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 Requirements

Network Requirments:

- 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

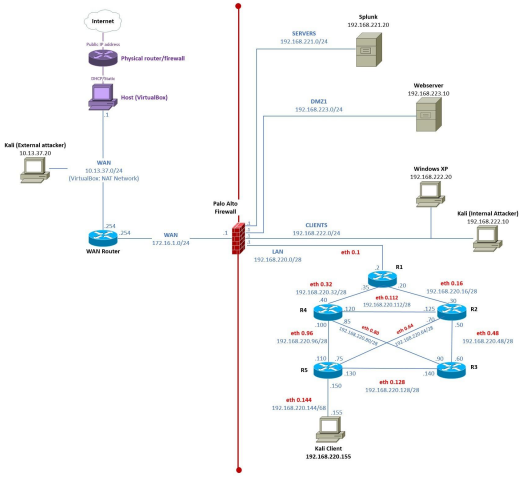
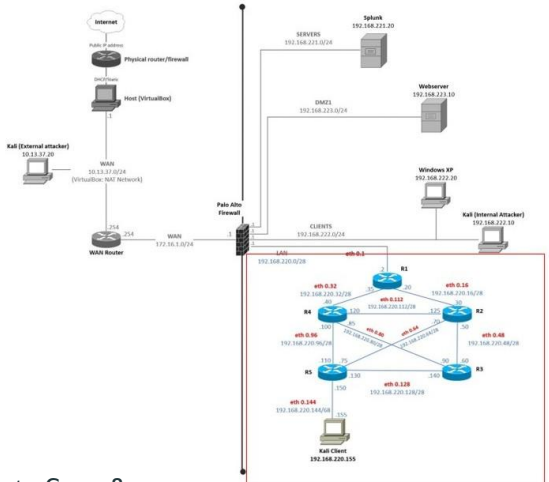


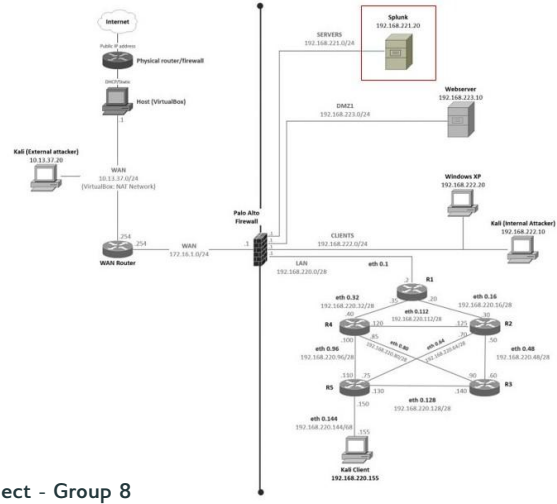
Figure 1: Infrastructure Topology.

Network Segmentation - LAN Network



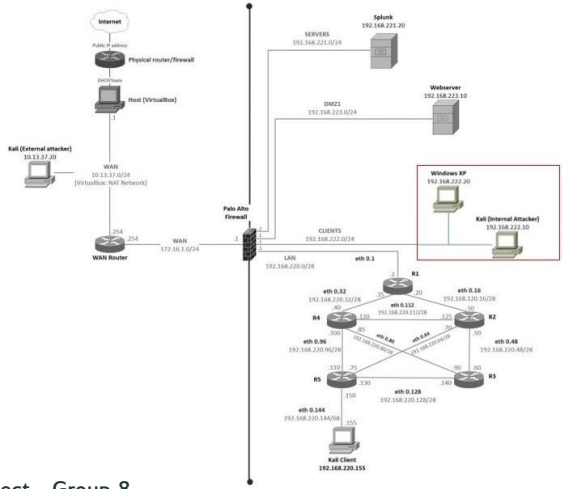
- 192.168.220.0/24;
- 5 Routers and 1 Client;
- **Can** initiate connections with any network

Network Segmentation - SERVERS Network



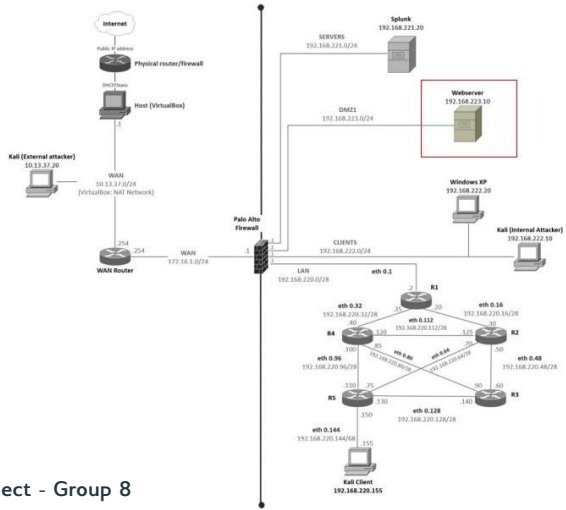
- 192.168.221.0/24
- Splunk Service
- Gets accessed by the CLIENTS network

Network Segmentation - CLIENTS Network



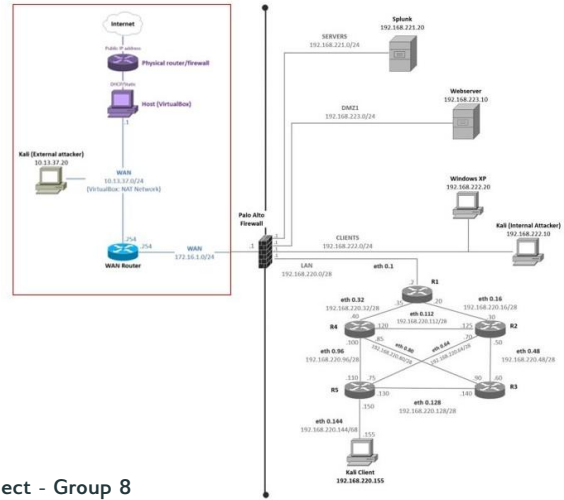
- 192.168.222.0/24
- Kali Internal Attacker & Windows XP
- CAN initiate connections with any network

Network Segmentation - DMZ Network



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

Network Segmentation - WAN Network

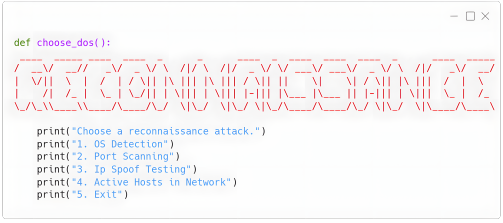


- 10.13.37.0/24
- Kali External Attacker & Internet
- Can access ONLY the DMZ

Attacks

Reconnaissance

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



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

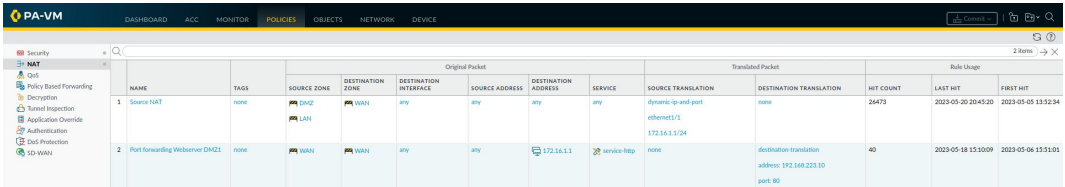


Figure 2: Network Address Translation.

Palo Alto - Flood Prevention

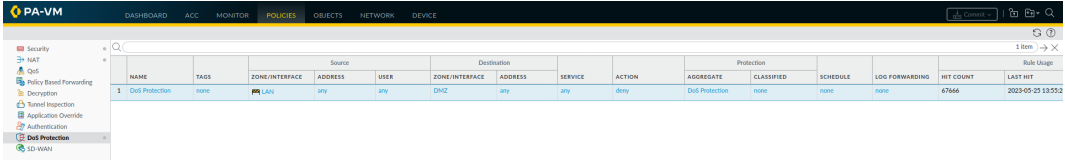


Figure 3: Rule for Flood Prevention.

```
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

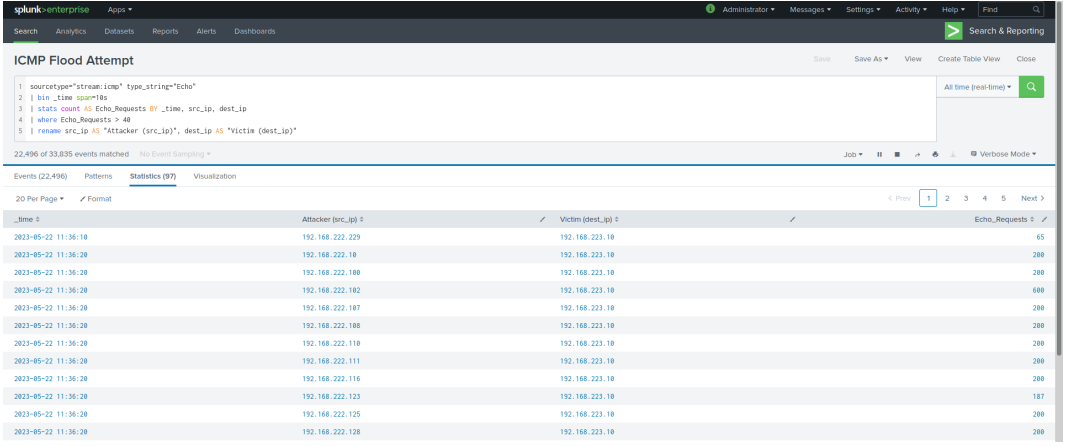


Figure 5: ICMP Flood Detection via SIEM Splunk.

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

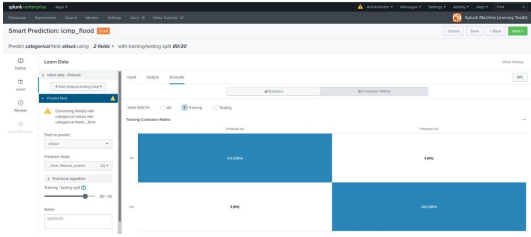


Figure 7: Training Confusion Matrix.

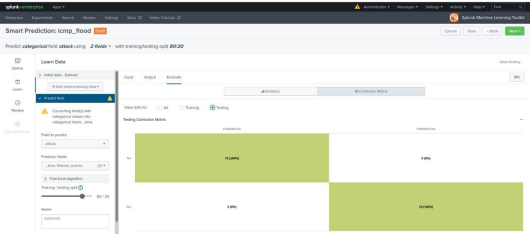


Figure 8: Testing Confusion Matrix.

Splunk MLTK - Smart Outliers Results

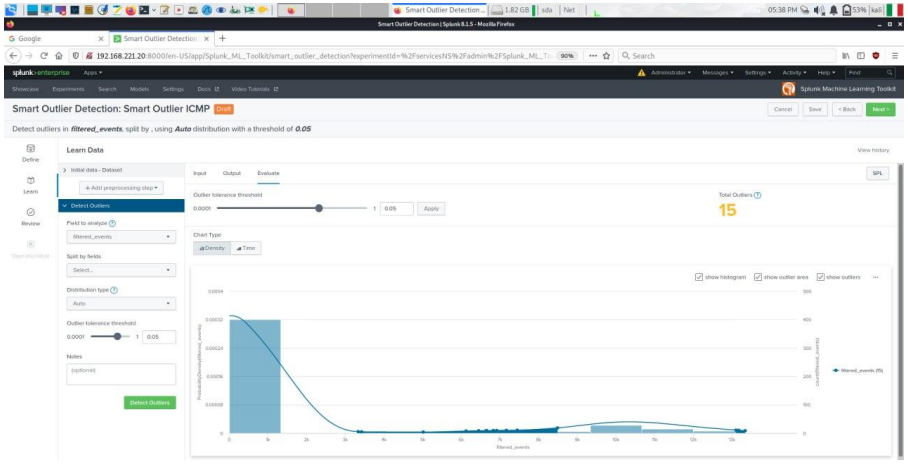


Figure 9: Time results.

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

Thanks for your attention!