Deployment of Network Security Controls

Braydan Newman - n11272031

October 12, 2024

Contents

1 Vulnerability Management . . . 2

1.1 Introduction to Vulnerability Scanning and Prioritisation . . . 2

1.2 Role of NVD in Vulnerability Scanning and Prioritisation . . . 2

1.3 Identification, Assessment and Prioritisation of Vulnerable Services . . . 3

1.4 Complementary Controls for Vulnerability Scanning and Prioritisation . 4

2 Intrusion Detection System . . . 4

2.1 Introduction to Intrusion Detection System - Snort . . . 4

2.2 Different ways to use or deploy Snort . . . 4

2.3 Logging and Monitoring Snort Alerts . . . 7

2.4 Detecting Risks and Attacks using Snort . . . 7

2.5 Complementary Controls for IDS . . . 12

3 Proxies . . . 12

3.1 Main purposes of Proxy . . . 12

3.2 Remaining Risk . . . 15

3.3 Complementary Controls to Proxy . . . 15

4 Security Information and Event Management (SIEM) . . . 16

4.1 Introduction to SIEM . . . 16

4.2 Wazuh as SIEM . . . 16

4.3 Enhancing network security with threat intelligence . . . 18

4.4 Identifying network attack techniques with MITRE ATT&CK . . . 19

4.5 Complementary Control to SIEM and Threat Intel . . . 24

1 Vulnerability Management

1.1 Introduction to Vulnerability Scanning and Prioritisation

Vulnerability scanning is used to automatically identify weaknesses in an organization's systems, networks, or applications by detecting outdated software, misconfigurations, or known vulnerabilities. The purpose is to provide a clear overview of potential security risks that could be exploited by attackers, enabling timely fixes.

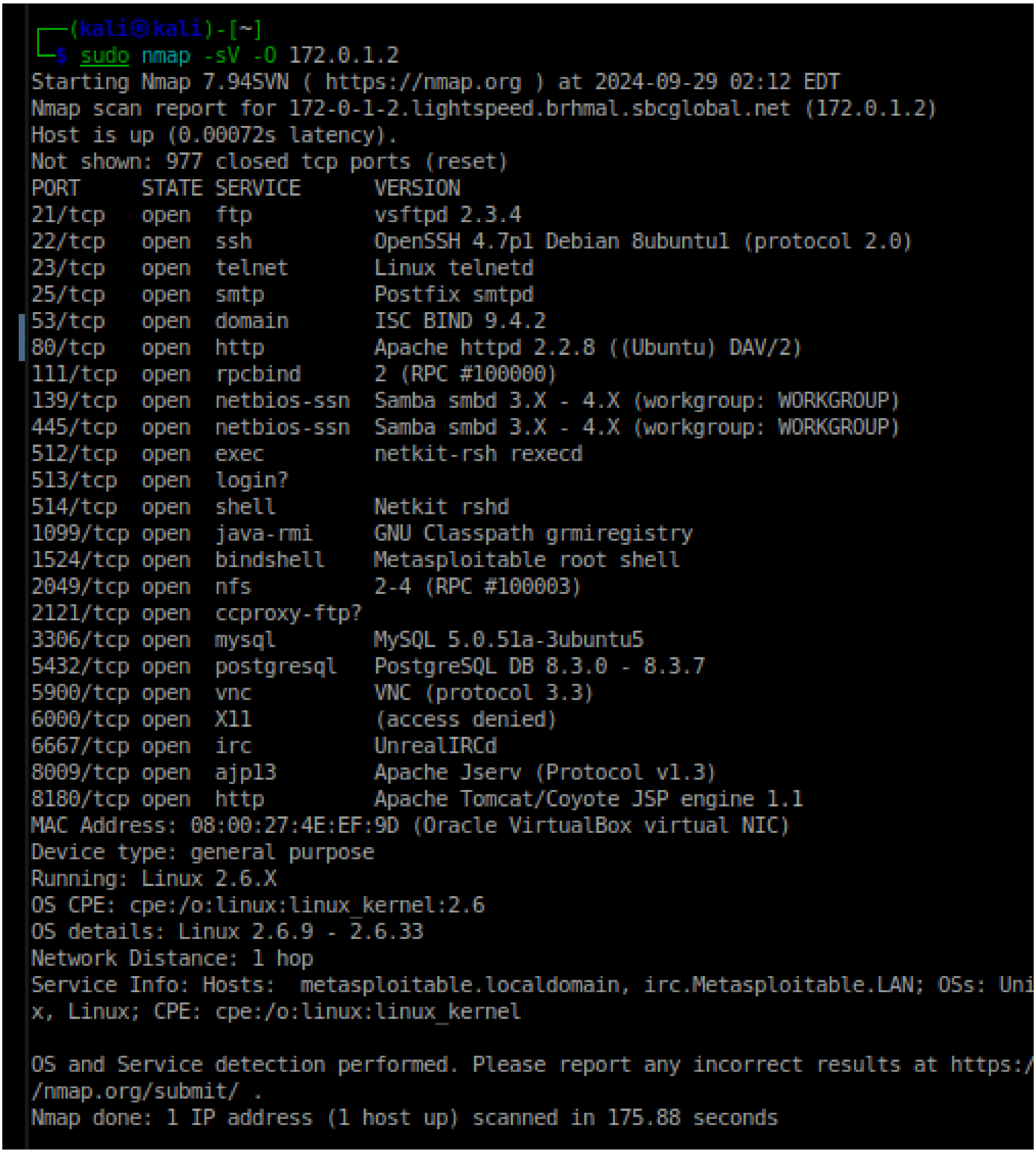
Vulnerability prioritisation is crucial because not all vulnerabilities pose the same level of threat. By ranking them based on severity, impact, and likelihood of exploitation, organizations can focus on addressing the most critical issues first, ensuring that resources are used effectively to mitigate high-risk vulnerabilities.

In the broader scope of network security, vulnerability scanning and prioritisation are essential components of proactive defense. They complement other security measures like firewalls, intrusion detection, and patch management by continuously assessing and addressing risks, helping to maintain a resilient security posture over time.

1.2 Role of NVD in Vulnerability Scanning and Prioritisation

The National Vulnerability Database (NVD) is a comprehensive repository of publicly disclosed cybersecurity vulnerabilities, maintained by the U.S. National Institute of Standards and Technology (NIST). It provides standardized data, including severity scores (using CVSS), descriptions, and impact ratings for vulnerabilities. The NVD is significant in vulnerability management because it helps organizations identify and assess vulnerabilities in their systems by referencing a trusted, centralized source. It also supports automation by integrating with various security tools, enabling more efficient vulnerability detection and prioritization efforts.

1.3 Identification, Assessment and Prioritisation of Vulnerable Services



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 172.0.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-29 02:12 EDT
Nmap scan report for 172-0-1-2.lightspeed.brhmal.sbcglobal.net (172.0.1.2)
Host is up (0.00072s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:4E:EF:9D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni
x, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 175.88 seconds
```

Vulnerable service	Vulnerability ID and CWE ID	Short description	Severity (CVSS)	Associated Vector (metrics) here provide	Affected Product	Remediation action
vsftpd	CVE-2011-2523 CWE-78	Contains a backdoor which can open a shell on port 6200/tcp	9.8 CRITICAL	Network, Low complexity	Vsftpd	Update software to version above 20110703
ISC BIND	CVE-2008-0122 CWE-189	An off-by-one error that can allow for DOS and ACE	10.0 HIGH	Network, Low complexity	BIND 9	Patch Software to version 7.0-PRERELEASE, or 6-STABLE
Linux kernel	CVE-2007-6762 CWE-119	\An off-by-one error that can allow for DOS and ACE	9.8 CRITICAL	Network, Low complexity	Linux	Apply patching git commit 2a2f11c227bdf292b3a 2900ad04139d301b56ac4
MySQL	CVE-2009-4484 CWE-787	Multiple buffer overflow vulnerability's that allows for DOS and ACE	7.5 HIGH	Network, N/A	MySQL	Update to latest version of MySQL
PostgreSQL	CVE-2009-0922 CWE-399	By triggering a failure in the conversion of a localized error message one allows remote authenticated users to cause a denial of service	4.0 MEDIUM	Network, Low complexity	PostgreSQL	Patch PostgreSQL to version 8.3.7, 8.2.13, 8.1.17, 8.0.21, or 7.4.25

1.4 Complementary Controls for Vulnerability Scanning and Prioritisation

A complementary control for vulnerability scanning and prioritisation is penetration testing, where security professionals simulate real-world attacks to actively exploit vulnerabilities in a system. Unlike automated vulnerability scans, penetration testing provides deeper insight by assessing how vulnerabilities can be exploited in practice, identifying risks that might be missed or misclassified by scanning tools. This hands-on approach allows organizations to better understand the potential impact of vulnerabilities and helps prioritize fixes based on real-world exploitability, enhancing the overall risk assessment process.

2 Intrusion Detection System

2.1 Introduction to Intrusion Detection System - Snort

An Intrusion Detection System (IDS) monitors network traffic to detect suspicious activities or potential security threats, alerting administrators when unusual behavior is detected. Its primary role is to identify potential breaches and malicious activities in real-time to maintain network security.

Snort, a popular open-source IDS, functions by analyzing network traffic against predefined rules to identify known attack patterns. It features packet sniffing, protocol analysis, and real-time intrusion detection capabilities, enabling administrators to detect and respond to threats effectively.

2.2 Different ways to use or deploy Snort

Deployment methods for Snort

Network Intrusion Detection System (NIDS) In this mode, Snort inspects network traffic passively and generates alerts when it detects suspicious activities or signatures that match its rule set. It doesn't block or modify the traffic, making it ideal for monitoring.

snort.conf

```
# Specify network variables
var HOME_NET 192.168.1.0/24
var EXTERNAL_NET any

# Define the rule files
```

```
include $RULE_PATH/local.rules
include $RULE_PATH/community.rules

# Enable logging and alerting
output alert_fast: /var/log/snort/alerts.log
output unified2: filename snort.u2, limit 128

# Preprocessors for detecting various attack types
preprocessor stream5_global: track_tcp yes, track_udp yes, track_icmp no
preprocessor stream5_tcp: policy windows, detect_anomalies
preprocessor http_inspect: global iis_unicode_map unicode.map 1252
```

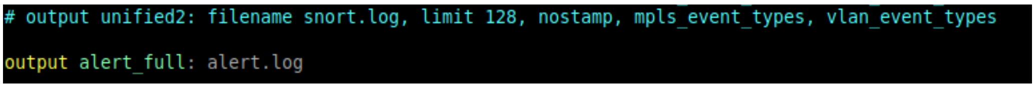
Intrusion Prevention System (IPS) In IPS mode, Snort actively blocks or modifies traffic that matches a set of rules. It can drop, reject, or alert on malicious packets to prevent the attack from succeeding.

local.rules

```
alert tcp any any -> $HOME_NET 80 (msg:"Suspicious Web Traffic";
 flow:to_server,established; content:"malicious"; sid:1000001; rev:1;)

drop tcp any any -> $HOME_NET 80 (msg:"Block Malicious Traffic";
 flow:to_server,established; content:"evil_payload"; sid:1000002; rev:1;)
```

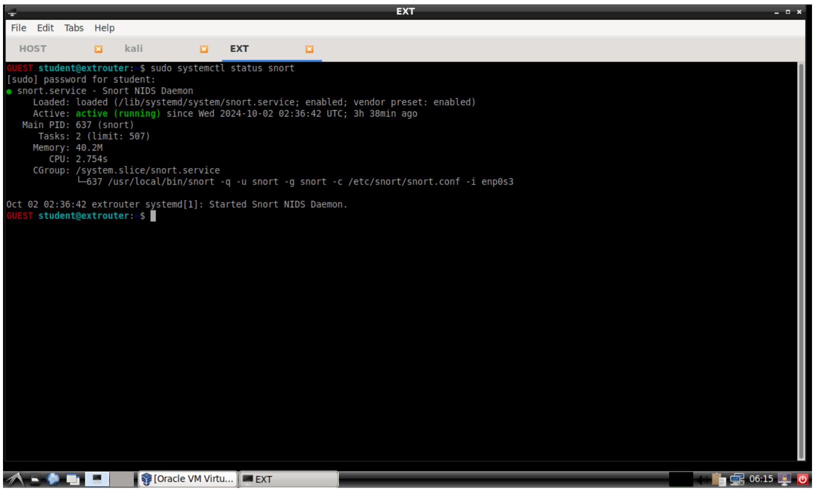
Packet Logger Snort can be used in packet logger mode to log all network traffic that passes through a specific network interface. This is useful for network forensics or deep packet inspection.

snort.conf

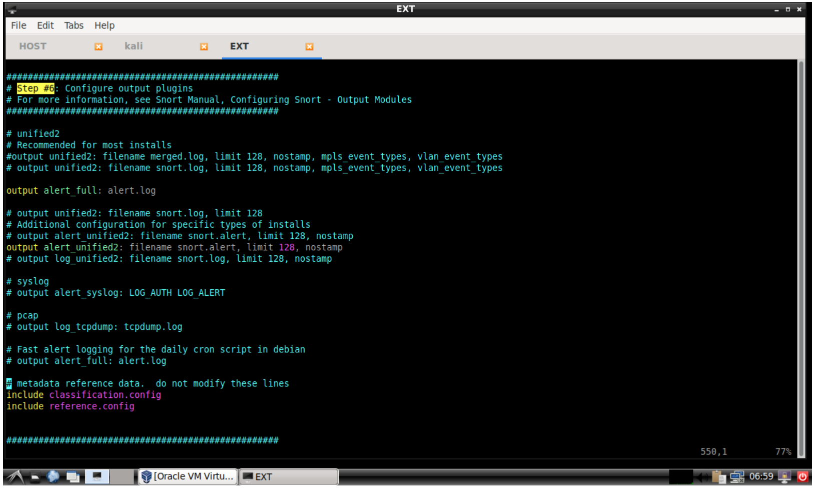


```
# output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan_event_types

output alert_full: alert.log
```

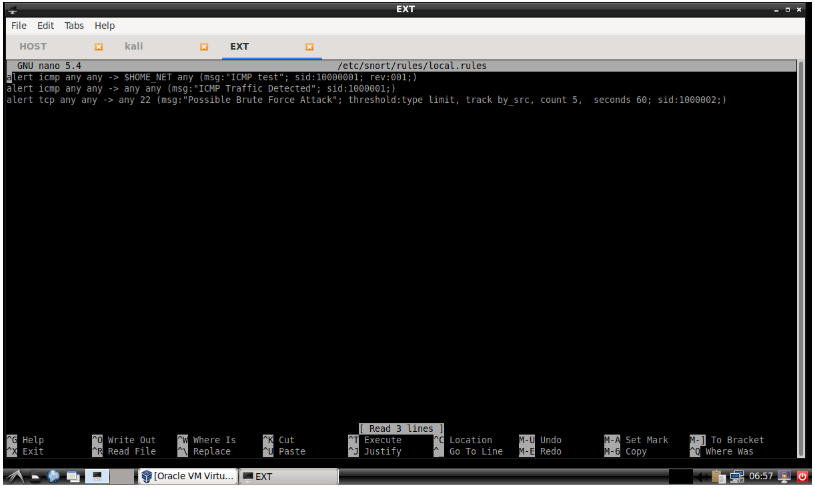
Proof of me doing it



```
GUEST student@extrouter:~$ sudo systemctl status snort
[sudo] password for student:
● snort.service - Snort NIDS Daemon
     Loaded: loaded (/lib/systemd/system/snort.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2024-10-02 02:36:42 UTC; 3h 38min ago
   Main PID: 637 (snort)
      Tasks: 2 (limit: 507)
     Memory: 40.2M
        CPU: 2.754s
     CGroup: /system.slice/snort.service
             └─637 /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3

Oct 02 02:36:42 extrouter systemd[1]: Started Snort NIDS Daemon.
GUEST student@extrouter:~$
```



```
###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################

# unified2
# Recommended for most installs
#output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
# output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan_event_types

output alert_full: alert.log

# output unified2: filename snort.log, limit 128
# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT

# pcap
# output log_tcpdump: tcpdump.log

# Fast alert logging for the daily cron script in debian
# output alert_full: alert.log

# metadata reference data.  do not modify these lines
include classification.config
include reference.config


###################################################
                                                                550,1          77%
```



```
  GNU nano 5.4                                  /etc/snort/rules/local.rules
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
alert icmp any any -> any any (msg:"ICMP Traffic Detected"; sid:1000001;)
alert tcp any any -> any 22 (msg:"Possible Brute Force Attack"; threshold:type limit, track by_src, count 5,  seconds 60; sid:1000002;)

                                          [ Read 3 lines ]
```

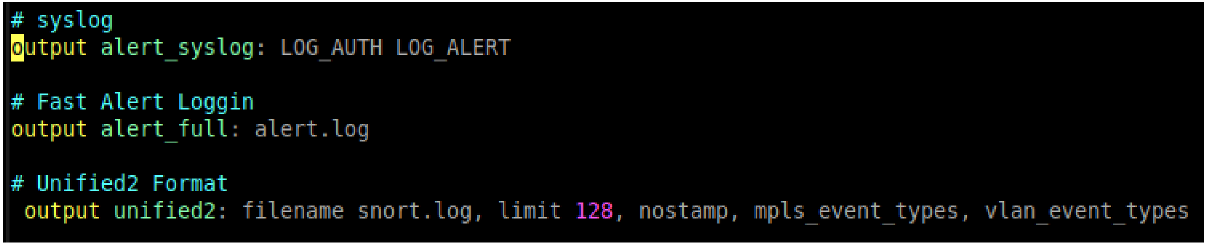
2.3 Logging and Monitoring Snort Alerts

Fast Alert Mode (Fast Logging) Fast Alert Mode is a simplified logging method where alerts are written in a concise, human-readable format. It provides only essential information about each alert, making it ideal for quick scanning and troubleshooting.

Unified2 Format (Binary Logging for Centralized Monitoring) The Unified2 format is a binary logging method suitable for use with centralized alert collection and analysis systems like Snorby, Barnyard2, or Security Onion. It captures more detailed data than the fast alert mode, making it ideal for large-scale or production environments.

Syslog (Remote Logging and Integration with SIEM Systems) Snort can send alerts directly to a syslog server, which can then forward these logs to a centralized monitoring system such as a Security Information and Event Management (SIEM) system (e.g., Splunk, Graylog, or ELK Stack). This method is ideal for real-time alerting and centralized monitoring.

The three different ways to log and monitor Snort Alerts



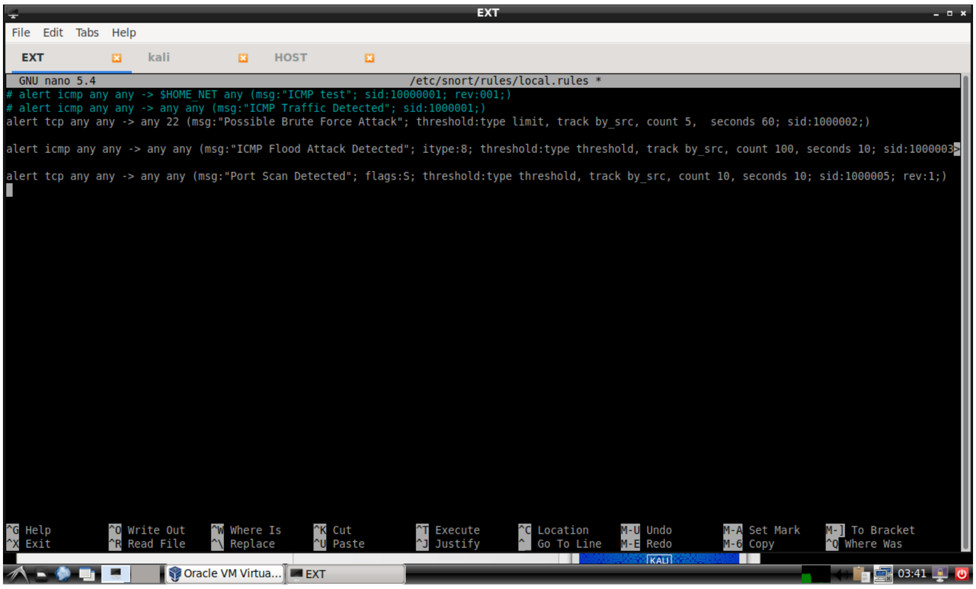
```
# syslog
output alert_syslog: LOG_AUTH LOG_ALERT

# Fast Alert Loggin
output alert_full: alert.log

# Unified2 Format
 output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan_event_types
```

2.4 Detecting Risks and Attacks using Snort

This will consist of 3 attacks:

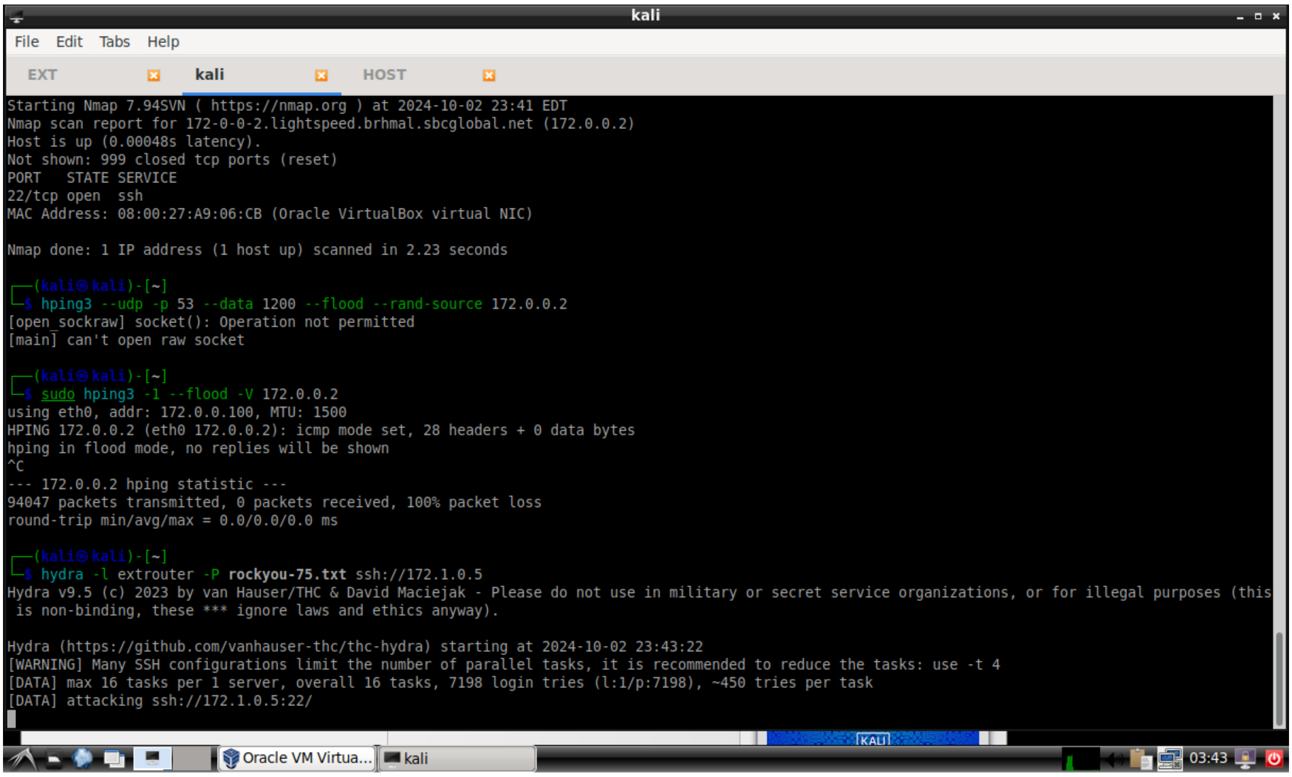
1. Brute Force Attack on SSH
2. ICMP (Ping) Flood (Denial of Service Attack)
3. Port Scanning (nmap) detection, which is commonly used when attacking a system or network

Here are the snort rule set used for the 3 attacks.



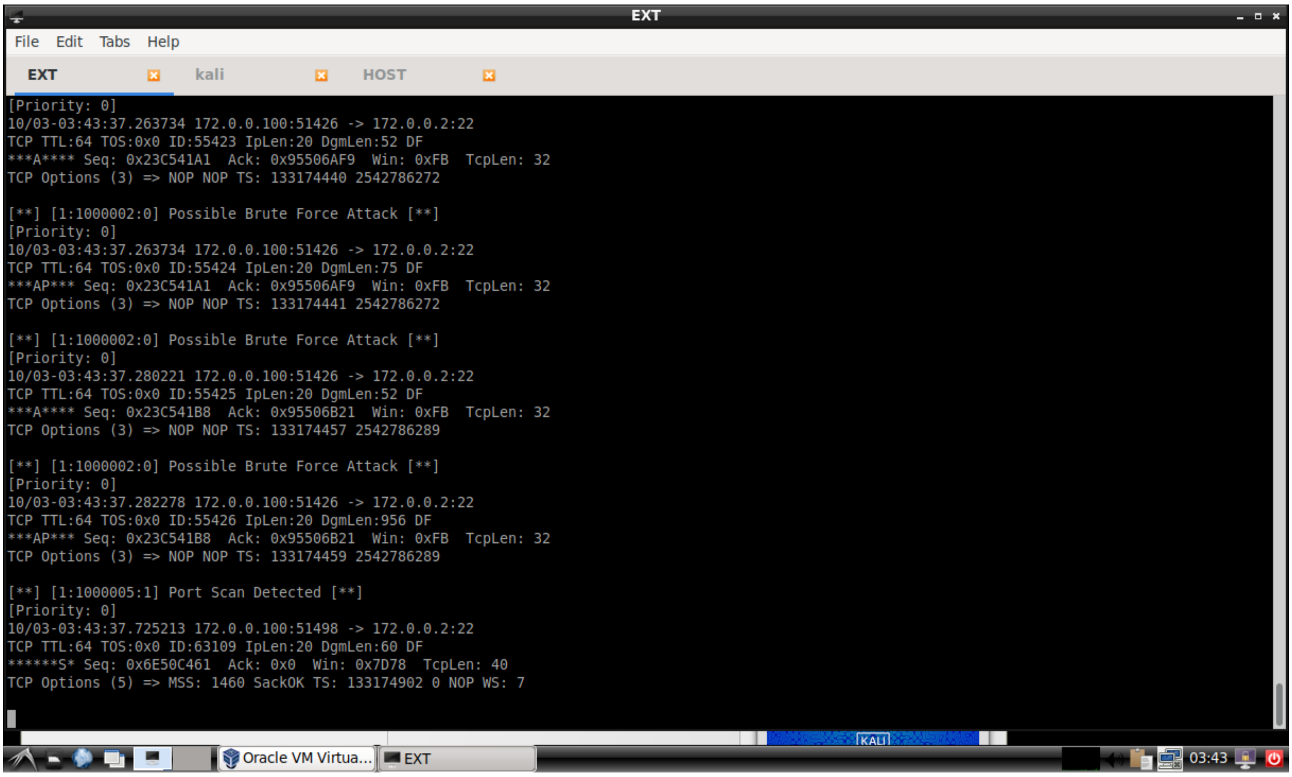
```
 GNU nano 5.4                          /etc/snort/rules/local.rules *
# alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
# alert icmp any any -> any any (msg:"ICMP Traffic Detected"; sid:1000001;)
alert tcp any any -> any 22 (msg:"Possible Brute Force Attack"; threshold:type limit, track by_src, count 5,  seconds 60; sid:1000002;)

alert icmp any any -> any any (msg:"ICMP Flood Attack Detected"; itype:8; threshold:type threshold, track by_src, count 100, seconds 10; sid:1000003>

alert tcp any any -> any any (msg:"Port Scan Detected"; flags:S; threshold:type threshold, track by_src, count 10, seconds 10; sid:1000005; rev:1;)
```

Brute Force Attack on SSH A brute force attack involves trying multiple combinations of usernames and passwords in an attempt to gain unauthorized access to a service, like SSH. The attacker typically uses tools like Hydra or Medusa to automate the guessing process. Snort can detect such attacks by identifying multiple failed login attempts from the same IP address.



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 23:41 EDT
Nmap scan report for 172-0-0-2.lightspeed.brhmal.sbcglobal.net (172.0.0.2)
Host is up (0.00048s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:A9:06:CB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.23 seconds

┌──(kali㉿kali)-[~]
└─$ hping3 --udp -p 53 --data 1200 --flood --rand-source 172.0.0.2
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

┌──(kali㉿kali)-[~]
└─$ sudo hping3 -1 --flood -V 172.0.0.2
using eth0, addr: 172.0.0.100, MTU: 1500
HPING 172.0.0.2 (eth0 172.0.0.2): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 172.0.0.2 hping statistic ---
94047 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(kali㉿kali)-[~]
└─$ hydra -l extrouter -P rockyou-75.txt ssh://172.1.0.5
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this
 is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-02 23:43:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 7198 login tries (l:1/p:7198), ~450 tries per task
[DATA] attacking ssh://172.1.0.5:22/
```

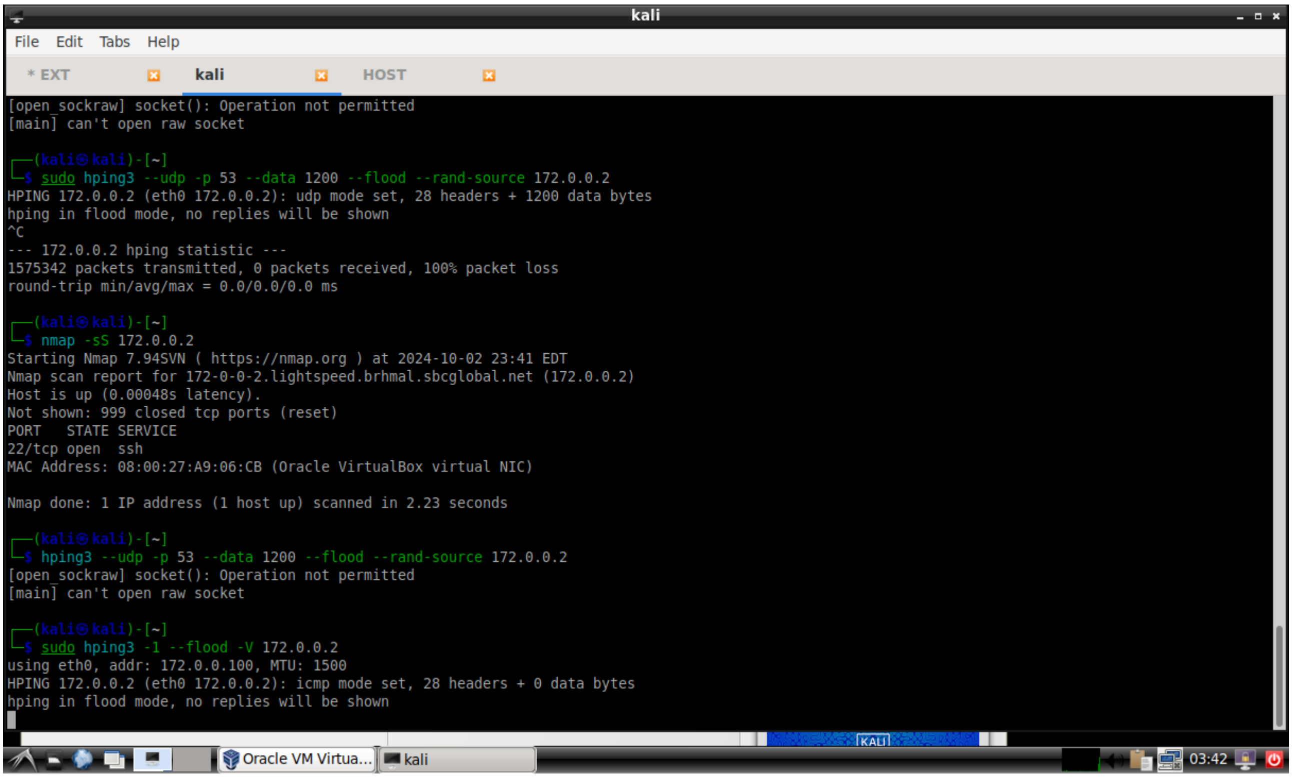
Figure 1: Screenshot showing an SSH Attack in progress using the hydra tool



```
[Priority: 0]
10/03-03:43:37.263734 172.0.0.100:51426 -> 172.0.0.2:22
TCP TTL:64 TOS:0x0 ID:55423 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x23C541A1  Ack: 0x95506AF9  Win: 0xFB  TcpLen: 32
TCP Options (3) => NOP NOP TS: 133174440 2542786272

[**] [1:1000002:0] Possible Brute Force Attack [**]
[Priority: 0]
10/03-03:43:37.263734 172.0.0.100:51426 -> 172.0.0.2:22
TCP TTL:64 TOS:0x0 ID:55424 IpLen:20 DgmLen:75 DF
***AP*** Seq: 0x23C541A1  Ack: 0x95506AF9  Win: 0xFB  TcpLen: 32
TCP Options (3) => NOP NOP TS: 133174441 2542786272

[**] [1:1000002:0] Possible Brute Force Attack [**]
[Priority: 0]
10/03-03:43:37.280221 172.0.0.100:51426 -> 172.0.0.2:22
TCP TTL:64 TOS:0x0 ID:55425 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x23C541B8  Ack: 0x95506B21  Win: 0xFB  TcpLen: 32
TCP Options (3) => NOP NOP TS: 133174457 2542786289

[**] [1:1000002:0] Possible Brute Force Attack [**]
[Priority: 0]
10/03-03:43:37.282278 172.0.0.100:51426 -> 172.0.0.2:22
TCP TTL:64 TOS:0x0 ID:55426 IpLen:20 DgmLen:956 DF
***AP*** Seq: 0x23C541B8  Ack: 0x95506B21  Win: 0xFB  TcpLen: 32
TCP Options (3) => NOP NOP TS: 133174459 2542786289

[**] [1:1000005:1] Port Scan Detected [**]
[Priority: 0]
10/03-03:43:37.725213 172.0.0.100:51498 -> 172.0.0.2:22
TCP TTL:64 TOS:0x0 ID:63109 IpLen:20 DgmLen:60 DF
******S* Seq: 0x6E50C461  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 133174902 0 NOP WS: 7
```

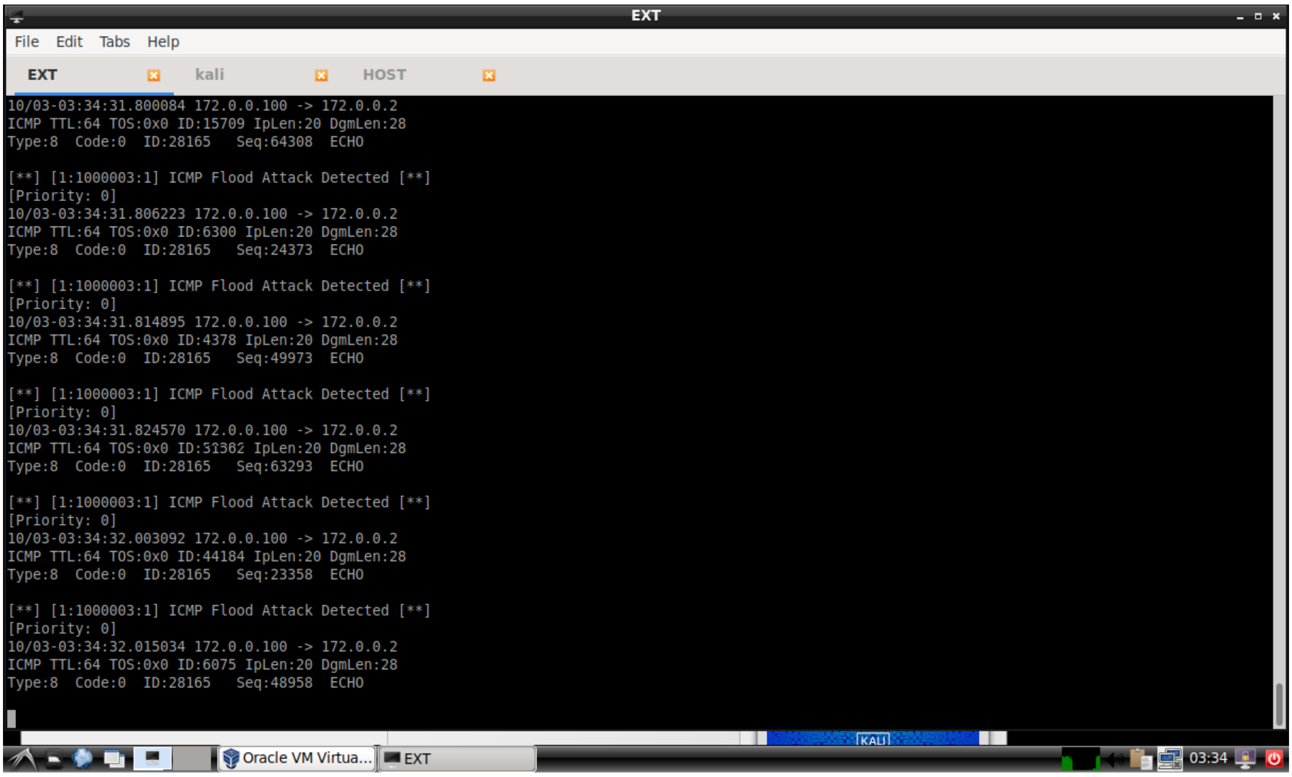
Figure 2: Screenshot showing Snort alerts about a SSH Attack

ICMP (Ping) Flood (Denial of Service Attack) A Ping Flood or ICMP flood attack involves sending a large number of ICMP echo request (ping) packets to a target system, overwhelming it and potentially causing a Denial of Service (DoS). Snort can detect this attack by monitoring the rate of ICMP requests coming from the same source IP.



```
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

┌──(kali㉿kali)-[~]
└─$ sudo hping3 --udp -p 53 --data 1200 --flood --rand-source 172.0.0.2
HPING 172.0.0.2 (eth0 172.0.0.2): udp mode set, 28 headers + 1200 data bytes
hping in flood mode, no replies will be shown
^C
--- 172.0.0.2 hping statistic ---
1575342 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(kali㉿kali)-[~]
└─$ nmap -sS 172.0.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 23:41 EDT
Nmap scan report for 172-0-0-2.lightspeed.brhmal.sbcglobal.net (172.0.0.2)
Host is up (0.00048s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:A9:06:CB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.23 seconds

┌──(kali㉿kali)-[~]
└─$ hping3 --udp -p 53 --data 1200 --flood --rand-source 172.0.0.2
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

┌──(kali㉿kali)-[~]
└─$ sudo hping3 -1 --flood -V 172.0.0.2
using eth0, addr: 172.0.0.100, MTU: 1500
HPING 172.0.0.2 (eth0 172.0.0.2): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

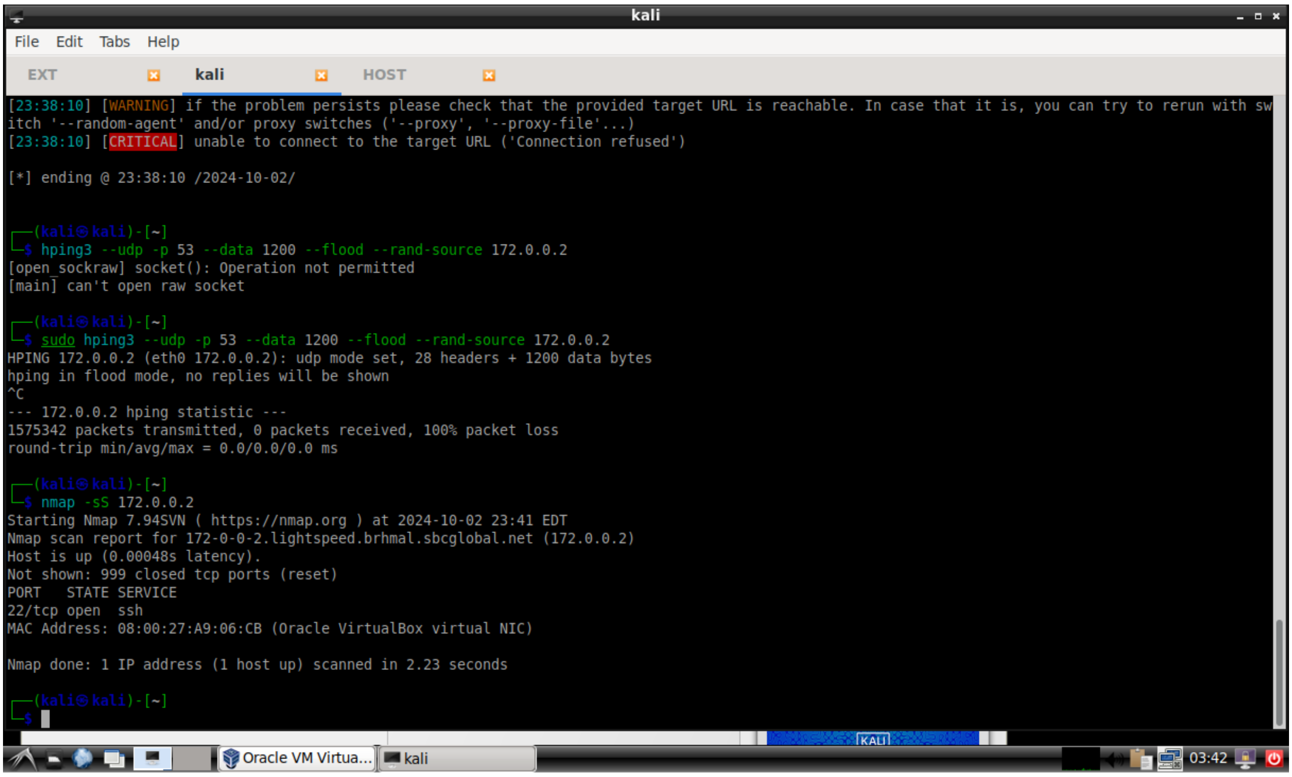
Figure 3: Screenshot showing an ICMP in progress using the hping3 tool



```
10/03-03:34:31.800084 172.0.0.100 -> 172.0.0.2
ICMP TTL:64 TOS:0x0 ID:15709 IpLen:20 DgmLen:28
Type:8  Code:0  ID:28165   Seq:64308  ECHO

[**] [1:1000003:1] ICMP Flood Attack Detected [**]
[Priority: 0]
10/03-03:34:31.806223 172.0.0.100 -> 172.0.0.2
ICMP TTL:64 TOS:0x0 ID:6300 IpLen:20 DgmLen:28
Type:8  Code:0  ID:28165   Seq:24373  ECHO

[**] [1:1000003:1] ICMP Flood Attack Detected [**]
[Priority: 0]
10/03-03:34:31.814895 172.0.0.100 -> 172.0.0.2
ICMP TTL:64 TOS:0x0 ID:4378 IpLen:20 DgmLen:28
Type:8  Code:0  ID:28165   Seq:49973  ECHO

[**] [1:1000003:1] ICMP Flood Attack Detected [**]
[Priority: 0]
10/03-03:34:31.824570 172.0.0.100 -> 172.0.0.2
ICMP TTL:64 TOS:0x0 ID:51362 IpLen:20 DgmLen:28
Type:8  Code:0  ID:28165   Seq:63293  ECHO

[**] [1:1000003:1] ICMP Flood Attack Detected [**]
[Priority: 0]
10/03-03:34:32.003092 172.0.0.100 -> 172.0.0.2
ICMP TTL:64 TOS:0x0 ID:44184 IpLen:20 DgmLen:28
Type:8  Code:0  ID:28165   Seq:23358  ECHO

[**] [1:1000003:1] ICMP Flood Attack Detected [**]
[Priority: 0]
10/03-03:34:32.015034 172.0.0.100 -> 172.0.0.2
ICMP TTL:64 TOS:0x0 ID:6075 IpLen:20 DgmLen:28
Type:8  Code:0  ID:28165   Seq:48958  ECHO
```

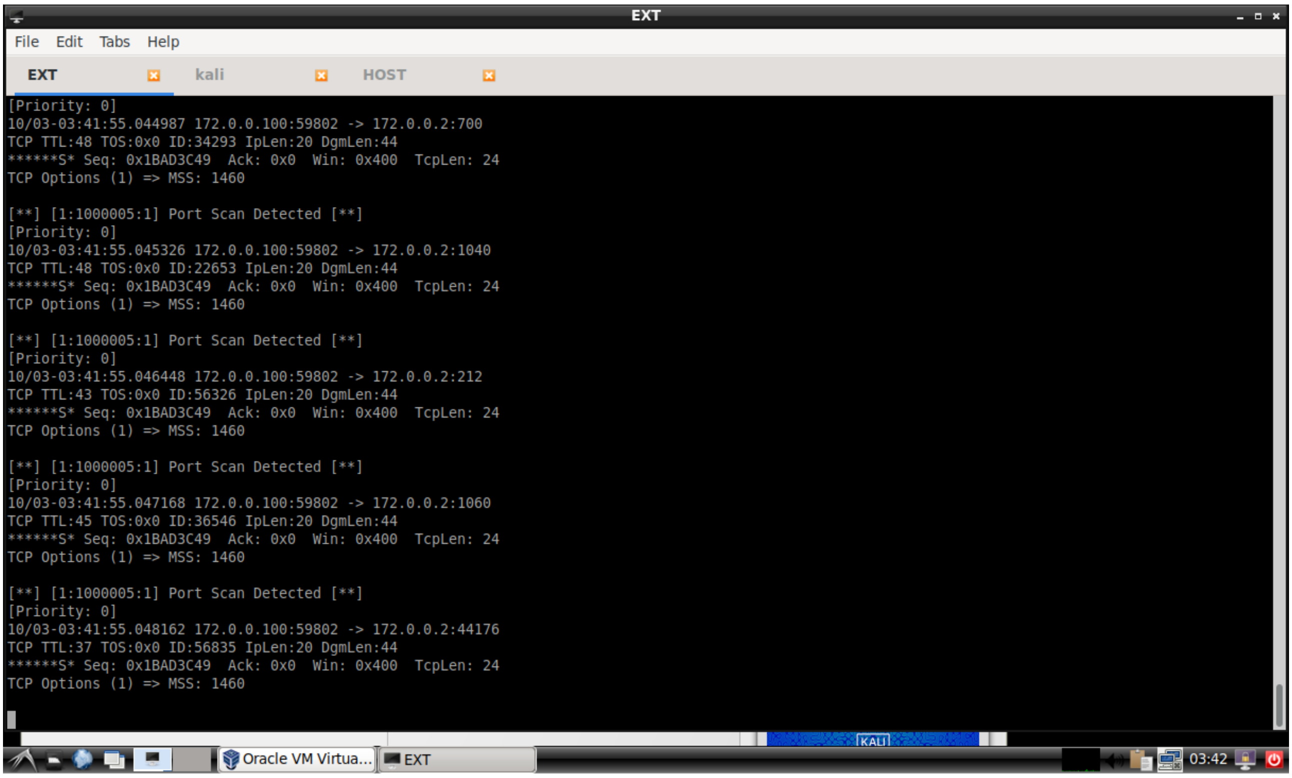
Figure 4: Screenshot showing Snort alerts about a ICMP Flood Attack

Port Scanning (Nmap) Port scanning is often used by attackers to identify open ports and services on a target system. Tools like Nmap are commonly used for this purpose. While port scanning isn't inherently malicious, it is often a precursor to more serious attacks. Snort can detect port scanning by monitoring for multiple connection attempts to different ports from the same source IP.



```
[23:38:10] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with sw
itch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file'...)
[23:38:10] [CRITICAL] unable to connect to the target URL ('Connection refused')

[*] ending @ 23:38:10 /2024-10-02/


┌──(kali㉿kali)-[~]
└─$ hping3 --udp -p 53 --data 1200 --flood --rand-source 172.0.0.2
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

┌──(kali㉿kali)-[~]
└─$ sudo hping3 --udp -p 53 --data 1200 --flood --rand-source 172.0.0.2
HPING 172.0.0.2 (eth0 172.0.0.2): udp mode set, 28 headers + 1200 data bytes
hping in flood mode, no replies will be shown
^C
--- 172.0.0.2 hping statistic ---
1575342 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(kali㉿kali)-[~]
└─$ nmap -sS 172.0.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 23:41 EDT
Nmap scan report for 172-0-0-2.lightspeed.brhmal.sbcglobal.net (172.0.0.2)
Host is up (0.00048s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:A9:06:CB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.23 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 5: Screenshot showing an Port Scan in progress using the NMAP tool



```
[Priority: 0]
10/03-03:41:55.044987 172.0.0.100:59802 -> 172.0.0.2:700
TCP TTL:48 TOS:0x0 ID:34293 IpLen:20 DgmLen:44
******S* Seq: 0x1BAD3C49  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460

[**] [1:1000005:1] Port Scan Detected [**]
[Priority: 0]
10/03-03:41:55.045326 172.0.0.100:59802 -> 172.0.0.2:1040
TCP TTL:48 TOS:0x0 ID:22653 IpLen:20 DgmLen:44
******S* Seq: 0x1BAD3C49  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460

[**] [1:1000005:1] Port Scan Detected [**]
[Priority: 0]
10/03-03:41:55.046448 172.0.0.100:59802 -> 172.0.0.2:212
TCP TTL:43 TOS:0x0 ID:56326 IpLen:20 DgmLen:44
******S* Seq: 0x1BAD3C49  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460

[**] [1:1000005:1] Port Scan Detected [**]
[Priority: 0]
10/03-03:41:55.047168 172.0.0.100:59802 -> 172.0.0.2:1060
TCP TTL:45 TOS:0x0 ID:36546 IpLen:20 DgmLen:44
******S* Seq: 0x1BAD3C49  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460

[**] [1:1000005:1] Port Scan Detected [**]
[Priority: 0]
10/03-03:41:55.048162 172.0.0.100:59802 -> 172.0.0.2:44176
TCP TTL:37 TOS:0x0 ID:56835 IpLen:20 DgmLen:44
******S* Seq: 0x1BAD3C49  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
```

Figure 6: Screenshot showing Snort alerts about a Port Scan

2.5 Complementary Controls for IDS

Firewall with Intrusion Prevention Capabilities (WAF or Network-Based Firewall) A firewall with built-in Intrusion Prevention System (IPS) or Web Application Firewall (WAF) capabilities can provide an additional layer of protection against various types of attacks, including SQL Injection (SQLi), Cross-Site Scripting (XSS), and Brute Force Attacks.

Network Segmentation and Access Control Lists (ACLs) Network Segmentation involves dividing a network into smaller sub-networks (or segments) to restrict lateral movement of attackers and limit access to critical systems. Combined with Access Control Lists (ACLs), this control helps mitigate risks from Port Scanning, DNS Amplification Attacks, and other reconnaissance activities by limiting access to sensitive services or devices.

3 Proxies

3.1 Main purposes of Proxy

Adding TLS to a Web Server Using a Reverse Proxy In this setup, a reverse proxy is used to add TLS encryption to a web server. The reverse proxy terminates TLS (HTTPS) connections from clients and forwards requests to the backend web server, which may not support TLS itself.

Security Goals:

Confidentiality LS encrypts the communication between the client and the reverse proxy, ensuring sensitive information (e.g., login credentials, personal data) isn't intercepted by attackers during transmission.

Integrity TLS also protects against data tampering during transmission. If data is modified in transit, the client or server will detect it through cryptographic checks.

Availability Reverse proxies can distribute traffic across multiple backend servers, preventing one server from being overwhelmed. This improves uptime and availability.

Security Principles:

Defense in Depth The reverse proxy acts as an additional layer of security between the client and the backend server, reducing direct exposure of the internal server.

ISeparation of Responsibilities The proxy manages TLS encryption, offloading the complexity from the backend server. This ensures a more manageable security architecture.

Fail-Safe Defaults If the TLS handshake fails or the proxy server detects suspicious behavior, connections can be rejected, reducing risks from improperly configured or malicious requests.

Setting up a Web Proxy with Filtering This configuration involves using mitmproxy to intercept, inspect, and filter HTTP/HTTPS traffic between clients and servers. The proxy sits between the client and the target website, decrypting and analyzing the content before passing it along.

Security Goals:

Confidentiality Although mitmproxy intercepts encrypted traffic, in legitimate scenarios (such as internal monitoring), it helps ensure that only authorized users or systems can view sensitive data.

Integrity mitmproxy allows filtering to block or modify malicious traffic, ensuring only legitimate and safe data reaches clients or servers.

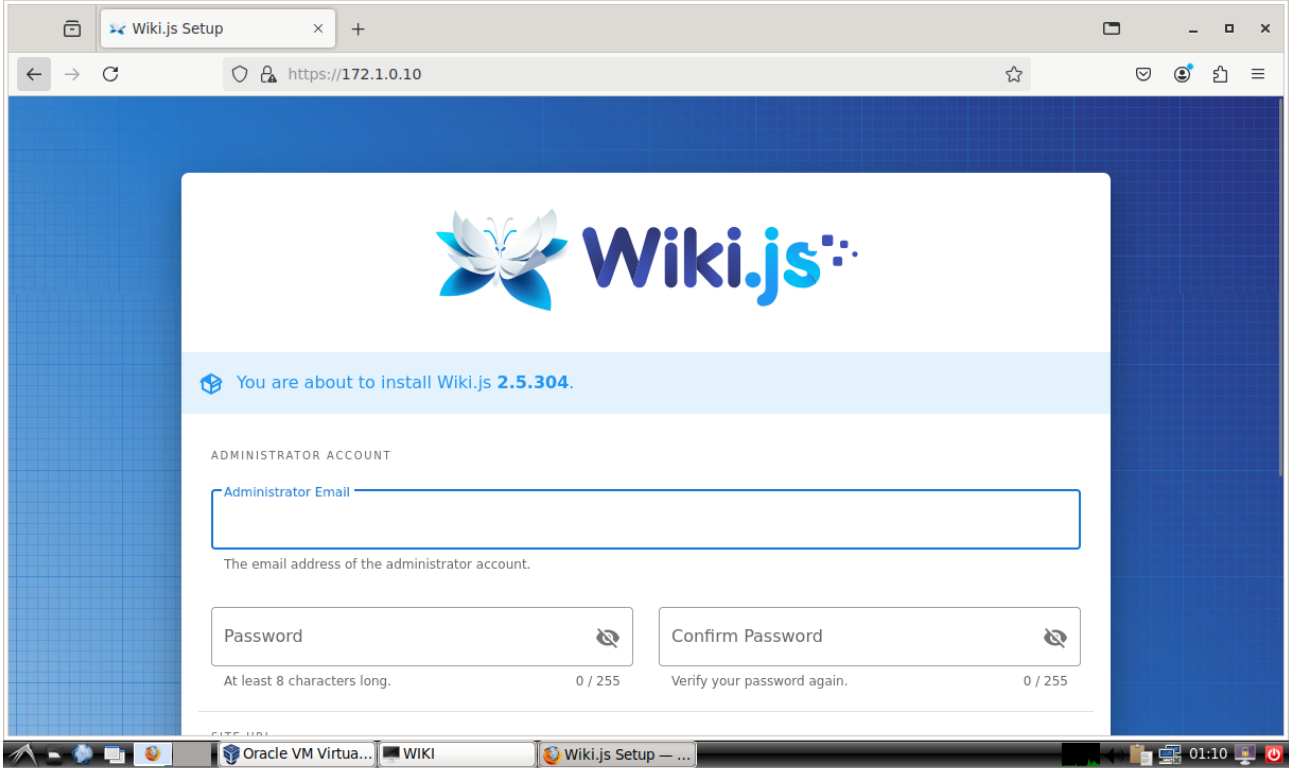
Availability By blocking harmful or unnecessary traffic (e.g., ads, malicious scripts), mitmproxy ensures that only important resources are accessed, optimizing network availability and reducing strain.

Security Principles:

Least Privilege Mitmproxy can be configured to monitor or filter only specific traffic types, ensuring that the proxy doesn't access more data than necessary.

Inspection and Auditing The proxy can be used to log and inspect traffic, supporting security audits and monitoring for compliance or security policy violations.

Fail-Secure Stance If mitmproxy detects malicious behavior or harmful content, it can block connections, preventing compromised data from reaching the client or server.



You are about to install Wiki.js **2.5.304**.

ADMINISTRATOR ACCOUNT

Administrator Email

The email address of the administrator account.

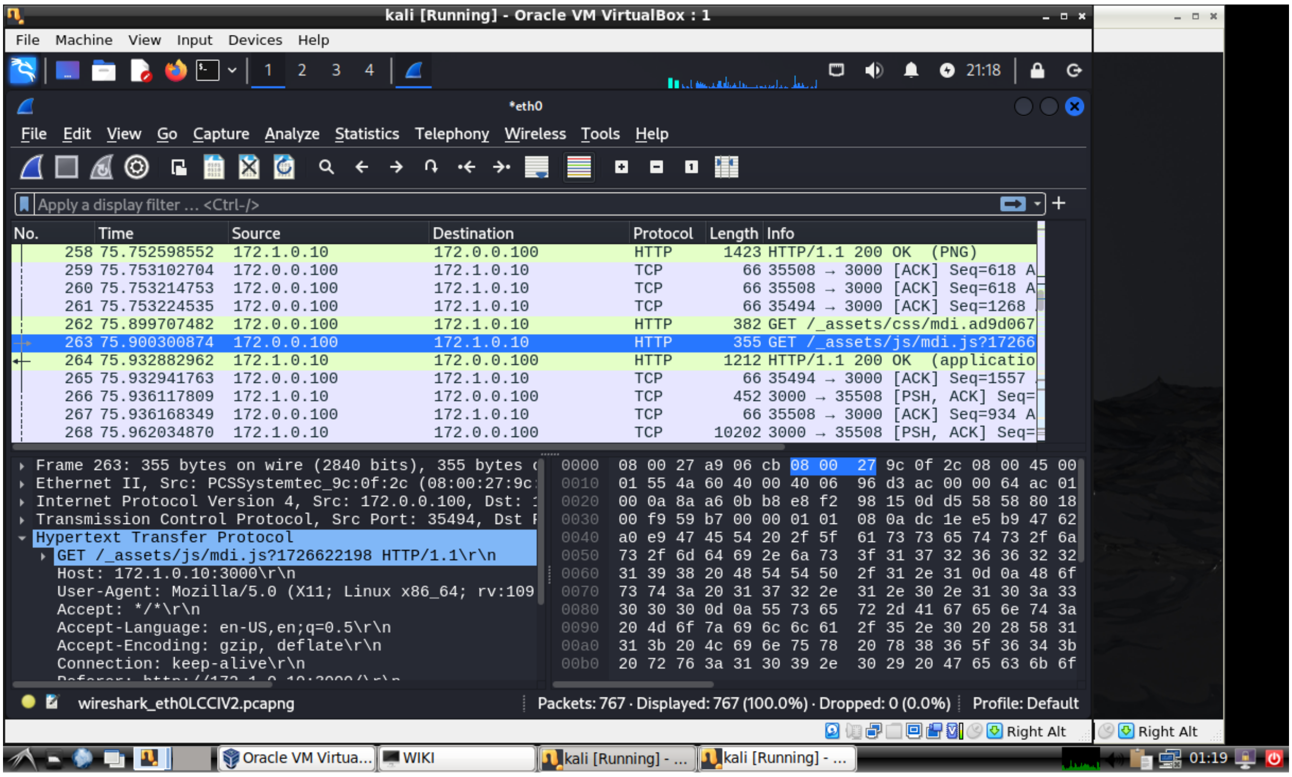
Password

At least 8 characters long. 0 / 255

Confirm Password

Verify your password again. 0 / 255

Figure 7: Web Page and URL of the nginx Proxy



kali [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
21:18
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Right Alt
Oracle VM Virtua…
WIKI
kali [Running] - …
01:19

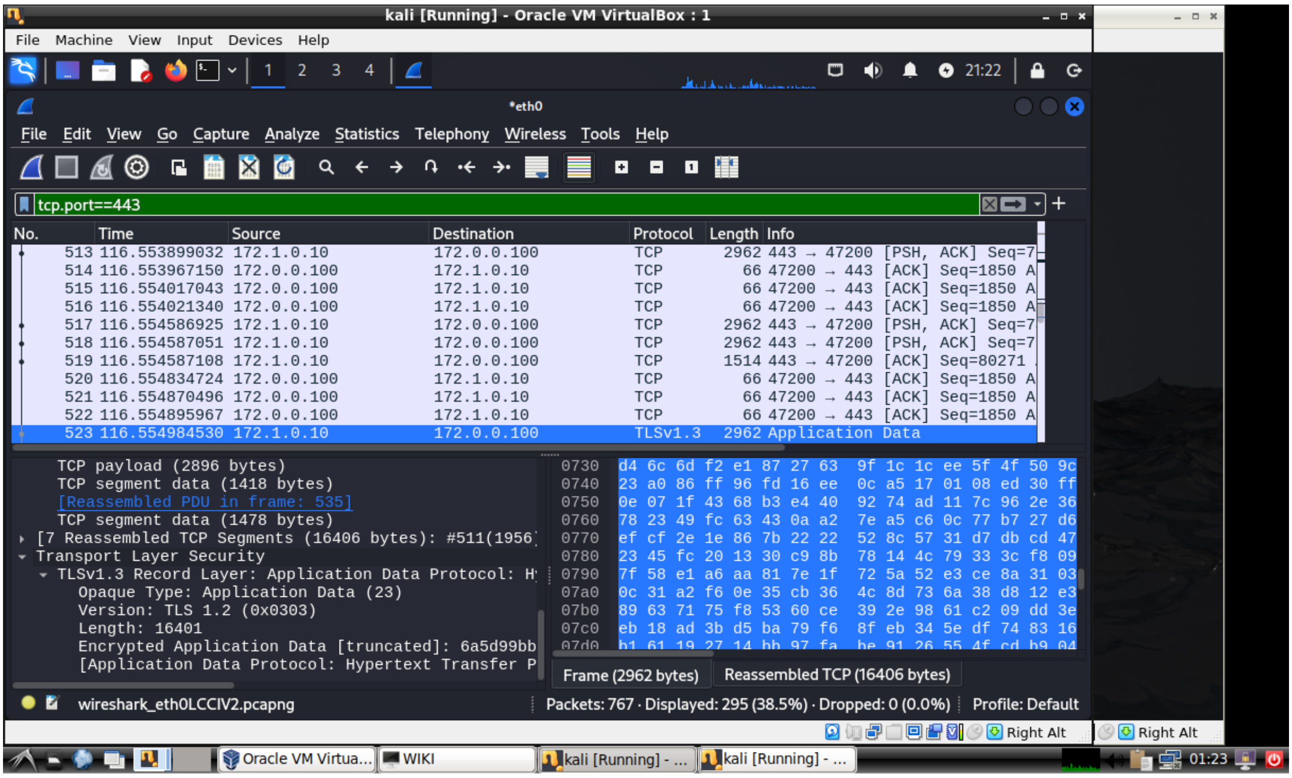
```
No.  Time           Source       Destination   Protocol Length Info
 258 75.752598552  172.1.0.10   172.0.0.100   HTTP      1423 HTTP/1.1 200 OK  (PNG)
 259 75.753102704  172.0.0.100  172.1.0.10    TCP         66 35508 → 3000 [ACK] Seq=618 A
 260 75.753214753  172.0.0.100  172.1.0.10    TCP         66 35508 → 3000 [ACK] Seq=618 A
 261 75.753224535  172.0.0.100  172.1.0.10    TCP         66 35494 → 3000 [ACK] Seq=1268
 262 75.899707482  172.0.0.100  172.1.0.10    HTTP       382 GET /_assets/css/mdi.ad9d067
 263 75.900300874  172.0.0.100  172.1.0.10    HTTP       355 GET /_assets/js/mdi.js?17266
 264 75.932882962  172.1.0.10   172.0.0.100   HTTP      1212 HTTP/1.1 200 OK  (applicatio
 265 75.932941763  172.0.0.100  172.1.0.10    TCP         66 35494 → 3000 [ACK] Seq=1557
 266 75.936117809  172.1.0.10   172.0.0.100   TCP        452 3000 → 35508 [PSH, ACK] Seq=
 267 75.936168349  172.0.0.100  172.1.0.10    TCP         66 35508 → 3000 [ACK] Seq=934 A
 268 75.962034870  172.1.0.10   172.0.0.100   TCP      10202 3000 → 35508 [PSH, ACK] Seq=
```

```
› Frame 263: 355 bytes on wire (2840 bits), 355 bytes c
› Ethernet II, Src: PCSSystemtec_9c:0f:2c (08:00:27:9c:
› Internet Protocol Version 4, Src: 172.0.0.100, Dst: 1
› Transmission Control Protocol, Src Port: 35494, Dst P
⌄ Hypertext Transfer Protocol
  › GET /_assets/js/mdi.js?1726622198 HTTP/1.1\r\n
    Host: 172.1.0.10:3000\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
```

```
0000  08 00 27 a9 06 cb 08 00  27 9c 0f 2c 08 00 45 00
0010  01 55 4a 60 40 00 40 06  96 d3 ac 00 00 64 ac 01
0020  00 0a 8a a6 0b b8 e8 f2  98 15 0d d5 58 58 80 18
0030  00 f9 59 b7 00 00 01 01  08 0a dc 1e e5 b9 47 62
0040  a0 e9 47 45 54 20 2f 5f  61 73 73 65 74 73 2f 6a
0050  73 2f 6d 64 69 2e 6a 73  3f 31 37 32 36 36 32 32
0060  31 39 38 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f
0070  73 74 3a 20 31 37 32 2e  31 2e 30 2e 31 30 3a 33
0080  30 30 30 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a
0090  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 58 31
00a0  31 3b 20 4c 69 6e 75 78  20 78 38 36 5f 36 34 3b
00b0  20 72 76 3a 31 30 39 2e  30 29 20 47 65 63 6b 6f
```

```
wireshark_eth0LCCIV2.pcapng    Packets: 767 · Displayed: 767 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 8: Wireshark unencrypted packet capture



kali [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
21:22
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Alt
Oracle VM Virtua…
WIKI
kali [Running] - …
01:23

```
tcp.port==443
```

```
No.  Time            Source       Destination   Protocol Length Info
 513 116.553899032  172.1.0.10   172.0.0.100   TCP       2962 443 → 47200 [PSH, ACK] Seq=7
 514 116.553967150  172.0.0.100  172.1.0.10    TCP         66 47200 → 443 [ACK] Seq=1850 A
 515 116.554017043  172.0.0.100  172.1.0.10    TCP         66 47200 → 443 [ACK] Seq=1850 A
 516 116.554021340  172.0.0.100  172.1.0.10    TCP         66 47200 → 443 [ACK] Seq=1850 A
 517 116.554586925  172.1.0.10   172.0.0.100   TCP       2962 443 → 47200 [PSH, ACK] Seq=7
 518 116.554587051  172.1.0.10   172.0.0.100   TCP       2962 443 → 47200 [PSH, ACK] Seq=7
 519 116.554587108  172.1.0.10   172.0.0.100   TCP       1514 443 → 47200 [ACK] Seq=80271
 520 116.554834724  172.0.0.100  172.1.0.10    TCP         66 47200 → 443 [ACK] Seq=1850 A
 521 116.554870496  172.0.0.100  172.1.0.10    TCP         66 47200 → 443 [ACK] Seq=1850 A
 522 116.554895967  172.0.0.100  172.1.0.10    TCP         66 47200 → 443 [ACK] Seq=1850 A
 523 116.554984530  172.1.0.10   172.0.0.100   TLSv1.3   2962 Application Data
```

```
    TCP payload (2896 bytes)
    TCP segment data (1418 bytes)
    [Reassembled PDU in frame: 535]
    TCP segment data (1478 bytes)
› [7 Reassembled TCP Segments (16406 bytes): #511(1956)
⌄ Transport Layer Security
  ⌄ TLSv1.3 Record Layer: Application Data Protocol: H
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 16401
      Encrypted Application Data [truncated]: 6a5d99bb
      [Application Data Protocol: Hypertext Transfer P
```

```
0730  d4 6c 6d f2 e1 87 27 63  9f 1c 1c ee 5f 4f 50 9c
0740  23 a0 86 ff 96 fd 16 ee  0c a5 17 01 08 ed 30 ff
0750  0e 07 1f 43 68 b3 e4 40  92 74 ad 11 7c 96 2e 36
0760  78 23 49 fc 63 43 0a a2  7e a5 c6 0c 77 b7 27 d6
0770  ef cf 2e 1e 86 7b 22 22  52 8c 57 31 d7 db cd 47
0780  23 45 fc 20 13 30 c9 8b  78 14 4c 79 33 3c f8 09
0790  7f 58 e1 a6 aa 81 7e 1f  72 5a 52 e3 ce 8a 31 03
07a0  0c 31 a2 f6 0e 35 cb 36  4c 8d 73 6a 38 d8 12 e3
07b0  89 63 71 75 f8 53 60 ce  39 2e 98 61 c2 09 dd 3e
07c0  eb 18 ad 3b d5 ba 79 f6  8f eb 34 5e df 74 83 16
```

```
Frame (2962 bytes)    Reassembled TCP (16406 bytes)
wireshark_eth0LCCIV2.pcapng    Packets: 767 · Displayed: 295 (38.5%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 9: Wireshark encrypted packet capture

MISSING SCREENSHOTS - No Internet connection on Kali VM:

- Set up Firefox on Kali to use the proxy
- Configure some filtering

3.2 Remaining Risk

Risks associated with each proxy configuration:

Adding TLS to a Web Server Using a Reverse Proxy

1. **TLS Misconfiguration Risk** - If the TLS configuration (e.g., cipher suites, certificates, or protocols) is not properly managed, the proxy might allow weak encryption methods, making it vulnerable to attacks such as downgrade attacks or cipher vulnerabilities (e.g., SWEET32). This can compromise the confidentiality and integrity of data in transit.

2. **Man-in-the-Middle Attack on the Proxy** - While the reverse proxy secures connections between the client and the proxy, attackers could target the connection between the reverse proxy and backend server if it isn't secured properly. This risk exposes backend data to interception or tampering.

3. **Single Point of Failure** - If the reverse proxy fails, the entire system may become unavailable. Although proxies often support high availability through load balancing, misconfigured failover mechanisms could still result in downtime and affect availability.

Setting up a Web Proxy with Filtering Using mitmproxy

1. **Privacy and Ethical Risks** - Since mitmproxy decrypts and inspects encrypted traffic, it can capture sensitive information such as passwords or personal data. This introduces privacy risks if access to logs or captured data is not properly controlled, or if the system is used unethically.

2. **Potential Introduction of New Vulnerabilities** - Intercepting and re-encrypting traffic introduces another point of vulnerability. If the proxy mishandles encryption keys or fails to re-encrypt traffic correctly, attackers could exploit these weaknesses, compromising the data's confidentiality and integrity.

3. **Detection and Evasion by Attackers** - Some sophisticated attackers or malware may detect the presence of a proxy and attempt to bypass it by using non-standard protocols, encrypted tunnels, or domain fronting techniques. This can limit the effectiveness of the filtering, leaving the system exposed to threats.

3.3 Complementary Controls to Proxy

Complementary controls to mitigate the identified risks:

Adding TLS to a Web Server Using a Reverse Proxy

1. **TLS Misconfiguration Risk → Regular Security Audits and Hardened Configuration** - Conduct periodic audits of the TLS configuration using tools like SSL Labs or OpenSSL to identify weak cipher suites and protocols. Implement hardened TLS settings (e.g., disabling TLS 1.0/1.1, using strong ciphers, and certificate pinning) to mitigate downgrade attacks.

2. **Man-in-the-Middle Attack on the Proxy → Secure Backend Communication with TLS** - Use TLS encryption between the reverse proxy and backend servers to prevent interception or tampering of internal traffic. Enable mutual TLS (mTLS) authentication between the proxy and backend to ensure that only authorized servers can communicate.

3. **Single Point of Failure → Load Balancing and Redundancy** - Implement load balancers and configure multiple reverse proxies to distribute traffic evenly. Use health checks and failover mechanisms to ensure availability in case one proxy instance goes down.

Setting up a Web Proxy with Filtering Using mitmproxy

1. **Privacy and Ethical Risks → Access Control and Data Retention Policies** - Implement strict access control to ensure that only authorized personnel can view decrypted traffic or logs. Establish data retention policies that limit how long captured data is stored and ensure sensitive information is deleted promptly.

2. **Introduction of New Vulnerabilities → Secure Key Management and Patching** - Use a centralized key management system to securely store and rotate encryption keys used by the proxy. Regularly update and patch the proxy software to address vulnerabilities and improve encryption handling.

3. **Detection and Evasion by Attackers → Deep Packet Inspection and Anomaly Detection** - Integrate deep packet inspection (DPI) tools alongside mitmproxy to detect non-standard protocols or encrypted tunnels used for evasion. Employ intrusion detection systems (IDS) to monitor for anomalous behavior that could indicate an attacker bypassing the proxy.

4 Security Information and Event Management (SIEM)

4.1 Introduction to SIEM

Primary purposes and roles of SIEM's

Centralized Log Collection and Correlation SIEM aggregates logs and events from various sources, such as firewalls, proxies, servers, and endpoints, into a unified system. It correlates data across these sources to identify patterns that might indicate security incidents or policy violations.

Real-Time Threat Detection and Alerts SIEM continuously monitors network traffic and system events to detect suspicious activity, such as unauthorized access attempts or malware. It provides real-time alerts to security teams, enabling swift responses to potential threats.

Incident Response and Forensics SIEM assists in the investigation of security incidents by providing detailed logs and reports that can help identify the scope and impact of an attack. It supports post-incident analysis and forensics to understand the root cause and improve defenses.

4.2 Wazuh as SIEM

Wazuh is an open-source SIEM platform that provides comprehensive security monitoring, threat detection, and incident response capabilities. It collects and analyzes logs from various sources, helping organizations identify security threats, ensure compliance, and manage vulnerabilities.

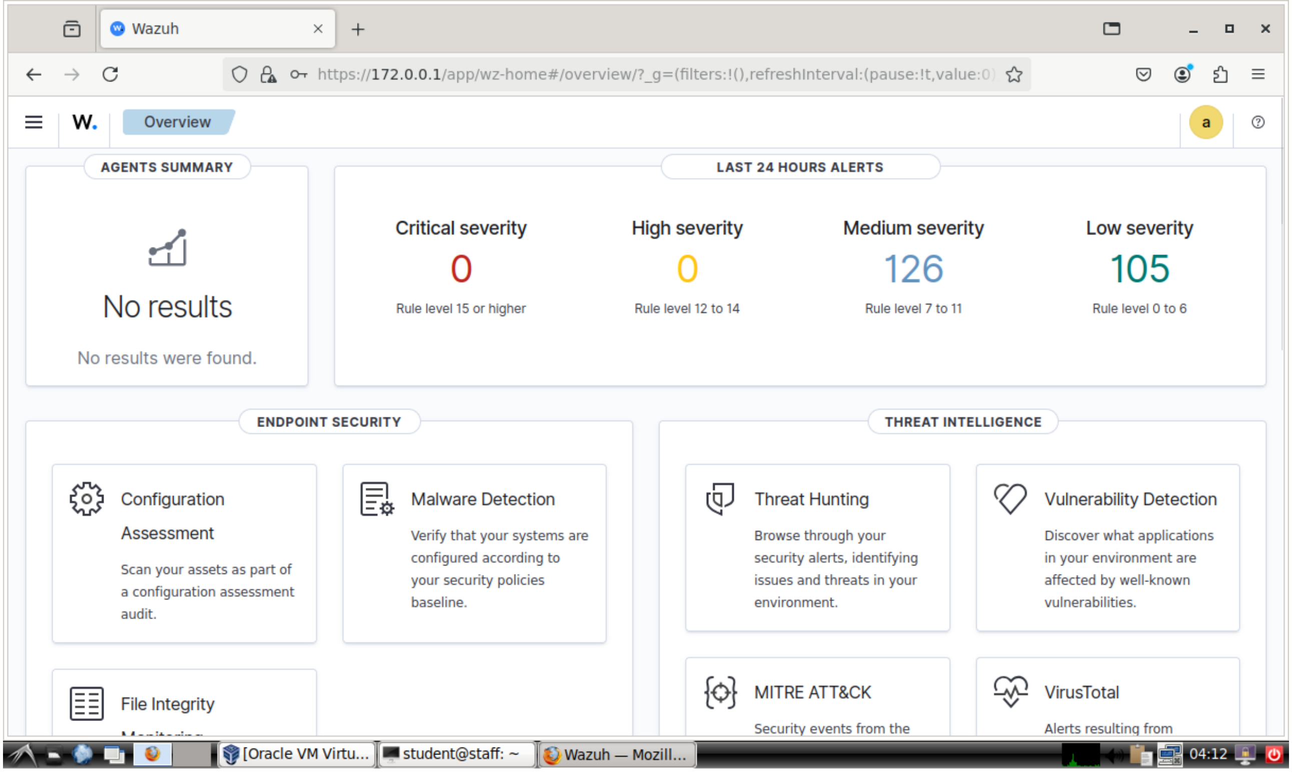
Features Supporting Security Monitoring and Threat Management

Log Collection and Analysis Wazuh collects logs from multiple systems (e.g., servers, firewalls, and proxies) and analyzes them to detect suspicious behavior. This aligns with activities such as monitoring HTTP/HTTPS traffic and identifying anomalies in proxy logs, similar to what is achieved with mitmproxy in this tutorial.

File Integrity Monitoring (FIM) Wazuh tracks changes to critical files and directories, alerting administrators of unauthorized modifications. This feature complements backend security in TLS-based reverse proxies, where ensuring the integrity of configuration files is essential for preventing tampering.

Real-Time Threat Detection Wazuh uses rules to correlate events and trigger alerts when suspicious activity is detected, such as brute-force attacks or malware. This supports filtering and blocking malicious traffic, much like the functionality explored using mitmproxy for web proxy filtering.

Vulnerability Detection and Compliance Management Wazuh scans systems for vulnerabilities and ensures they meet compliance standards. This feature can complement TLS hardening activities in the tutorial by ensuring that servers are patched and secure, reducing exposure to attacks.



https://172.0.0.1/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0)

No results

No results were found.

Critical severity 0 Rule level 15 or higher

High severity 0 Rule level 12 to 14

Medium severity 126 Rule level 7 to 11

Low severity 105 Rule level 0 to 6

Configuration Assessment

Scan your assets as part of a configuration assessment audit.

Malware Detection

Verify that your systems are configured according to your security policies baseline.

File Integrity Monitoring

Threat Hunting

Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection

Discover what applications in your environment are affected by well-known vulnerabilities.

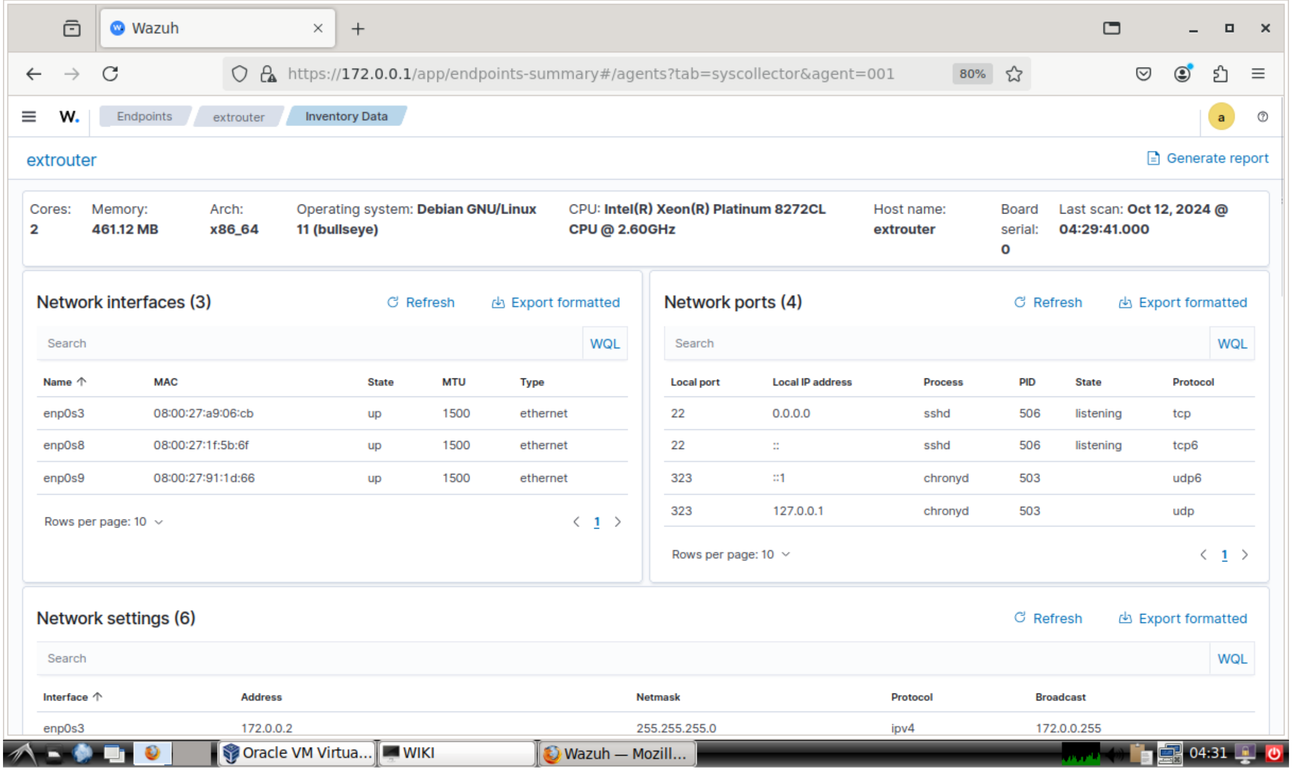
MITRE ATT&CK

Security events from the

VirusTotal

Alerts resulting from

Figure 10: Wazuh's Dashboard



extrouter

Cores: 2 | Memory: 461.12 MB | Arch: x86_64 | Operating system: Debian GNU/Linux 11 (bullseye) | CPU: Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz | Host name: extrouter | Board serial: 0 | Last scan: Oct 12, 2024 @ 04:29:41.000

Network interfaces (3)

Name ↑	MAC	State	MTU	Type
enp0s3	08:00:27:a9:06:cb	up	1500	ethernet
enp0s8	08:00:27:1f:5b:6f	up	1500	ethernet
enp0s9	08:00:27:91:1d:66	up	1500	ethernet

Rows per page: 10

Network ports (4)

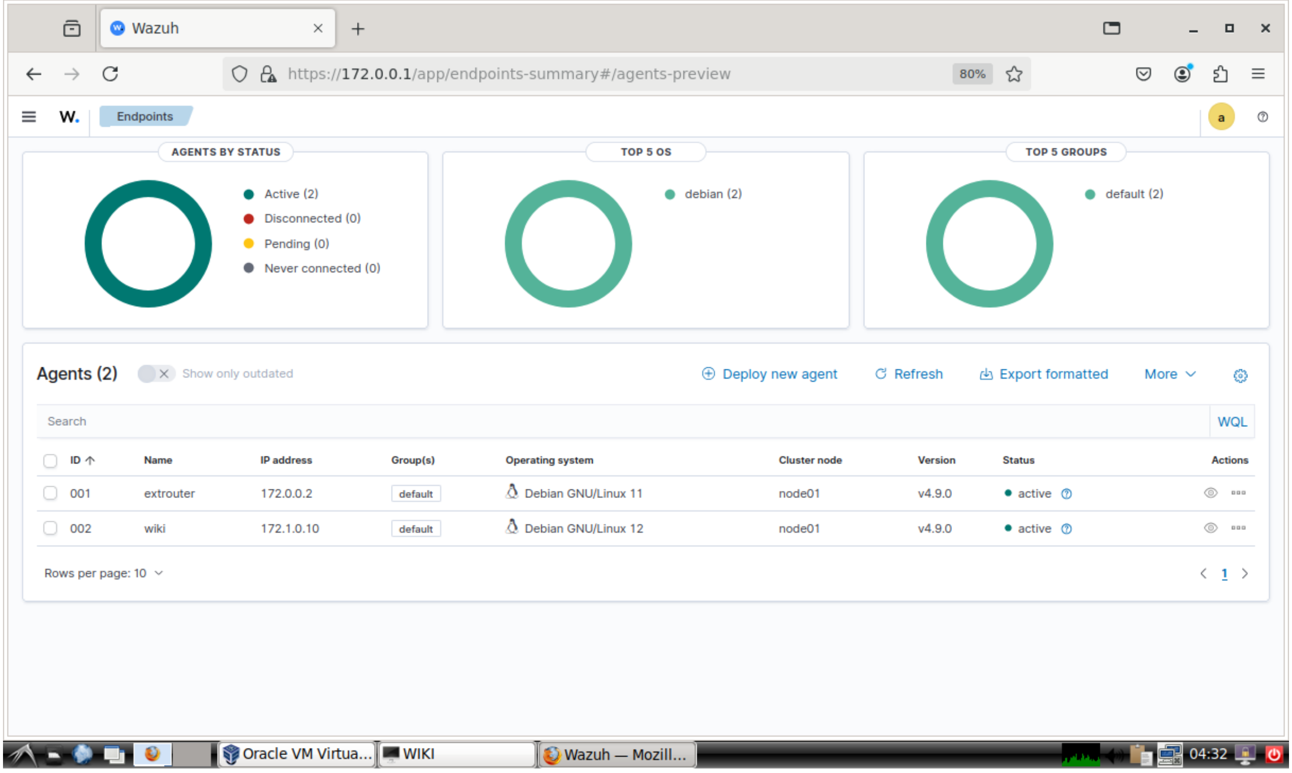
Local port	Local IP address	Process	PID	State	Protocol
22	0.0.0.0	sshd	506	listening	tcp
22	::	sshd	506	listening	tcp6
323	::1	chronyd	503		udp6
323	127.0.0.1	chronyd	503		udp

Rows per page: 10

Network settings (6)

Interface ↑	Address	Netmask	Protocol	Broadcast
enp0s3	172.0.0.2	255.255.255.0	ipv4	172.0.0.255

Figure 11: Extrouter Wazuh Details



Agents (2)

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	extrouter	172.0.0.2	default	Debian GNU/Linux 11	node01	v4.9.0	● active	
002	wiki	172.1.0.10	default	Debian GNU/Linux 12	node01	v4.9.0	● active	

Rows per page: 10

Figure 12: Multiple active agents in Wazuh (Extrouter, Wiki)

4.3 Enhancing network security with threat intelligence

Threat Intelligence and Its Role in Network Security Threat intelligence refers to the collection, analysis, and sharing of information about potential or existing threats that can target an organization's network. It helps security teams stay ahead of emerging threats by providing insights into attack vectors, malicious actors, and indicators of compromise (IOCs). This information enables proactive threat detection, mitigation, and incident response to protect the network.

MITRE ATT&CK Framework and Its Role in Threat Intelligence MITRE ATT&CK is a globally accessible, structured framework that catalogs adversary tactics, techniques, and procedures (TTPs) used by attackers across different phases of a cyberattack. It serves as a valuable threat intelligence source by detailing how attackers operate and what actions they take to compromise systems.

Detection SIEM tools like Wazuh can map incoming alerts to specific techniques described in the MITRE ATT&CK framework. This helps detect threats more accurately by identifying known behaviors such as credential dumping or phishing attacks.

Classification Security events can be classified into phases (e.g., initial access, lateral movement, privilege escalation) based on MITRE ATT&CK's catalog. This structured classification assists in understanding where the attack stands in the kill chain and helps prioritize responses.

Mitigation The framework provides actionable advice on countermeasures for each tactic and technique, helping organizations build effective defensive strategies. SIEM platforms can use this intelligence to automate threat responses or recommend specific actions to mitigate detected attacks.

4.4 Identifying network attack techniques with MITRE ATT&CK

Adversary Groups Using Password Spraying

Silent Librarian (G0122) This group targets universities, research institutes, and government agencies to steal academic data and intellectual property. They are known to have affiliations with the Iranian government, using cyber intrusions to gather sensitive information.

Leafminer (G0077) An Iranian threat group targeting government and business entities in the Middle East. They focus on exploiting vulnerabilities for espionage and persistent access to compromised systems.

Lazarus Group (G0032) A North Korean state-sponsored group linked to financial theft and destructive cyber campaigns, including major breaches like the Sony Pictures attack. They use credential-based attacks, including password spraying, to achieve access and conduct espionage or financial gain.

Mitigation Strategies for Password Spraying

Password Policies (M1027) Implementing strict password complexity policies to reduce the use of common passwords that can be easily guessed by attackers. This includes enforcing a minimum length and combination of characters.

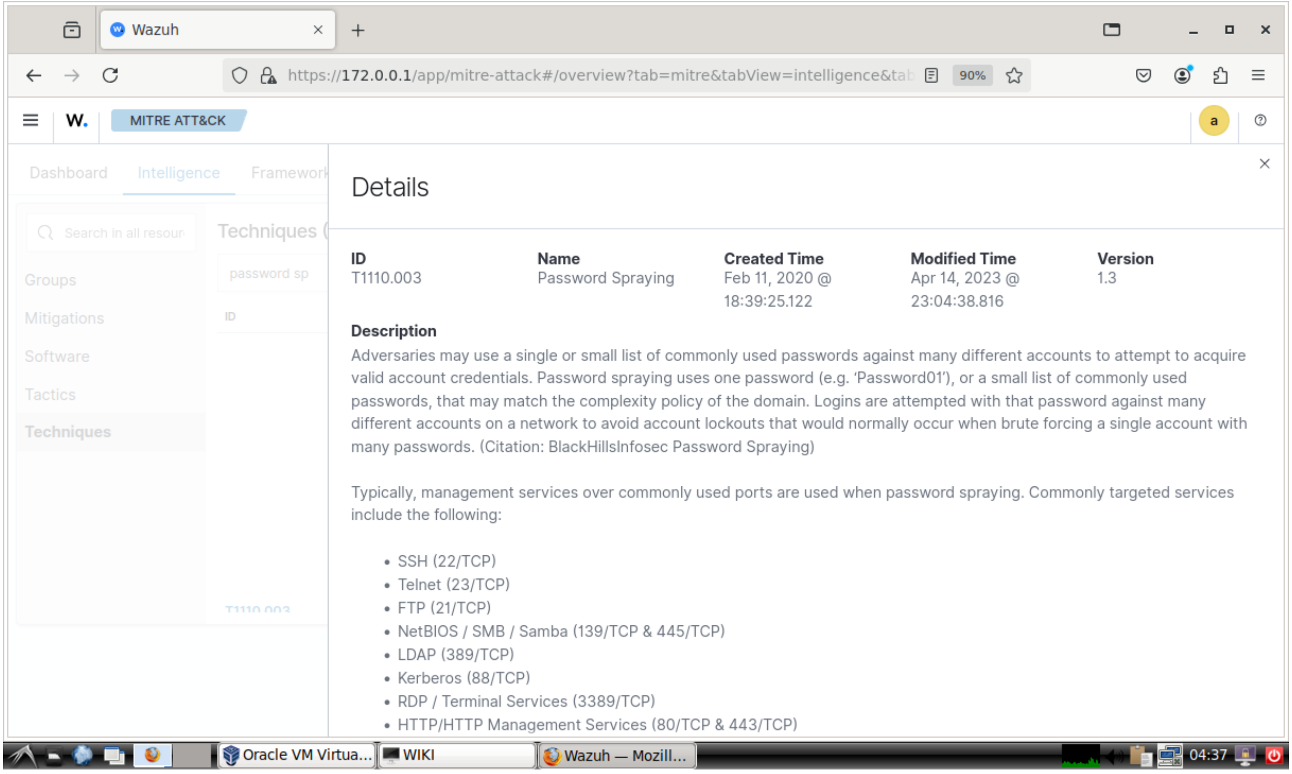
Multi-Factor Authentication (MFA) (M1032) Adding an additional layer of security, such as one-time passwords (OTPs) or hardware tokens, ensures that compromised credentials alone are not sufficient for access.

Account Use Policies (M1036) Limiting the number of login attempts and implementing account lockouts after multiple failed attempts can prevent password spraying attacks from succeeding.

Software Tools Used in Password Spraying Attacks

MailSniper (S0413) A penetration testing tool often used to search for credentials and sensitive information in Microsoft Exchange environments. It can automate password spraying against email systems to compromise accounts.

Bad Rabbit (S0606) A self-propagating ransomware that relies on credential access techniques, including password spraying, to spread across networks and systems rapidly. It is associated with attacks on transportation sectors and organizations in Eastern Europe and Russia.



Details

ID	Name	Created Time	Modified Time	Version
T1110.003	Password Spraying	Feb 11, 2020 @ 18:39:25.122	Apr 14, 2023 @ 23:04:38.816	1.3

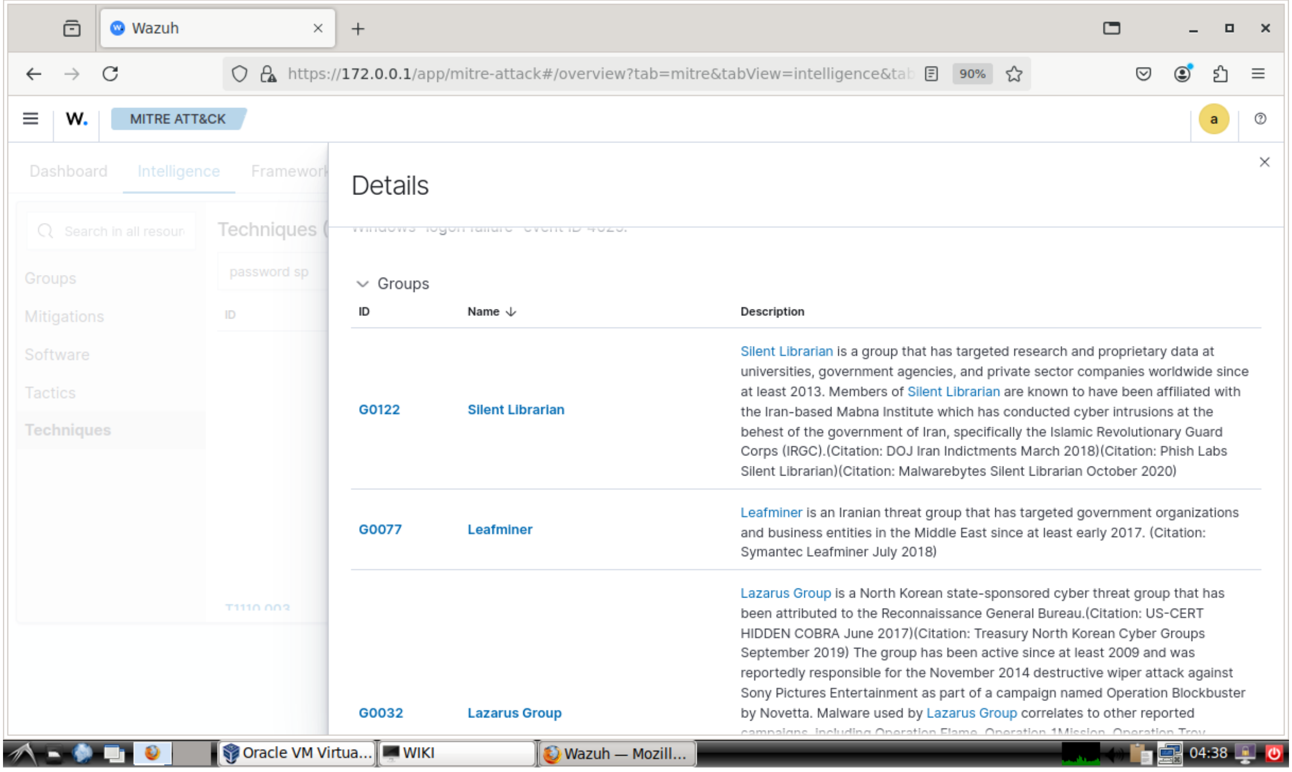
Description

Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. (Citation: BlackHillsInfosec Password Spraying)

Typically, management services over commonly used ports are used when password spraying. Commonly targeted services include the following:

- SSH (22/TCP)
- Telnet (23/TCP)
- FTP (21/TCP)
- NetBIOS / SMB / Samba (139/TCP & 445/TCP)
- LDAP (389/TCP)
- Kerberos (88/TCP)
- RDP / Terminal Services (3389/TCP)
- HTTP/HTTP Management Services (80/TCP & 443/TCP)

Figure 13: MITRE ATT&CK 1 Part 1



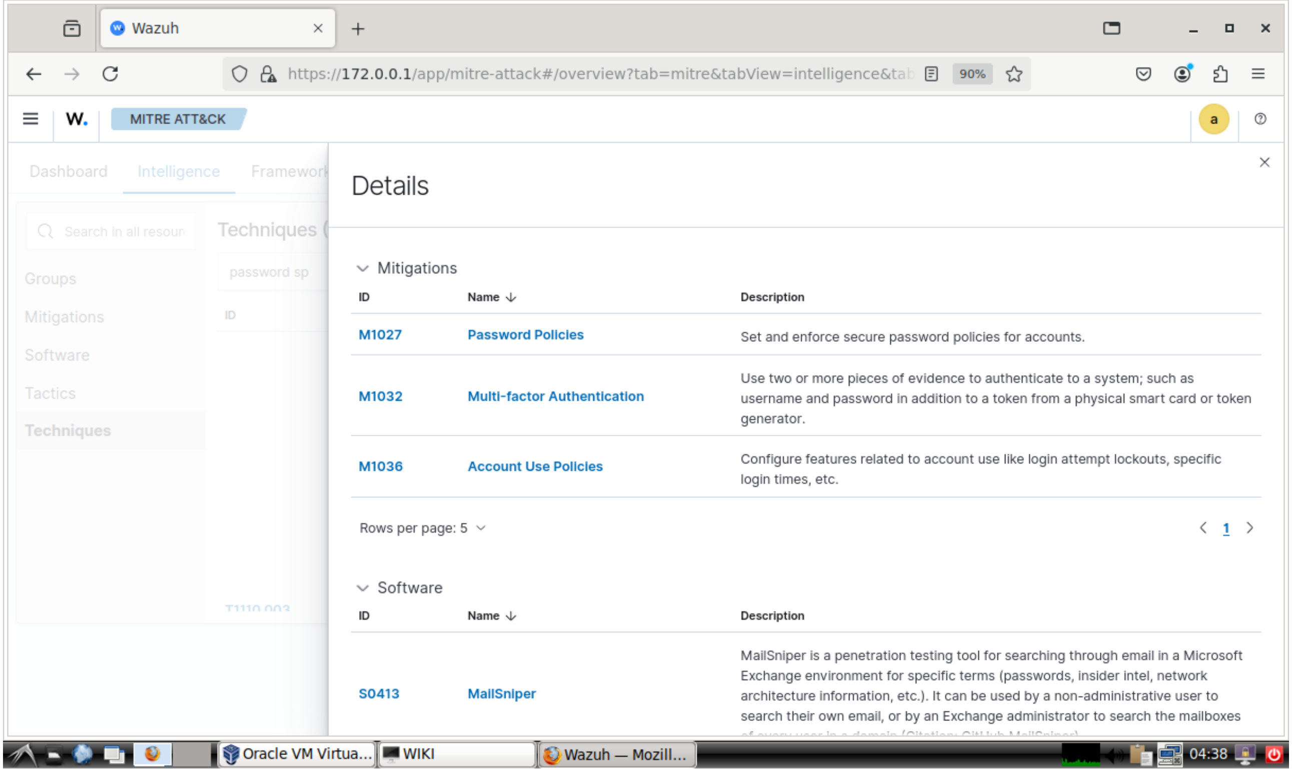
Details

Windows - logon failure - event ID 4625.

Groups

ID	Name ↓	Description
G0122	Silent Librarian	Silent Librarian is a group that has targeted research and proprietary data at universities, government agencies, and private sector companies worldwide since at least 2013. Members of Silent Librarian are known to have been affiliated with the Iran-based Mabna Institute which has conducted cyber intrusions at the behest of the government of Iran, specifically the Islamic Revolutionary Guard Corps (IRGC).(Citation: DOJ Iran Indictments March 2018)(Citation: Phish Labs Silent Librarian)(Citation: Malwarebytes Silent Librarian October 2020)
G0077	Leafminer	Leafminer is an Iranian threat group that has targeted government organizations and business entities in the Middle East since at least early 2017. (Citation: Symantec Leafminer July 2018)
G0032	Lazarus Group	Lazarus Group is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau.(Citation: US-CERT HIDDEN COBRA June 2017)(Citation: Treasury North Korean Cyber Groups September 2019) The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy

Figure 14: MITRE ATT&CK 1 Part 2



Details

Mitigations

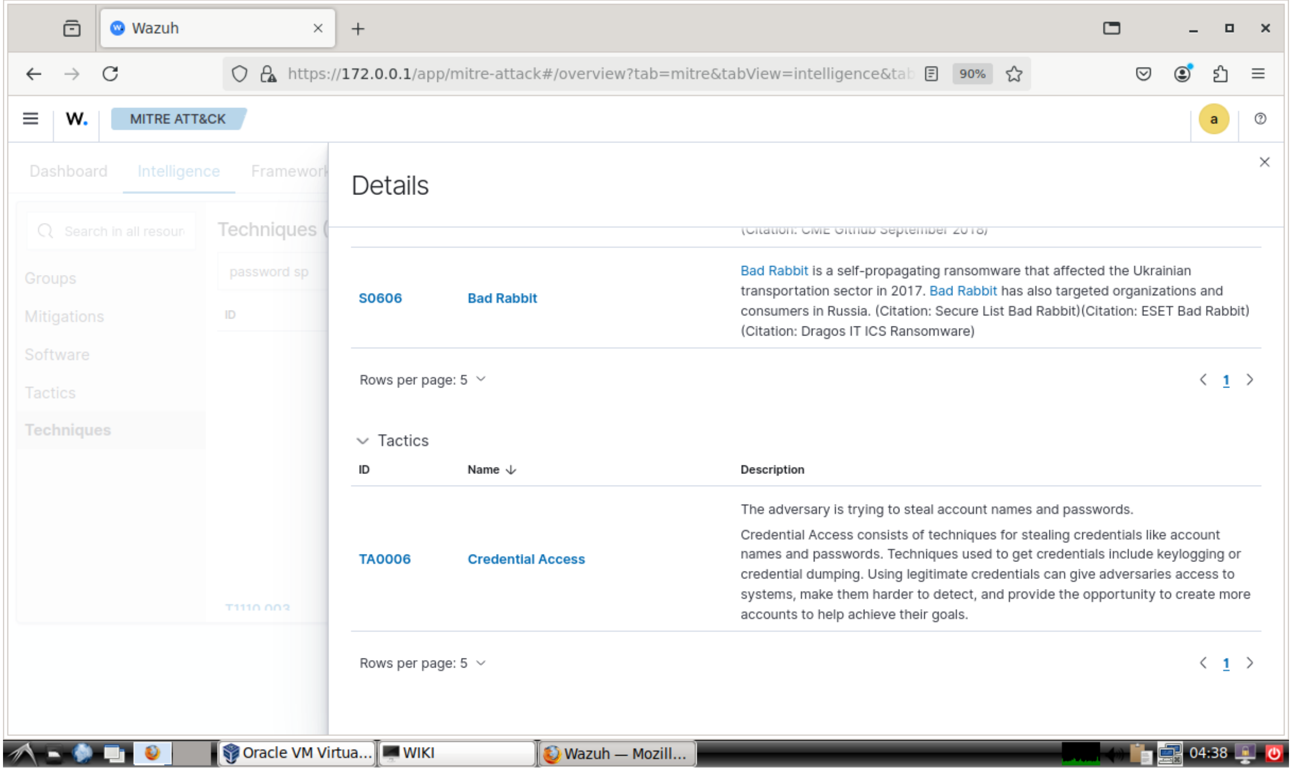
ID	Name ↓	Description
M1027	Password Policies	Set and enforce secure password policies for accounts.
M1032	Multi-factor Authentication	Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.

Rows per page: 5 ⌄ ‹ 1 ›

Software

ID	Name ↓	Description
S0413	MailSniper	MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used by a non-administrative user to search their own email, or by an Exchange administrator to search the mailboxes of every user in a domain.(Citation: GitHub MailSniper)

Figure 15: MITRE ATT&CK 1 Part 3



Details

(Citation: CME Github September 2018)

S0606	Bad Rabbit	Bad Rabbit is a self-propagating ransomware that affected the Ukrainian transportation sector in 2017. Bad Rabbit has also targeted organizations and consumers in Russia. (Citation: Secure List Bad Rabbit)(Citation: ESET Bad Rabbit)(Citation: Dragos IT ICS Ransomware)

Rows per page: 5

Tactics

ID	Name	Description
TA0006	Credential Access	The adversary is trying to steal account names and passwords. Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Rows per page: 5

Figure 16: MITRE ATT&CK 1 Part 4

Adversary Groups Using Authentication Package

No specific adversary groups There are no specific adversary groups explicitly identified associated with this technique (T1547.002 – Authentication Package). However, this attack vector is used for persistence and privilege escalation, typically by sophisticated groups looking to maintain access in compromised systems.

Mitigation Strategies For Authentication Package

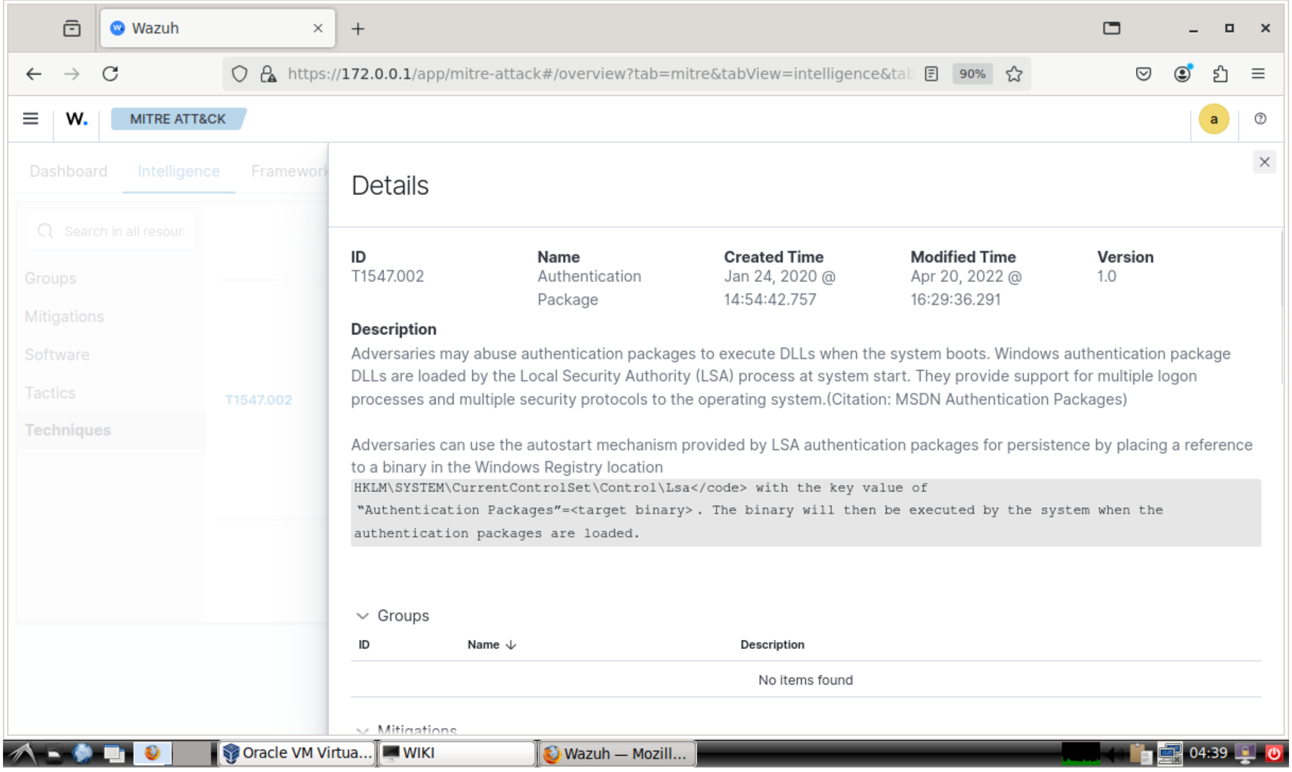
Privileged Process Integrity (M1025) Protecting processes with high privileges through mechanisms such as protected process light (PPL), anti-injection defenses, and strict enforcement of process integrity policies. This helps ensure that only trusted binaries can run with elevated privileges, reducing the risk of malicious DLLs being loaded.

Registry Monitoring Regular monitoring of Windows registry keys, especially the HKLM/ SYSTEM/ CurrentControlSet/ Control/ Lsa key, can detect unauthorized changes used to load malicious authentication packages. Alerting on suspicious modifications can help in detecting an active attack early.

Application Whitelisting Implementing application whitelisting ensures that only trusted executables can run on the system. This makes it harder for attackers to introduce malicious DLLs into the Local Security Authority (LSA) process for persistence.

Software Tools Used in Authentication Package Attack

Flame (S0143) Flame is a sophisticated malware toolkit known for collecting information from systems, primarily targeting entities in the Middle East. It exploits various techniques, including privilege escalation, to gain and maintain persistence on the victim's machine. Flame can leverage techniques such as the authentication package attack to execute code during system startup and maintain long-term access.



Details

ID	Name	Created Time	Modified Time	Version
T1547.002	Authentication Package	Jan 24, 2020 @ 14:54:42.757	Apr 20, 2022 @ 16:29:36.291	1.0

Description

Adversaries may abuse authentication packages to execute DLLs when the system boots. Windows authentication package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system.(Citation: MSDN Authentication Packages)

Adversaries can use the autostart mechanism provided by LSA authentication packages for persistence by placing a reference to a binary in the Windows Registry location

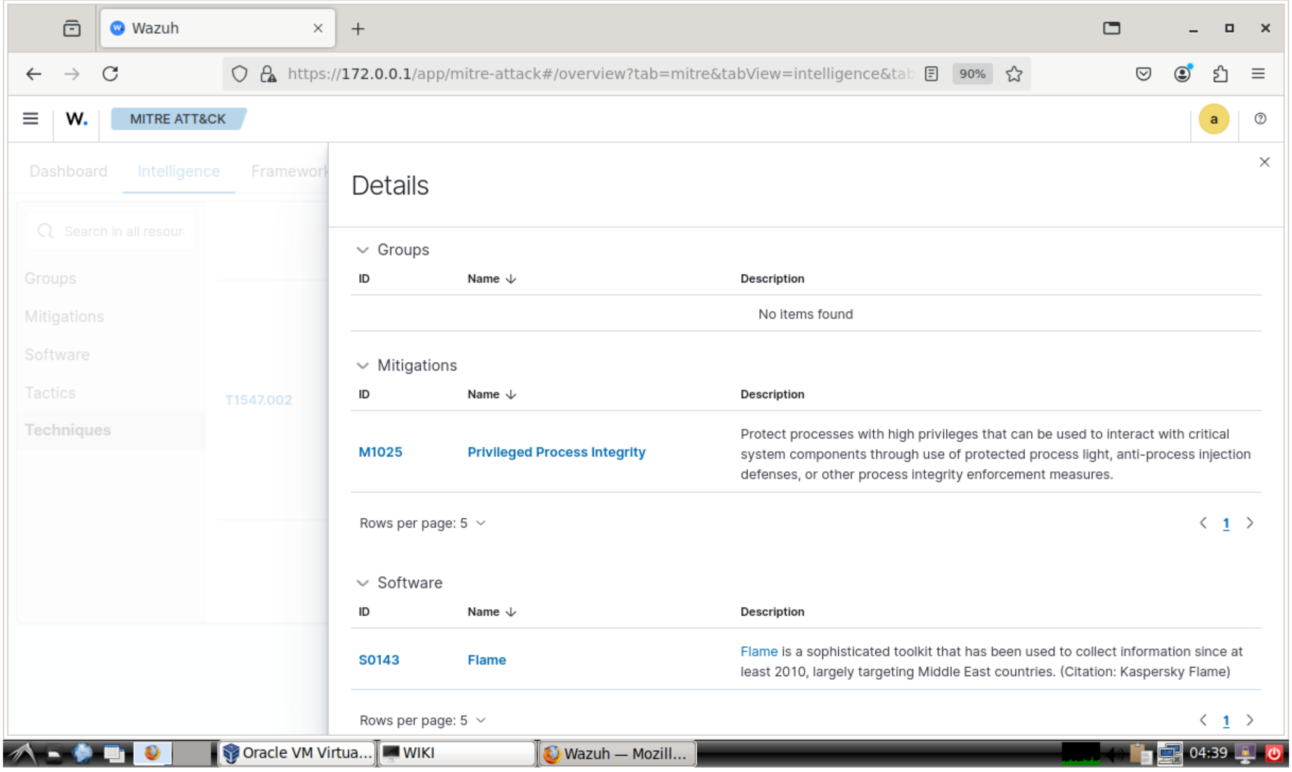
```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa</code> with the key value of
"Authentication Packages"=<target binary>. The binary will then be executed by the system when the
authentication packages are loaded.
```

Groups

ID	Name ↓	Description
	No items found	

Mitigations

Figure 17: MITRE ATT&CK 2 Part 1



Details

Groups

ID	Name ↓	Description
		No items found

Mitigations

ID	Name ↓	Description
M1025	Privileged Process Integrity	Protect processes with high privileges that can be used to interact with critical system components through use of protected process light, anti-process injection defenses, or other process integrity enforcement measures.

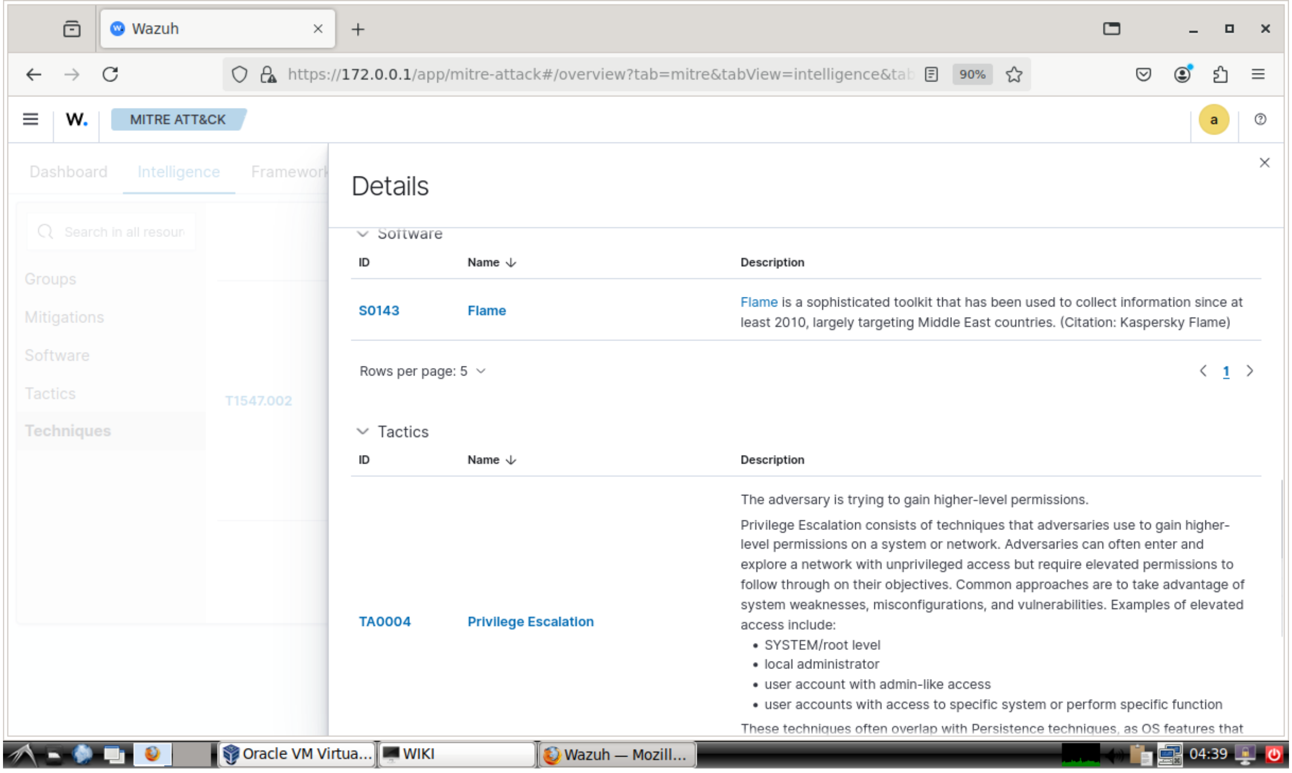
Rows per page: 5

Software

ID	Name ↓	Description
S0143	Flame	Flame is a sophisticated toolkit that has been used to collect information since at least 2010, largely targeting Middle East countries. (Citation: Kaspersky Flame)

Rows per page: 5

Figure 18: MITRE ATT&CK 2 Part 2



Details

Software

ID	Name ↓	Description
S0143	Flame	Flame is a sophisticated toolkit that has been used to collect information since at least 2010, largely targeting Middle East countries. (Citation: Kaspersky Flame)

Rows per page: 5

Tactics

ID	Name ↓	Description
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions. Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include: • SYSTEM/root level • local administrator • user account with admin-like access • user accounts with access to specific system or perform specific function These techniques often overlap with Persistence techniques, as OS features that

Figure 19: MITRE ATT&CK 2 Part 3

4.5 Complementary Control to SIEM and Threat Intel

A complementary control to SIEM and threat intelligence is Endpoint Detection and Response (EDR), which provides real-time monitoring and threat detection at the endpoint level. While

SIEM aggregates and correlates logs from across the network, EDR focuses on identifying suspicious behavior on individual devices, such as malware infections or unauthorized access attempts. EDR integrates with SIEM by feeding detailed endpoint data and alerts, enhancing visibility and enabling faster incident response. Additionally, EDR leverages threat intelligence to detect known indicators of compromise (IOCs) and can automatically contain threats by isolating compromised endpoints, creating a more comprehensive security framework. Together, SIEM, EDR, and threat intelligence ensure robust, multi-layered protection across both networks and endpoints.