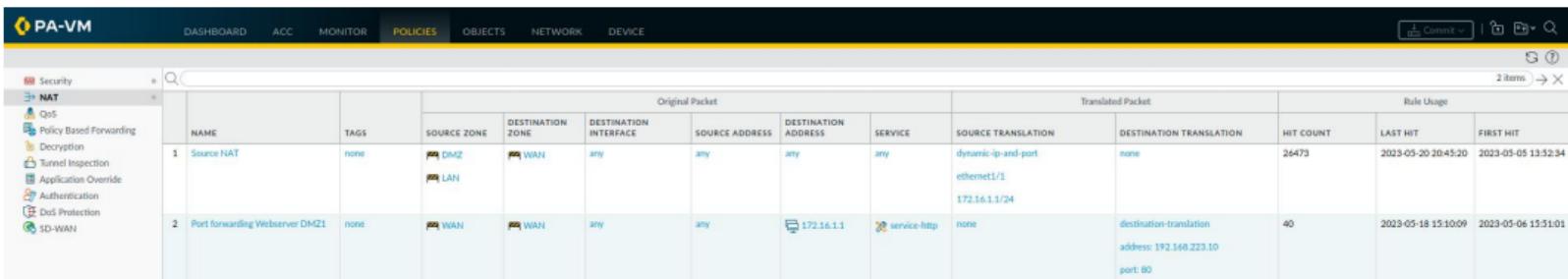
```
def choose_exploit():
    print("Choose an exploit.")
    print("1. DNS Amplification Attack")
    print("2. SQL Injection")
```

# LIVE DEMO

## Defences

---

# Palo Alto - NAT and Port Forwarding



The screenshot shows the Palo Alto VM interface with the 'Policies' tab selected. On the left, a sidebar lists various security features: Security, NAT, QoS, Policy-Based Forwarding, Decryption, Tunnel Inspection, Application Overlay, Authentication, DoS Protection, and SD-WAN. The 'NAT' section is expanded, showing two rules:

NAME	TAGS	Original Packet						Translated Packet		Rule Usage		
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT COUNT	LAST HIT	FIRST HIT
1 Source NAT	none	DMZ	WAN	any	any	any	any	dynamic-ip-and-port	none	26473	2023-05-20 20:45:20	2023-05-05 13:32:34
2 Port forwarding Webserver DMZ1	none	WAN	WAN	any	any	172.16.1.1	service-http	none	destination-translation address: 192.168.223.10 port: 80	40	2023-05-18 15:10:09	2023-05-06 15:51:01

Figure 2: Network Address Translation.

# Palo Alto - Flood Prevention

The screenshot shows the Palo Alto Network Management UI. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES (which is selected), OBJECTS, NETWORK, and DEVICE. On the left, a sidebar lists various policy categories: Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection (selected), and SD-WAN. The main content area displays a table of rules. The table has columns for NAME, TAGS, Source (Zone/Interface, Address, User), Destination (Zone/Interface, Address), SERVICE, ACTION, Protection (Aggregate, Classified), SCHEDULE, LOG FORWARDING, HIT COUNT, and LAST HIT. There is one rule listed:

NAME	TAGS	Source			Destination		SERVICE	ACTION	Protection		SCHEDULE	LOG FORWARDING	HIT COUNT	LAST HIT
		ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS			AGGREGATE	CLASSIFIED				
1 DoS Protection	none	LAN	any	any	DMZ	any	any	deny	DoS Protection	none	none	none	67666	2023-05-25 13:55:2

Figure 3: Rule for Flood Prevention.

## SIEM Splunk - Query

- □ ×

```
sourcetype = "stream:icmp" type_string = "Echo"  
  
| bin _time span = 10s  
| stats count AS Echo_Requests BY _time, src_ip, dest_ip  
| where Echo_Requests > 40  
| rename src_ip AS "Attacker (src_ip)", dest_ip AS "Victim (dest_ip)"
```

**Figure 4:** Query for ICMP Flood Detection via SIEM Splunk.

# SIEM Splunk - Detection

The screenshot shows the Splunk Enterprise web interface. The top navigation bar includes 'splunk>enterprise', 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', 'Dashboards', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. A search bar at the top right contains the query 'Search & Reporting'.

The main search area has a title 'ICMP Flood Attempt' and displays the following SPL query:

```
1 sourcetype="stream:icmp" type_string="Echo"
2 | bin _time span=10s
3 | stats count AS Echo_Requests BY _time, src_ip, dest_ip
4 | where Echo_Requests > 40
5 | rename src_ip AS "Attacker (src_ip)", dest_ip AS "Victim (dest_ip)"
```

Below the query, it says '22,496 of 33,835 events matched' and 'No Event Sampling'.

The interface includes tabs for 'Events (22,496)', 'Patterns', 'Statistics (97)', and 'Visualization'. The 'Statistics' tab is selected, showing a table with columns: '\_time', 'Attacker (src\_ip)', 'Victim (dest\_ip)', and 'Echo\_Requests'. The table lists 14 rows of data, each corresponding to a timestamp and two IP addresses. The 'Echo\_Requests' column shows values such as 65, 280, 200, 600, etc.

_time	Attacker (src_ip)	Victim (dest_ip)	Echo_Requests
2023-05-22 11:36:10	192.168.222.229	192.168.223.10	65
2023-05-22 11:36:20	192.168.222.10	192.168.223.10	280
2023-05-22 11:36:20	192.168.222.100	192.168.223.10	200
2023-05-22 11:36:20	192.168.222.102	192.168.223.10	600
2023-05-22 11:36:20	192.168.222.107	192.168.223.10	200
2023-05-22 11:36:20	192.168.222.108	192.168.223.10	200
2023-05-22 11:36:20	192.168.222.110	192.168.223.10	200
2023-05-22 11:36:20	192.168.222.111	192.168.223.10	200
2023-05-22 11:36:20	192.168.222.116	192.168.223.10	200
2023-05-22 11:36:20	192.168.222.123	192.168.223.10	187
2023-05-22 11:36:20	192.168.222.125	192.168.223.10	200
2023-05-22 11:36:20	192.168.222.128	192.168.223.10	200

Figure 5: ICMP Flood Detection via SIEM Splunk.

## Splunk MLTK - Dataset definition

```
sourcetype = "stream:icmp"

| bin _time span = 5s
| stats count AS filtered_events BY _time, dst_ip, src_ip
| eval attack = if(filtered_events > 150, "Yes", "No")
| table src_ip, dst_ip, _time, filtered_events, attack
```

Figure 6: Splunk query to LOG an ICMP Flood - Dataset Definition.

# Splunk MLTK - Smart Prediction Results

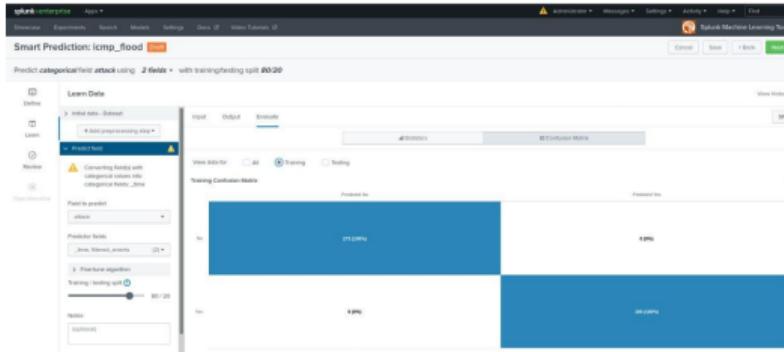


Figure 7: Training Confusion Matrix.

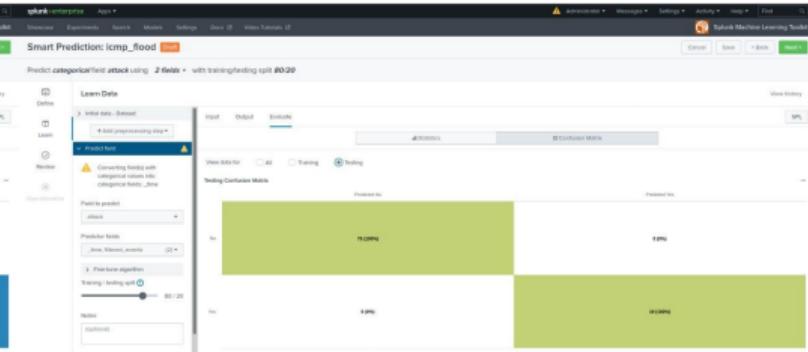


Figure 8: Testing Confusion Matrix.

# Splunk MLTK - Smart Outliers Results

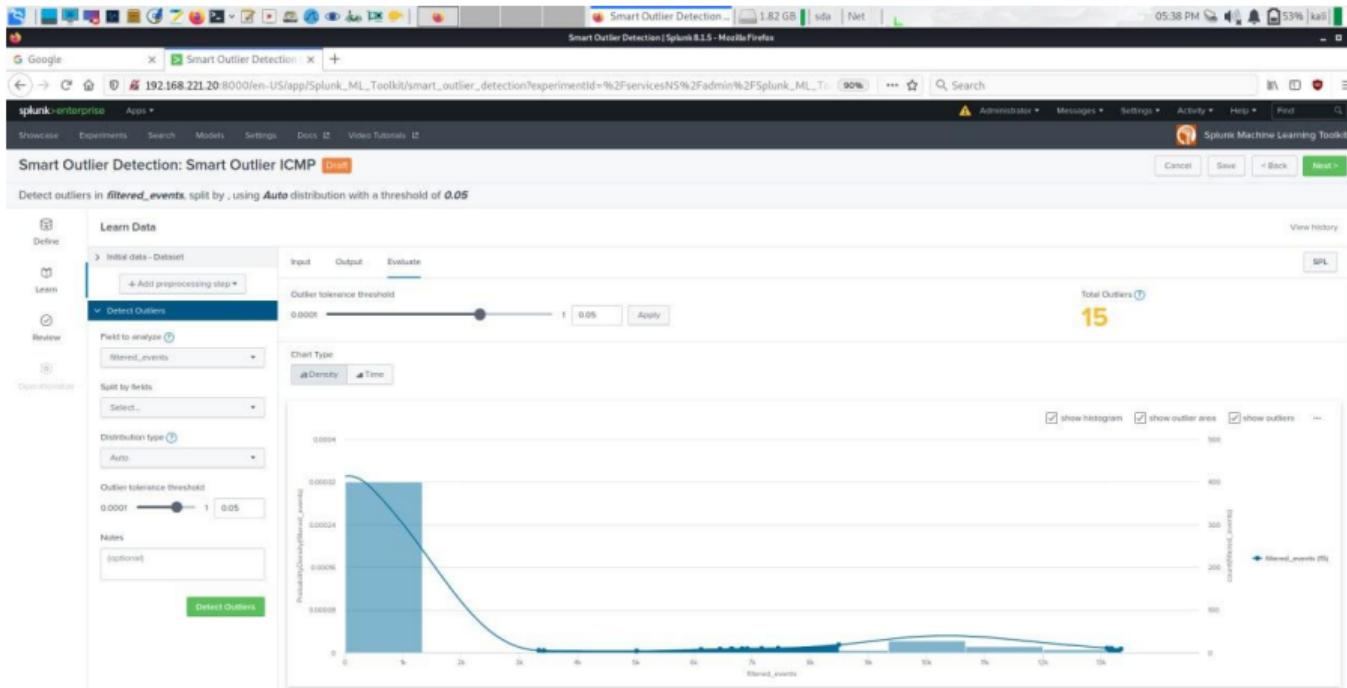


Figure 9: Time results.



DIPARTIMENTO  
DI INGEGNERIA  
DELL'INFORMAZIONE

# Thanks for your attention!