SURICATA IDS/IPS INSTALLATION AND DETECTION RULES CREATION

This document demonstrates the installation of the Suricata IDS/IPS platform as well as the creation of detection rules to notify when malicious activities occur on the network

Jordan Patterson

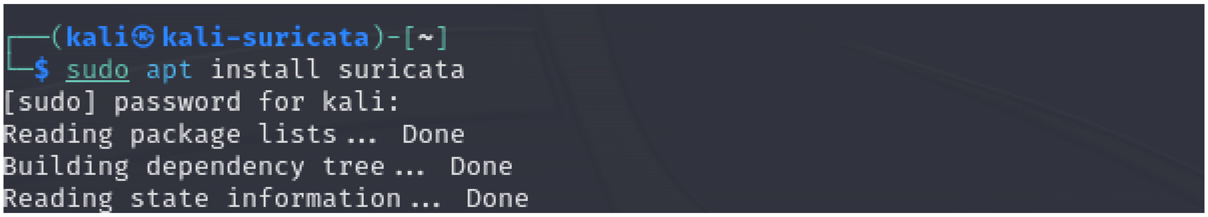
2024

Installation of Suricata IDS/IPS and the creation of detection rules

Jordan Patterson 2024

Installation:

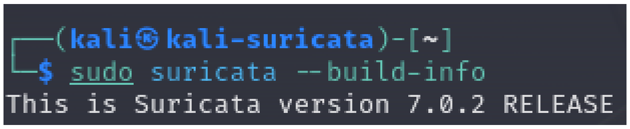
I used the command *sudo apt install suricata* to install suricata.



```
┌──(kali㉿kali-suricata)-[~]
└─$ sudo apt install suricata
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Verify Suricata version:

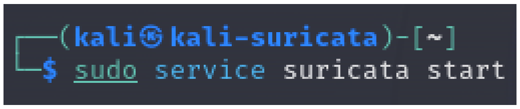
I used the command *sudo suricata –build-info* to ensure that the correct version of Suricata installed successfully.



```
┌──(kali㉿kali-suricata)-[~]
└─$ sudo suricata --build-info
This is Suricata version 7.0.2 RELEASE
```

Start Service:

I used the command *sudo service suricata start* to start the service.



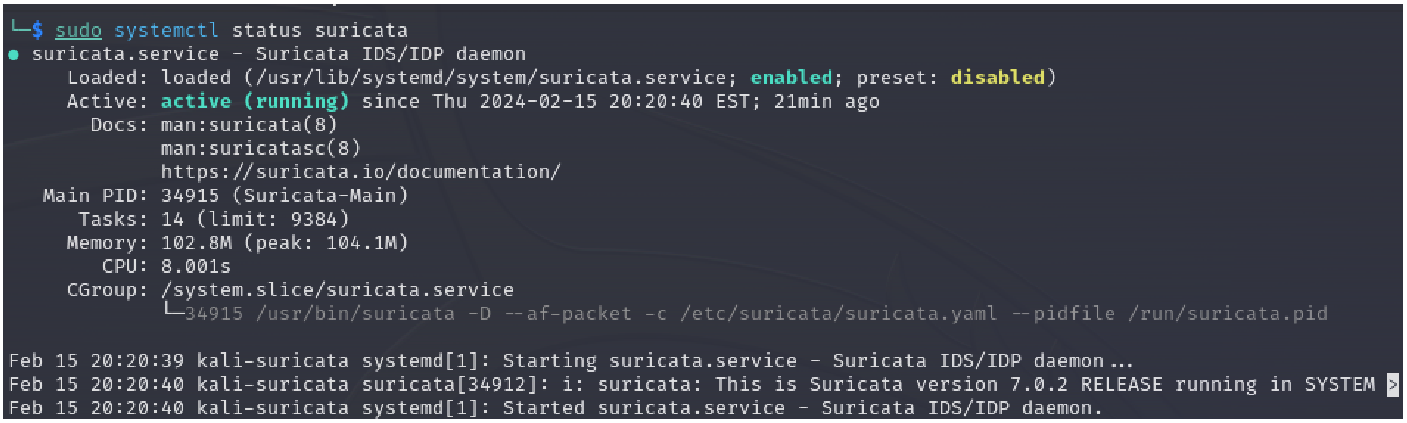
```
┌──(kali㉿kali-suricata)-[~]
└─$ sudo service suricata start
```

Installation of Suricata IDS/IPS and the creation of detection rules

Jordan Patterson 2024

Verify Suricata service status:

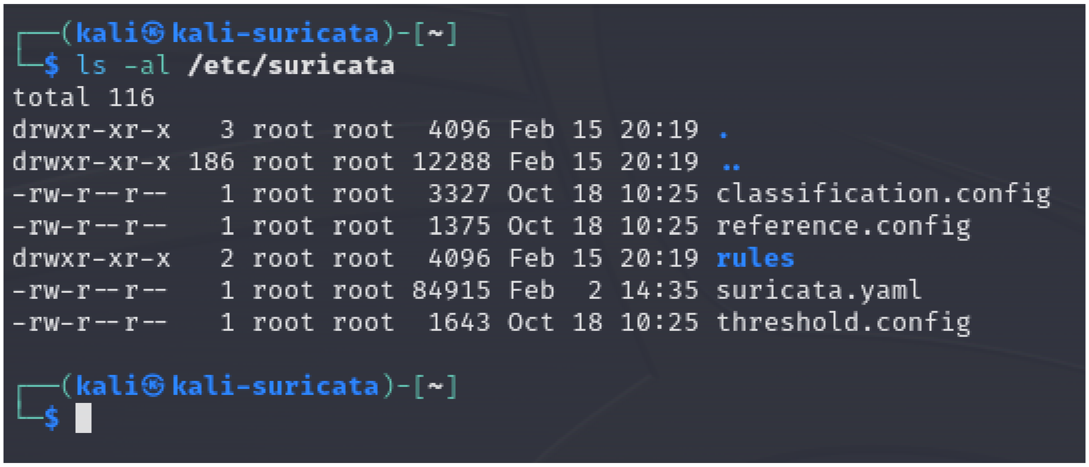
I used the command *systemctl status suricata* to verify that the service was running.



```
└─$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: disabled)
     Active: active (running) since Thu 2024-02-15 20:20:40 EST; 21min ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
   Main PID: 34915 (Suricata-Main)
      Tasks: 14 (limit: 9384)
     Memory: 102.8M (peak: 104.1M)
        CPU: 8.001s
     CGroup: /system.slice/suricata.service
             └─34915 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Feb 15 20:20:39 kali-suricata systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Feb 15 20:20:40 kali-suricata suricata[34912]: i: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM >
Feb 15 20:20:40 kali-suricata systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
```

View Suricata directory:

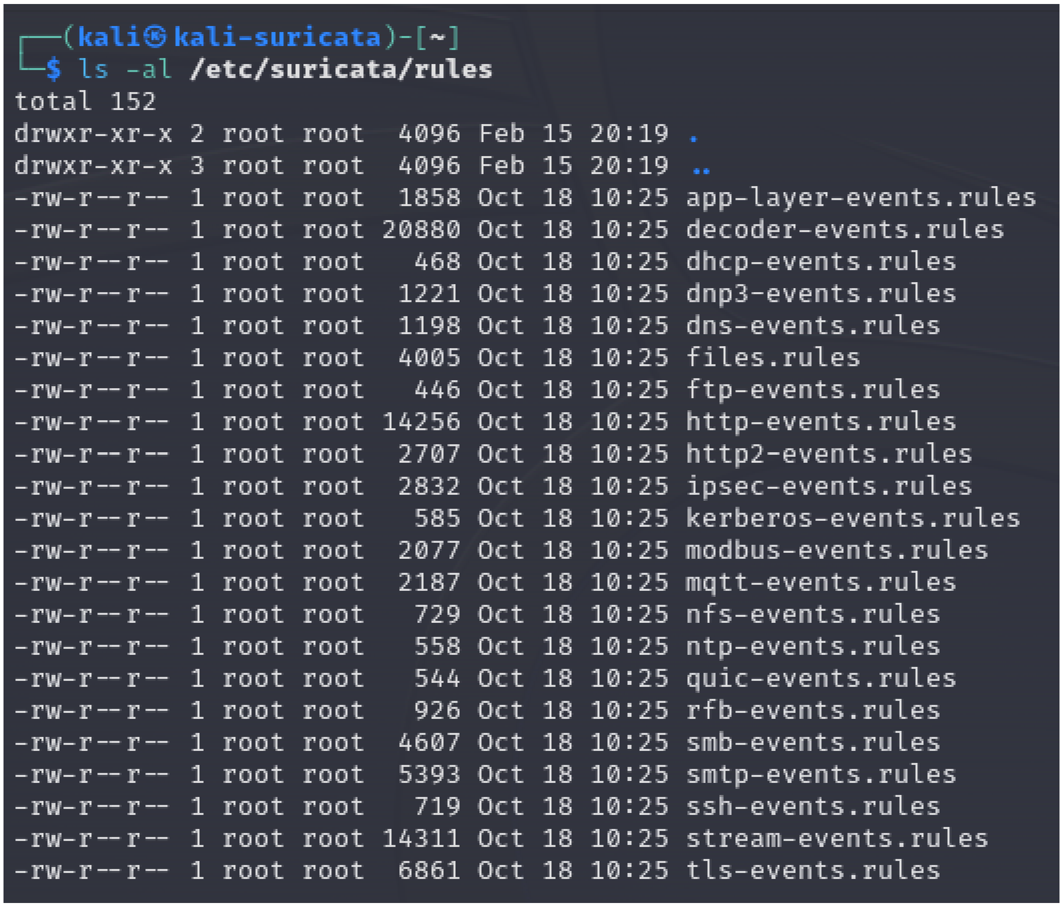
I viewed the Suricata directory.



```
┌──(kali㉿kali-suricata)-[~]
└─$ ls -al /etc/suricata
total 116
drwxr-xr-x   3 root root  4096 Feb 15 20:19 .
drwxr-xr-x 186 root root 12288 Feb 15 20:19 ..
-rw-r--r--   1 root root  3327 Oct 18 10:25 classification.config
-rw-r--r--   1 root root  1375 Oct 18 10:25 reference.config
drwxr-xr-x   2 root root  4096 Feb 15 20:19 rules
-rw-r--r--   1 root root 84915 Feb  2 14:35 suricata.yaml
-rw-r--r--   1 root root  1643 Oct 18 10:25 threshold.config

┌──(kali㉿kali-suricata)-[~]
└─$ 
```

View Suricata rules:

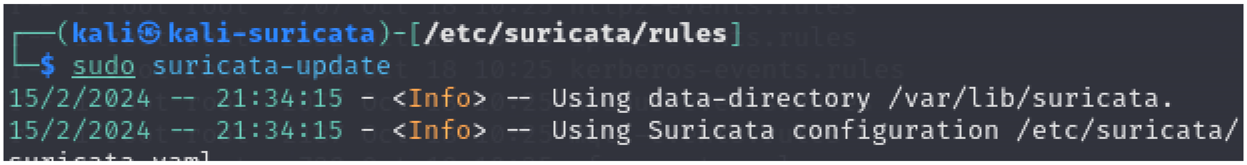
I viewed the Suricata rules directory and its contents.



```
┌──(kali㉿kali-suricata)-[~]
└─$ ls -al /etc/suricata/rules
total 152
drwxr-xr-x 2 root root  4096 Feb 15 20:19 .
drwxr-xr-x 3 root root  4096 Feb 15 20:19 ..
-rw-r--r-- 1 root root  1858 Oct 18 10:25 app-layer-events.rules
-rw-r--r-- 1 root root 20880 Oct 18 10:25 decoder-events.rules
-rw-r--r-- 1 root root   468 Oct 18 10:25 dhcp-events.rules
-rw-r--r-- 1 root root  1221 Oct 18 10:25 dnp3-events.rules
-rw-r--r-- 1 root root  1198 Oct 18 10:25 dns-events.rules
-rw-r--r-- 1 root root  4005 Oct 18 10:25 files.rules
-rw-r--r-- 1 root root   446 Oct 18 10:25 ftp-events.rules
-rw-r--r-- 1 root root 14256 Oct 18 10:25 http-events.rules
-rw-r--r-- 1 root root  2707 Oct 18 10:25 http2-events.rules
-rw-r--r-- 1 root root  2832 Oct 18 10:25 ipsec-events.rules
-rw-r--r-- 1 root root   585 Oct 18 10:25 kerberos-events.rules
-rw-r--r-- 1 root root  2077 Oct 18 10:25 modbus-events.rules
-rw-r--r-- 1 root root  2187 Oct 18 10:25 mqtt-events.rules
-rw-r--r-- 1 root root   729 Oct 18 10:25 nfs-events.rules
-rw-r--r-- 1 root root   558 Oct 18 10:25 ntp-events.rules
-rw-r--r-- 1 root root   544 Oct 18 10:25 quic-events.rules
-rw-r--r-- 1 root root   926 Oct 18 10:25 rfb-events.rules
-rw-r--r-- 1 root root  4607 Oct 18 10:25 smb-events.rules
-rw-r--r-- 1 root root  5393 Oct 18 10:25 smtp-events.rules
-rw-r--r-- 1 root root   719 Oct 18 10:25 ssh-events.rules
-rw-r--r-- 1 root root 14311 Oct 18 10:25 stream-events.rules
-rw-r--r-- 1 root root  6861 Oct 18 10:25 tls-events.rules
```

Update Suricata/download rules:

I updated Suricata and ensured all up to date rules were downloaded.



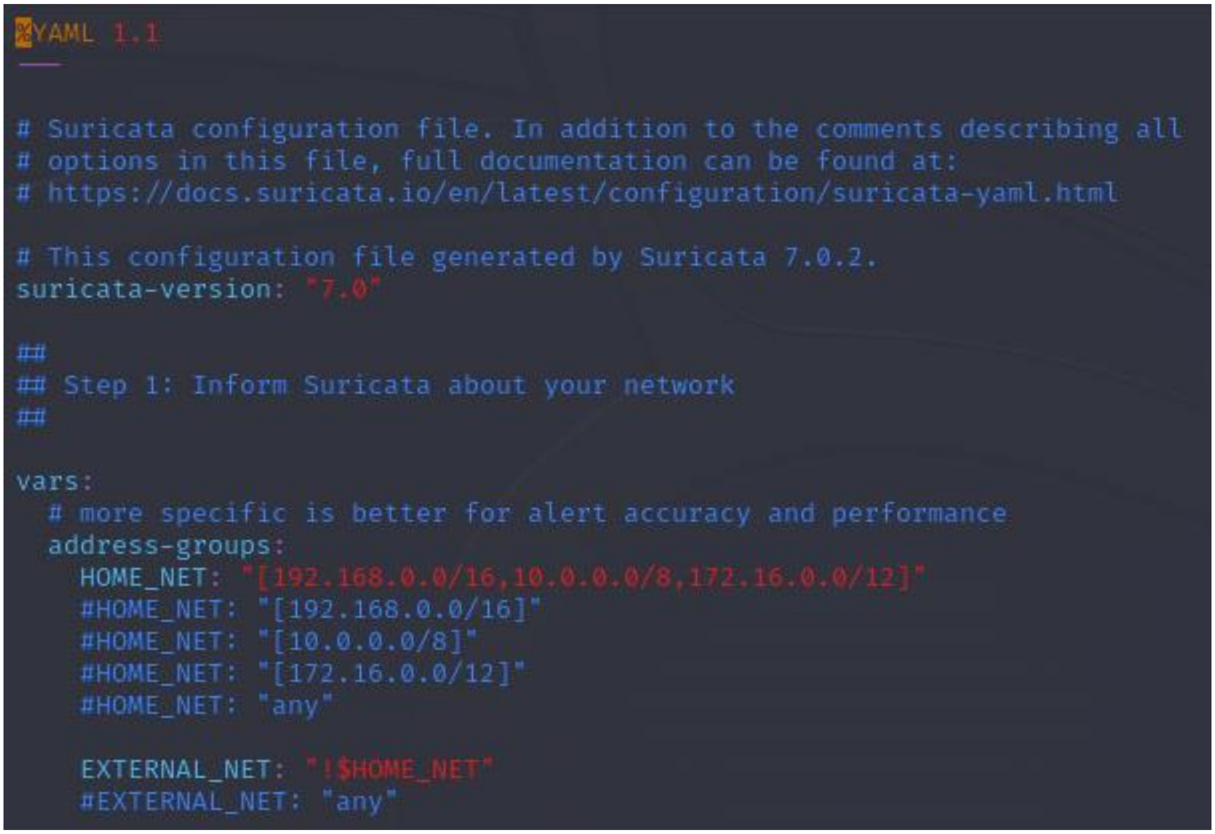
```
┌──(kali㉿kali-suricata)-[/etc/suricata/rules]
└─$ sudo suricata-update
15/2/2024 -- 21:34:15 - <Info> -- Using data-directory /var/lib/suricata.
15/2/2024 -- 21:34:15 - <Info> -- Using Suricata configuration /etc/suricata/
suricata.yaml
```

Installation of Suricata IDS/IPS and the creation of detection rules

Jordan Patterson 2024

Editing the Suricata .yaml file:

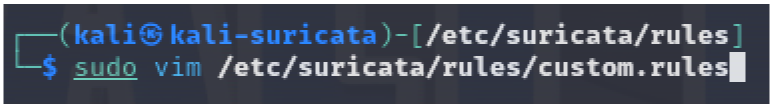
I inspected the Suricata .yaml file and added in my own custom rules file which I named “custom.rules”



```
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.2.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"
```

Modify custom rules file that I created:

I opened my custom rules file in VIM



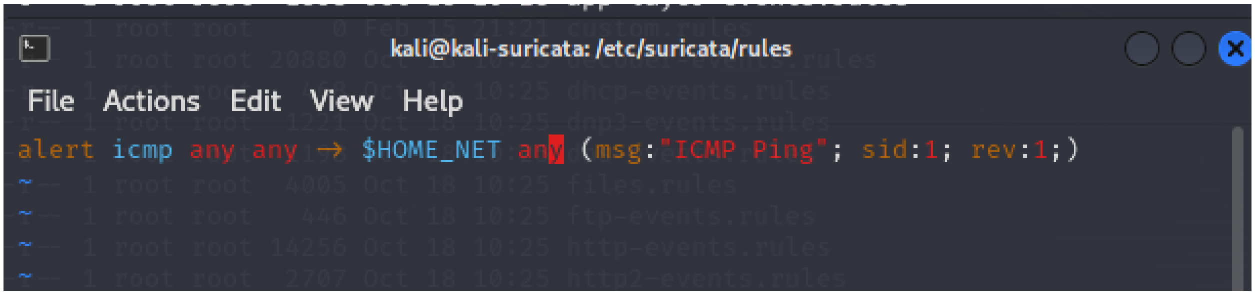
```
┌──(kali㉿kali-suricata)-[/etc/suricata/rules]
└─$ sudo vim /etc/suricata/rules/custom.rules
```

Installation of Suricata IDS/IPS and the creation of detection rules

Jordan Patterson 2024

Create custom rule:

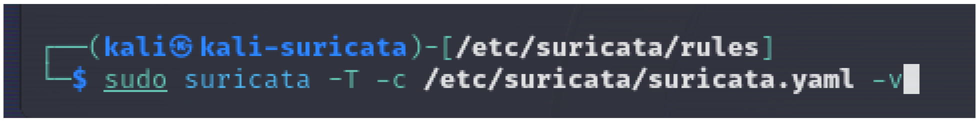
I began to create custom rules.



```
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping"; sid:1; rev:1;)
~
~
~
~
```

Test that my rules load correctly in Suricata:

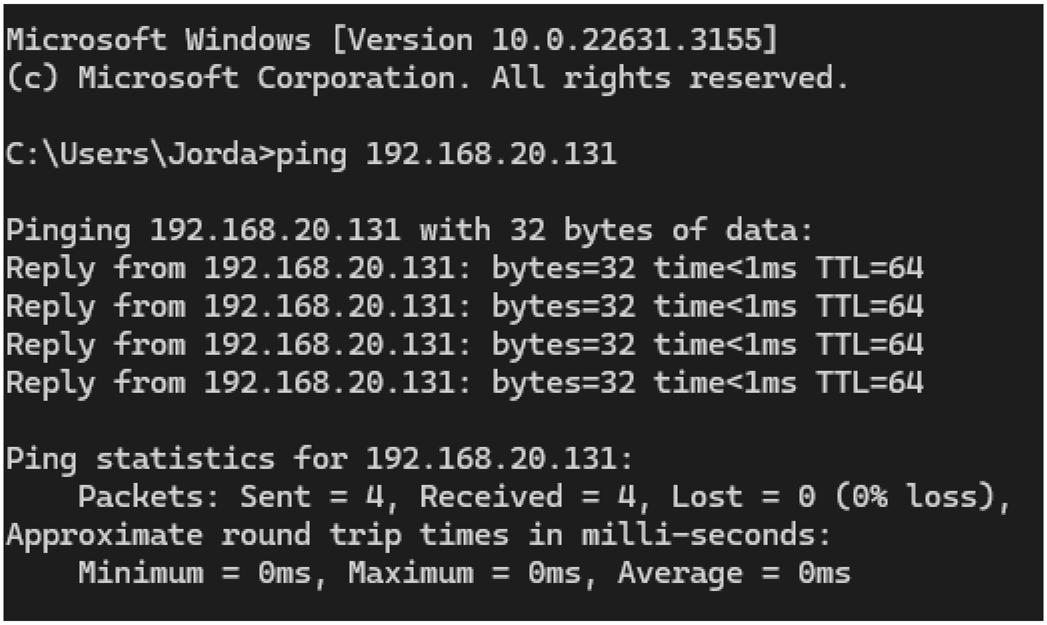
This command will tell me if there are any basic errors in my custom rules.



```
┌──(kali㉿kali-suricata)-[/etc/suricata/rules]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
```

Testing rule from local machine:

I sent a ping from my host machine to trigger the alert that I created.



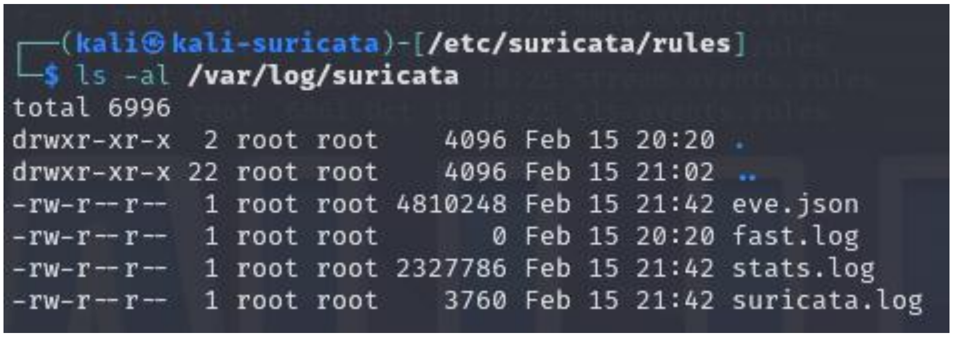
```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Jorda>ping 192.168.20.131

Pinging 192.168.20.131 with 32 bytes of data:
Reply from 192.168.20.131: bytes=32 time<1ms TTL=64
Reply from 192.168.20.131: bytes=32 time<1ms TTL=64
Reply from 192.168.20.131: bytes=32 time<1ms TTL=64
Reply from 192.168.20.131: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.20.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Installation of Suricata IDS/IPS and the creation of detection rules

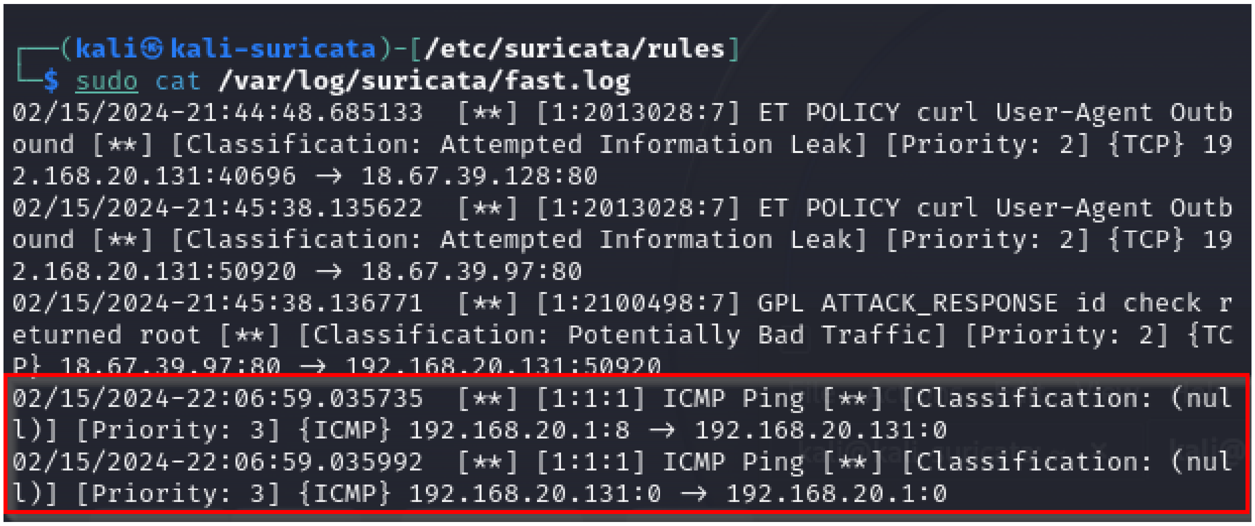
Jordan Patterson 2024

Suricata log directory review:

I opened the logs directory and opened the fast.log file. I found that my rule worked and alerted that a Ping came from an external device (my host machine).



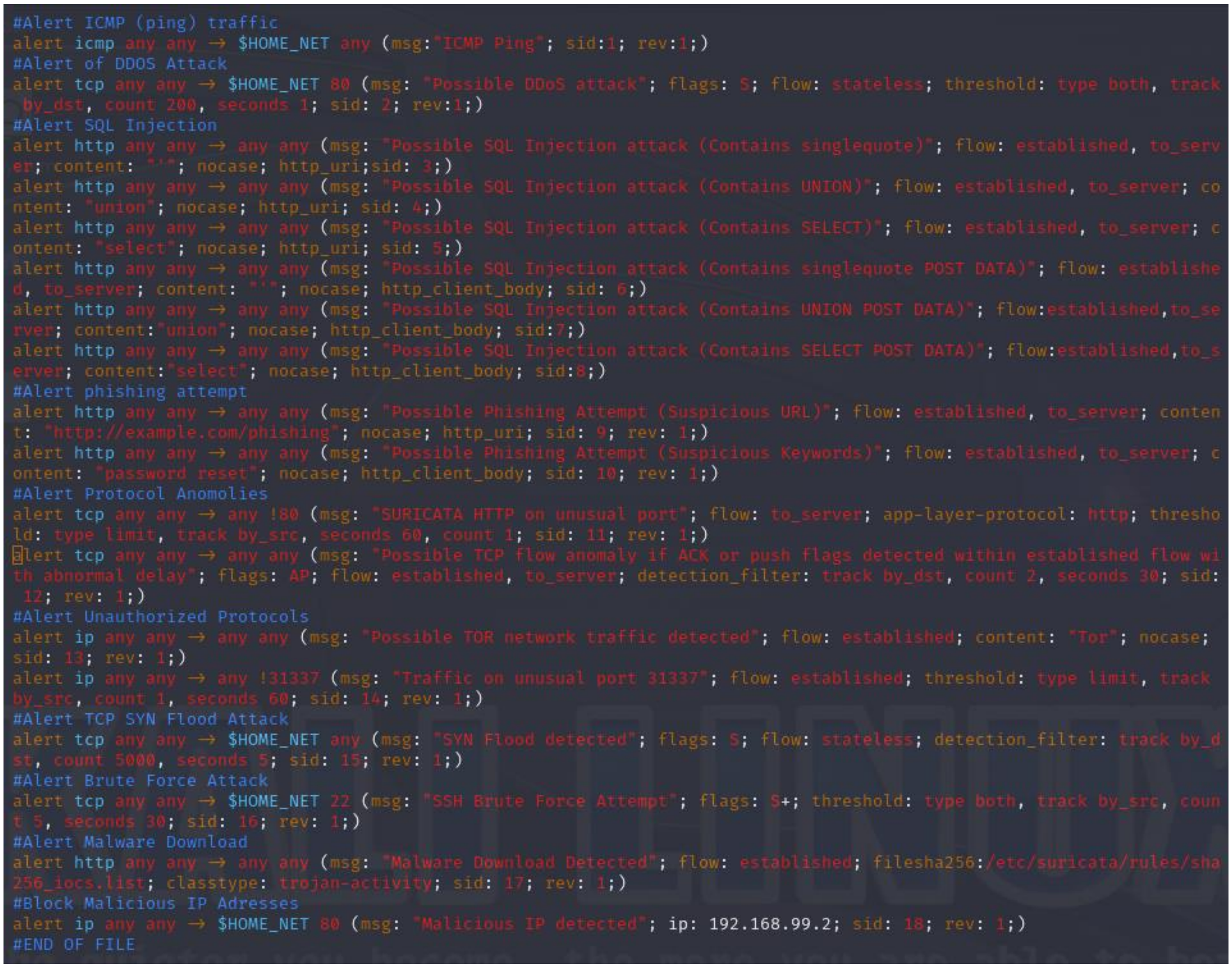
```
┌──(kali㉿kali-suricata)-[/etc/suricata/rules]
└─$ ls -al /var/log/suricata
total 6996
drwxr-xr-x  2 root root    4096 Feb 15 20:20 .
drwxr-xr-x 22 root root    4096 Feb 15 21:02 ..
-rw-r--r--  1 root root 4810248 Feb 15 21:42 eve.json
-rw-r--r--  1 root root       0 Feb 15 20:20 fast.log
-rw-r--r--  1 root root 2327786 Feb 15 21:42 stats.log
-rw-r--r--  1 root root    3760 Feb 15 21:42 suricata.log
```



```
┌──(kali㉿kali-suricata)-[/etc/suricata/rules]
└─$ sudo cat /var/log/suricata/fast.log
02/15/2024-21:44:48.685133  [**] [1:2013028:7] ET POLICY curl User-Agent Outb
ound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 19
2.168.20.131:40696 → 18.67.39.128:80
02/15/2024-21:45:38.135622  [**] [1:2013028:7] ET POLICY curl User-Agent Outb
ound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 19
2.168.20.131:50920 → 18.67.39.97:80
02/15/2024-21:45:38.136771  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check r
eturned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TC
P} 18.67.39.97:80 → 192.168.20.131:50920
02/15/2024-22:06:59.035735  [**] [1:1:1] ICMP Ping [**] [Classification: (nul
l)] [Priority: 3] {ICMP} 192.168.20.1:8 → 192.168.20.131:0
02/15/2024-22:06:59.035992  [**] [1:1:1] ICMP Ping [**] [Classification: (nul
l)] [Priority: 3] {ICMP} 192.168.20.131:0 → 192.168.20.1:0
```

IDS/IPS Rules

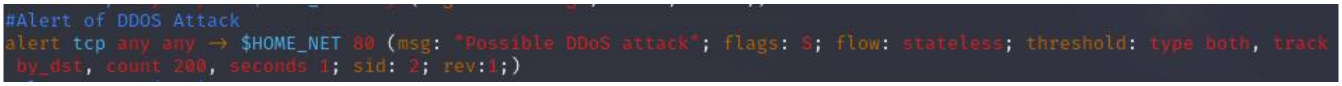
Screenshot of all rules that I created:



```
#Alert ICMP (ping) traffic
alert icmp any any → $HOME_NET any (msg:"ICMP Ping"; sid:1; rev:1;)
#Alert of DDOS Attack
alert tcp any any → $HOME_NET 80 (msg: "Possible DDoS attack"; flags: S; flow: stateless; threshold: type both, track
 by_dst, count 200, seconds 1; sid: 2; rev:1;)
#Alert SQL Injection
alert http any any → any any (msg: "Possible SQL Injection attack (Contains singlequote)"; flow: established, to_serv
er; content: "'"; nocase; http_uri;sid: 3;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains UNION)"; flow: established, to_server; co
ntent: "union"; nocase; http_uri; sid: 4;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains SELECT)"; flow: established, to_server; c
ontent: "select"; nocase; http_uri; sid: 5;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains singlequote POST DATA)"; flow: establishe
d, to_server; content: "'"; nocase; http_client_body; sid: 6;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains UNION POST DATA)"; flow:established,to_se
rver; content:"union"; nocase; http_client_body; sid:7;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains SELECT POST DATA)"; flow:established,to_s
erver; content:"select"; nocase; http_client_body; sid:8;)
#Alert phishing attempt
alert http any any → any any (msg: "Possible Phishing Attempt (Suspicious URL)"; flow: established, to_server; conten
t: "http://example.com/phishing"; nocase; http_uri; sid: 9; rev: 1;)
alert http any any → any any (msg: "Possible Phishing Attempt (Suspicious Keywords)"; flow: established, to_server; c
ontent: "password reset"; nocase; http_client_body; sid: 10; rev: 1;)
#Alert Protocol Anomolies
alert tcp any any → any !80 (msg: "SURICATA HTTP on unusual port"; flow: to_server; app-layer-protocol: http; thresho
ld: type limit, track by_src, seconds 60, count 1; sid: 11; rev: 1;)
alert tcp any any → any any (msg: "Possible TCP flow anomaly if ACK or push flags detected within established flow wi
th abnormal delay"; flags: AP; flow: established, to_server; detection_filter: track by_dst, count 2, seconds 30; sid:
 12; rev: 1;)
#Alert Unauthorized Protocols
alert ip any any → any any (msg: "Possible TOR network traffic detected"; flow: established; content: "Tor"; nocase;
sid: 13; rev: 1;)
alert ip any any → any !31337 (msg: "Traffic on unusual port 31337"; flow: established; threshold: type limit, track
by_src, count 1, seconds 60; sid: 14; rev: 1;)
#Alert TCP SYN Flood Attack
alert tcp any any → $HOME_NET any (msg: "SYN Flood detected"; flags: S; flow: stateless; detection_filter: track by_d
st, count 5000, seconds 5; sid: 15; rev: 1;)
#Alert Brute Force Attack
alert tcp any any → $HOME_NET 22 (msg: "SSH Brute Force Attempt"; flags: S+; threshold: type both, track by_src, coun
t 5, seconds 30; sid: 16; rev: 1;)
#Alert Malware Download
alert http any any → any any (msg: "Malware Download Detected"; flow: established; filesha256:/etc/suricata/rules/sha
256_iocs.list; classtype: trojan-activity; sid: 17; rev: 1;)
#Block Malicious IP Adresses
alert ip any any → $HOME_NET 80 (msg: "Malicious IP detected"; ip: 192.168.99.2; sid: 18; rev: 1;)
#END OF FILE
```

1. **Detect DDOS attack:**

   This rule will alert me if there is a DDOS attack if there are 200 or more SYN tcp packets in a second.

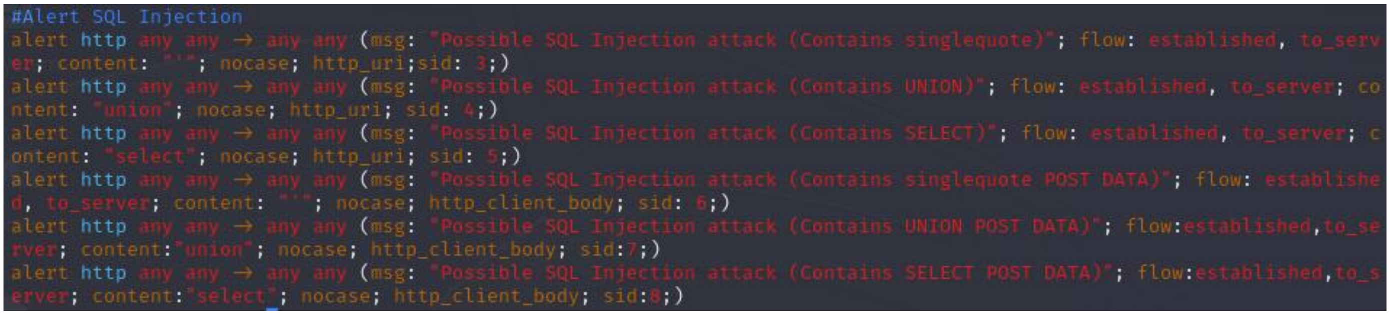


```
#Alert of DDOS Attack
alert tcp any any → $HOME_NET 80 (msg: "Possible DDoS attack"; flags: S; flow: stateless; threshold: type both, track
 by_dst, count 200, seconds 1; sid: 2; rev:1;)
```

alert tcp any any -> $HOME_NET 80 (msg: "Possible DDoS attack"; flags: S; flow: stateless; threshold: type both, track by_dst, count 200, seconds 1; sid: 2; rev: 1;)

2. **Detect SQL injection:**

   This set of rules will alert me if a SQL injection is attempted.



```
#Alert SQL Injection
alert http any any → any any (msg: "Possible SQL Injection attack (Contains singlequote)"; flow: established, to_server; content: "'"; nocase; http_uri;sid: 3;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains UNION)"; flow: established, to_server; content: "union"; nocase; http_uri; sid: 4;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains SELECT)"; flow: established, to_server; content: "select"; nocase; http_uri; sid: 5;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains singlequote POST DATA)"; flow: established, to_server; content: "'"; nocase; http_client_body; sid: 6;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains UNION POST DATA)"; flow:established,to_server; content:"union"; nocase; http_client_body; sid:7;)
alert http any any → any any (msg: "Possible SQL Injection attack (Contains SELECT POST DATA)"; flow:established,to_server; content:"select"; nocase; http_client_body; sid:8;)
```

alert http any any -> any any (msg: "Possible SQL Injection attack (Contains singlequote)"; flow: established, to_server; content: """; nocase; http_uri; sid: 3;)

alert http any any -> any any (msg: "Possible SQL Injection attack (Contains UNION)"; flow: established, to_server; content: "union"; nocase; http_uri; sid: 4;)

alert http any any -> any any (msg: "Possible SQL Injection attack (Contains SELECT)"; flow: established, to_server; content: "select"; nocase; http_uri; sid: 5;)

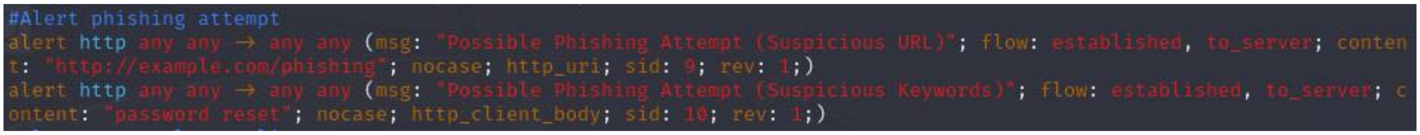
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains singlequote POST DATA)"; flow: established, to_server; content: """; nocase; http_client_body; sid: 6;)

alert http any any -> any any (msg: "Possible SQL Injection attack (Contains UNION POST DATA)"; flow: established, to_server; content: "union"; nocase; http_client_body; sid: 7;)

alert http any any -> any any (msg: "Possible SQL Injection attack (Contains SELECT POST DATA)"; flow: established, to_server; content: "select"; nocase; http_client_body; sid: 8;)

3. **Detect Phishing Attempts:**

   These two rules will alert me if a phishing attempt is attempted. If the email contains a malicious URL or a key word such as “password rest”, a notification will be logged.



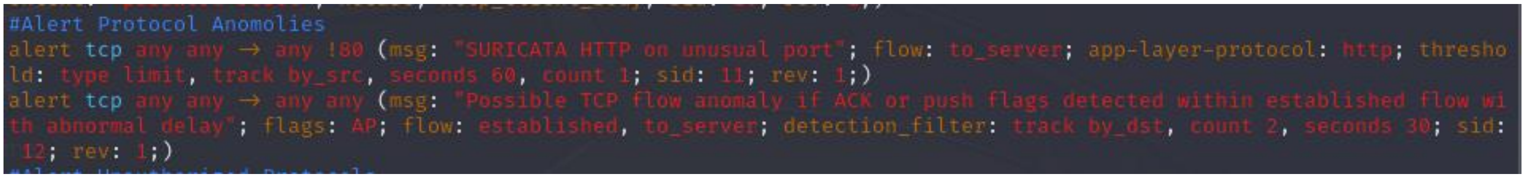
```
#Alert phishing attempt
alert http any any → any any (msg: "Possible Phishing Attempt (Suspicious URL)"; flow: established, to_server; conten
t: "http://example.com/phishing"; nocase; http_uri; sid: 9; rev: 1;)
alert http any any → any any (msg: "Possible Phishing Attempt (Suspicious Keywords)"; flow: established, to_server; c
ontent: "password reset"; nocase; http_client_body; sid: 10; rev: 1;)
```

alert http any any -> any any (msg: "Possible Phishing Attempt (Suspicious URL)"; flow: established, to_server; content: "http://example.com/phishing"; nocase; http_uri; sid: 9; rev: 1;)

alert http any any -> any any (msg: "Possible Phishing Attempt (Suspicious Keywords)"; flow: established, to_server; content: "password reset"; nocase; http_client_body; sid: 10; rev: 1;)

4. **Detect Protocol Anomalies**:

   These rules will alert me if there are anomalies such as http traffic coming in through a port that is not port 80.



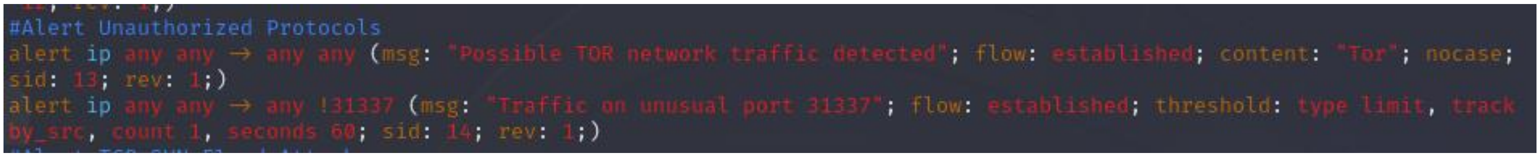
```
#Alert Protocol Anomolies
alert tcp any any → any !80 (msg: "SURICATA HTTP on unusual port"; flow: to_server; app-layer-protocol: http; thresho
ld: type limit, track by_src, seconds 60, count 1; sid: 11; rev: 1;)
alert tcp any any → any any (msg: "Possible TCP flow anomaly if ACK or push flags detected within established flow wi
th abnormal delay"; flags: AP; flow: established, to_server; detection_filter: track by_dst, count 2, seconds 30; sid:
 12; rev: 1;)
```

alert tcp any any -> any !80 (msg: "SURICATA HTTP on unusual port"; flow: to_server; app-layer-protocol: http; threshold: type limit, track by_src, seconds 60, count 1; sid: 11; rev: 1;)

alert tcp any any -> any any (msg: "Possible TCP flow anomaly if ACK or push flags detected within established flow with abnormal delay"; flags: AP; flow: established, to_server; detection_filter: track by_dst, count 2, seconds 30; sid: 12; rev: 1;)

5. **Detect unauthorized protocols or traffic:**

   These rules detect and alert about unauthorized traffic. For example, someone using TOR.



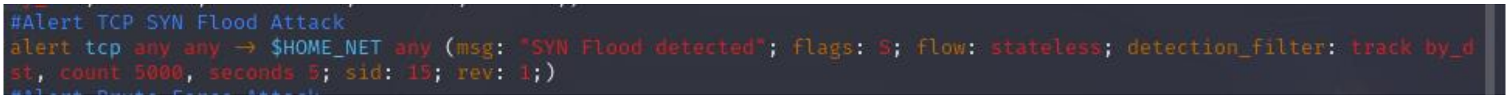
```
#Alert Unauthorized Protocols
alert ip any any → any any (msg: "Possible TOR network traffic detected"; flow: established; content: "Tor"; nocase;
sid: 13; rev: 1;)
alert ip any any → any !31337 (msg: "Traffic on unusual port 31337"; flow: established; threshold: type limit, track
by_src, count 1, seconds 60; sid: 14; rev: 1;)
```

alert ip any any -> any any (msg: "Possible TOR network traffic detected"; flow: established; content: "Tor"; nocase; sid: 13; rev: 1;)

alert ip any any -> any !31337 (msg: "Traffic on unusual port 31337"; flow: established; threshold: type limit, track by_src, count 1, seconds 60; sid: 14; rev: 1;)

6. **Detect TCP SYN Flood attacks:**

   This alert will let me know if there is a SYN flood attack, 5000 syn messages received in 5 seconds or less.

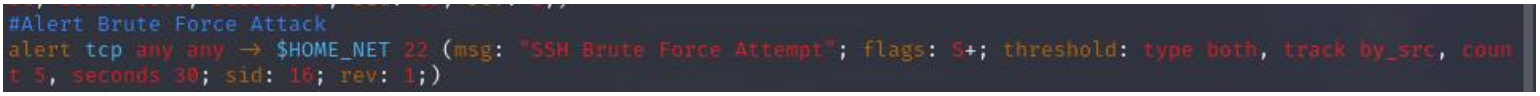


```
#Alert TCP SYN Flood Attack
alert tcp any any → $HOME_NET any (msg: "SYN Flood detected"; flags: S; flow: stateless; detection_filter: track by_d
st, count 5000, seconds 5; sid: 15; rev: 1;)
```

alert tcp any any -> $HOME_NET any (msg: "SYN Flood detected"; flags: S; flow: stateless; detection_filter: track by_dst, count 5000, seconds 5; sid: 15; rev: 1;)

7. **Detecting and Blocking Brute Force Attacks:**

   This alert will notify me of a brute force attempt if SSH is tried 5 times within 30 seconds.

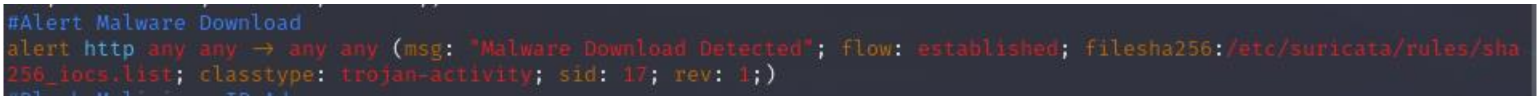


```
#Alert Brute Force Attack
alert tcp any any → $HOME_NET 22 (msg: "SSH Brute Force Attempt"; flags: S+; threshold: type both, track by_src, coun
t 5, seconds 30; sid: 16; rev: 1;)
```

alert tcp any any -> $HOME_NET 22 (msg: "SSH Brute Force Attempt"; flags: S+; threshold: type both, track by_src, count 5, seconds 30; sid: 16; rev: 1;)

8. **Detect and Alerting on Malware Download:**

   For this alert I had to generate a file containing common maliscious Sha256 hashes and place it in the /etc/suricata/rules/ directory. When a file is downloaded, this files is referenced to check for malware in the download.



```
#Alert Malware Download
alert http any any → any any (msg: "Malware Download Detected"; flow: established; filesha256:/etc/suricata/rules/sha
256_iocs.list; classtype: trojan-activity; sid: 17; rev: 1;)
```

alert http any any -> any any (msg: "Malware Download Detected"; flow: established; filesha256:/etc/suricata/rules/sha256_iocs.list; classtype: trojan-activity; sid: 17; rev: 1;)

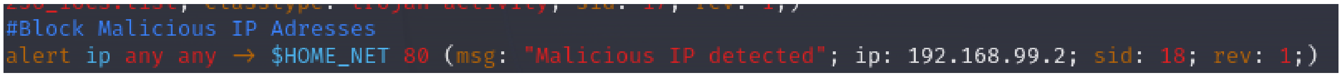
Installation of Suricata IDS/IPS and the creation of detection rules

Jordan Patterson 2024

9. **Block malicious IP addresses:**

   Suricata cant block malicious IP addresses on its own so I created an IPTABLES and added the IP 192.168.99.2 to it. I then added an alert in suricata to notify me if this IP attemps to contact my virtual machine.

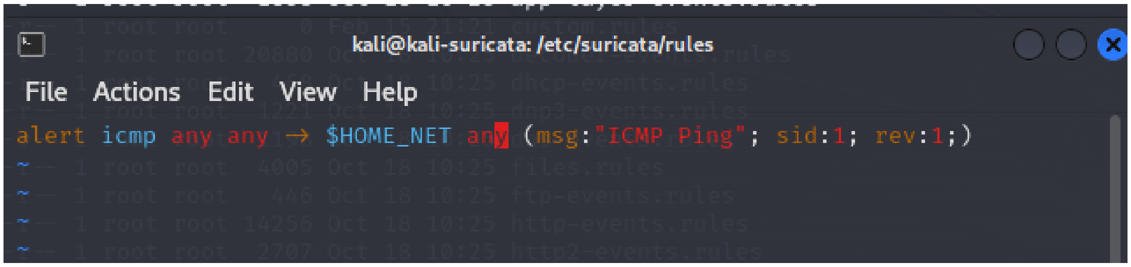
alert ip any any -> any 80 (msg: "Malicious IP detected"; ip: 192.168.99.2; sid: 18; rev: 1;)



```
#Block Malicious IP Adresses
alert ip any any → $HOME_NET 80 (msg: "Malicious IP detected"; ip: 192.168.99.2; sid: 18; rev: 1;)
```

10. **Detect ICMP Ping traffic:**

    This rule will alert you if someboy tries to PING the virtual machine.

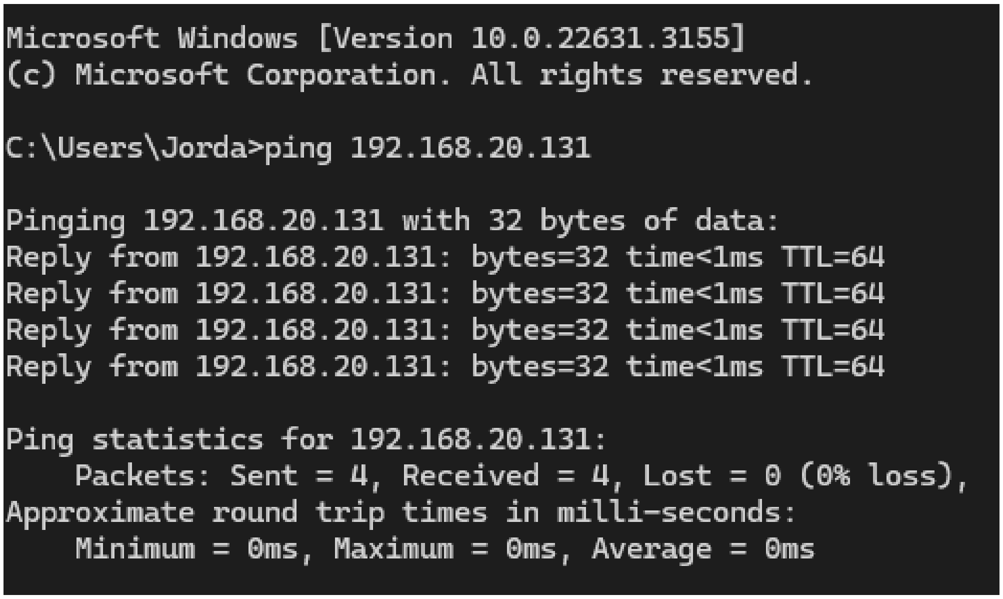


kali@kali-suricata: /etc/suricata/rules
File Actions Edit View Help

```
alert icmp any any → $HOME_NET any (msg:"ICMP Ping"; sid:1; rev:1;)
~
~
~
~
```

Alert icmp any any -> $HOME_NET any (msg:”ICMP Ping”; sid:1; rev:1;)

I sent a ping from my host machine to trigger the alert that I created.

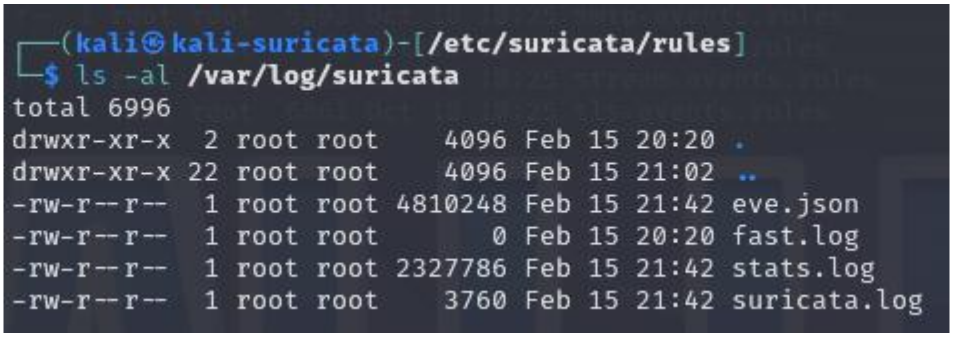


```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Jorda>ping 192.168.20.131

Pinging 192.168.20.131 with 32 bytes of data:
Reply from 192.168.20.131: bytes=32 time<1ms TTL=64
Reply from 192.168.20.131: bytes=32 time<1ms TTL=64
Reply from 192.168.20.131: bytes=32 time<1ms TTL=64
Reply from 192.168.20.131: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.20.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

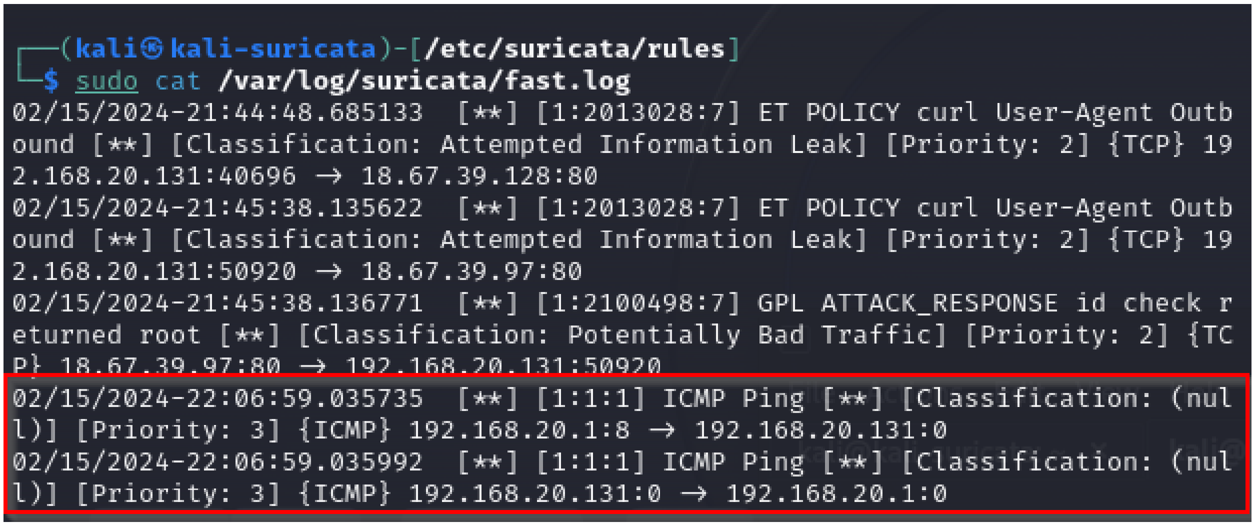
Installation of Suricata IDS/IPS and the creation of detection rules

Jordan Patterson 2024

I opened the logs directory and opened the fast.log file. I found that my rule worked and alerted that a Ping came from an external device (my host machine).



```
┌──(kali㉿kali-suricata)-[/etc/suricata/rules]
└─$ ls -al /var/log/suricata
total 6996
drwxr-xr-x  2 root root    4096 Feb 15 20:20 .
drwxr-xr-x 22 root root    4096 Feb 15 21:02 ..
-rw-r--r--  1 root root 4810248 Feb 15 21:42 eve.json
-rw-r--r--  1 root root       0 Feb 15 20:20 fast.log
-rw-r--r--  1 root root 2327786 Feb 15 21:42 stats.log
-rw-r--r--  1 root root    3760 Feb 15 21:42 suricata.log
```



```
┌──(kali㉿kali-suricata)-[/etc/suricata/rules]
└─$ sudo cat /var/log/suricata/fast.log
02/15/2024-21:44:48.685133  [**] [1:2013028:7] ET POLICY curl User-Agent Outb
ound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 19
2.168.20.131:40696 → 18.67.39.128:80
02/15/2024-21:45:38.135622  [**] [1:2013028:7] ET POLICY curl User-Agent Outb
ound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 19
2.168.20.131:50920 → 18.67.39.97:80
02/15/2024-21:45:38.136771  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check r
eturned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TC
P} 18.67.39.97:80 → 192.168.20.131:50920
02/15/2024-22:06:59.035735  [**] [1:1:1] ICMP Ping [**] [Classification: (nul
l)] [Priority: 3] {ICMP} 192.168.20.1:8 → 192.168.20.131:0
02/15/2024-22:06:59.035992  [**] [1:1:1] ICMP Ping [**] [Classification: (nul
l)] [Priority: 3] {ICMP} 192.168.20.131:0 → 192.168.20.1:0
```