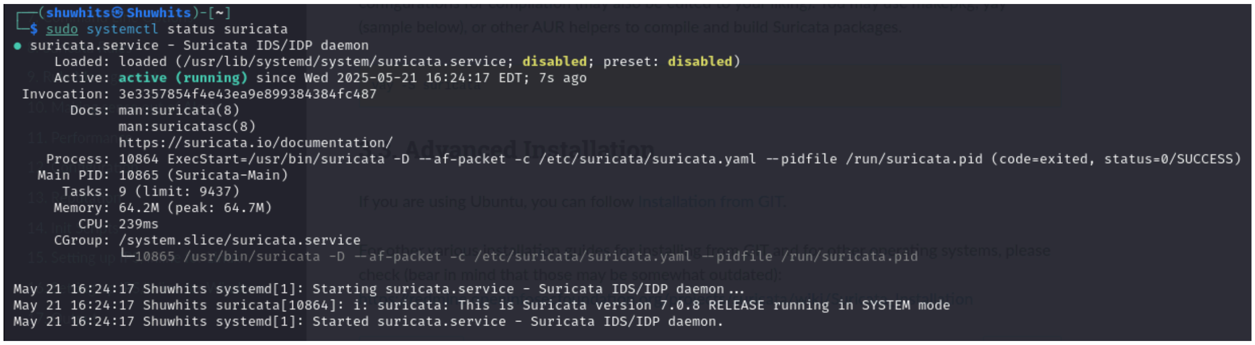
Advanced Network Defense Infrastructure

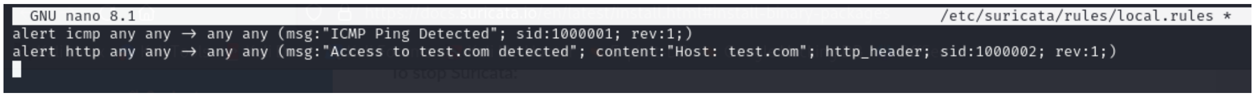
Installation



```
┌──(shuwhits㉿Shuwhits)-[~]
└─$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
     Active: active (running) since Wed 2025-05-21 16:24:17 EDT; 7s ago
 Invocation: 3e3357854f4e43ea9e899384384fc487
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 10864 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid (code=exited, status=0/SUCCESS)
   Main PID: 10865 (Suricata-Main)
      Tasks: 9 (limit: 9437)
     Memory: 64.2M (peak: 64.7M)
        CPU: 239ms
     CGroup: /system.slice/suricata.service
             └─10865 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

May 21 16:24:17 Shuwhits systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
May 21 16:24:17 Shuwhits suricata[10864]: i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
May 21 16:24:17 Shuwhits systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
```

2 Custom Rules

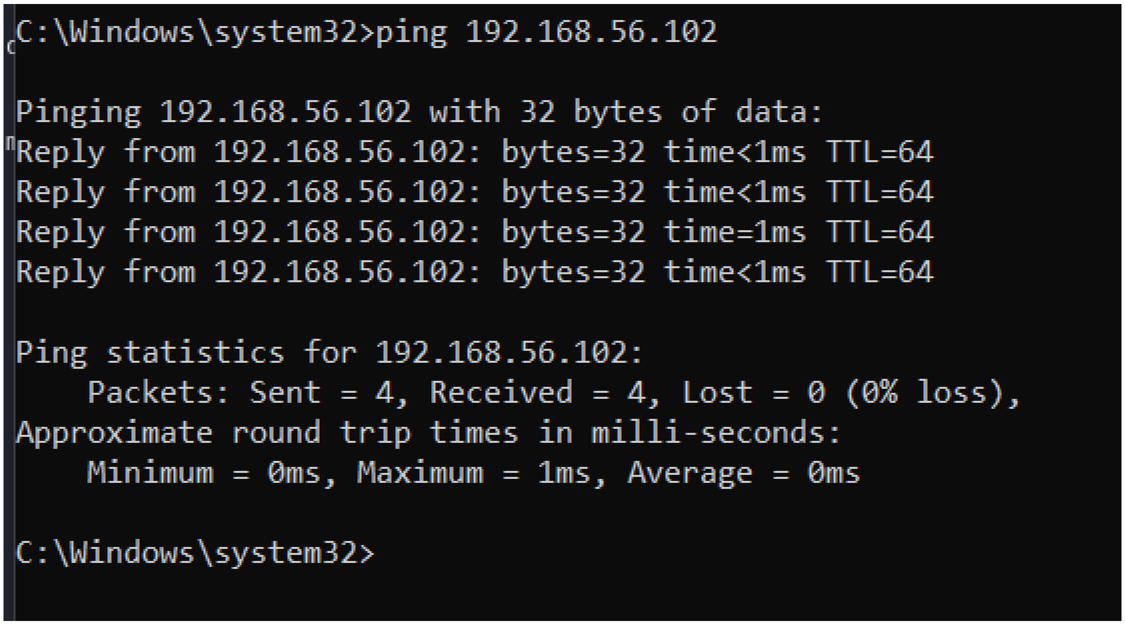


```
  GNU nano 8.1                                                                    /etc/suricata/rules/local.rules *
alert icmp any any → any any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)
alert http any any → any any (msg:"Access to test.com detected"; content:"Host: test.com"; http_header; sid:1000002; rev:1;)
```

These rules generate alerts when:

- Any ICMP packet is detected (simulates basic ping sweep)
- An HTTP request targets a specific host (basic application layer detection

Connectivity



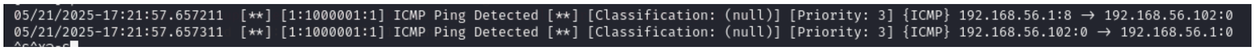
```
C:\Windows\system32>ping 192.168.56.102

Pinging 192.168.56.102 with 32 bytes of data:
Reply from 192.168.56.102: bytes=32 time<1ms TTL=64
Reply from 192.168.56.102: bytes=32 time<1ms TTL=64
Reply from 192.168.56.102: bytes=32 time=1ms TTL=64
Reply from 192.168.56.102: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>
```

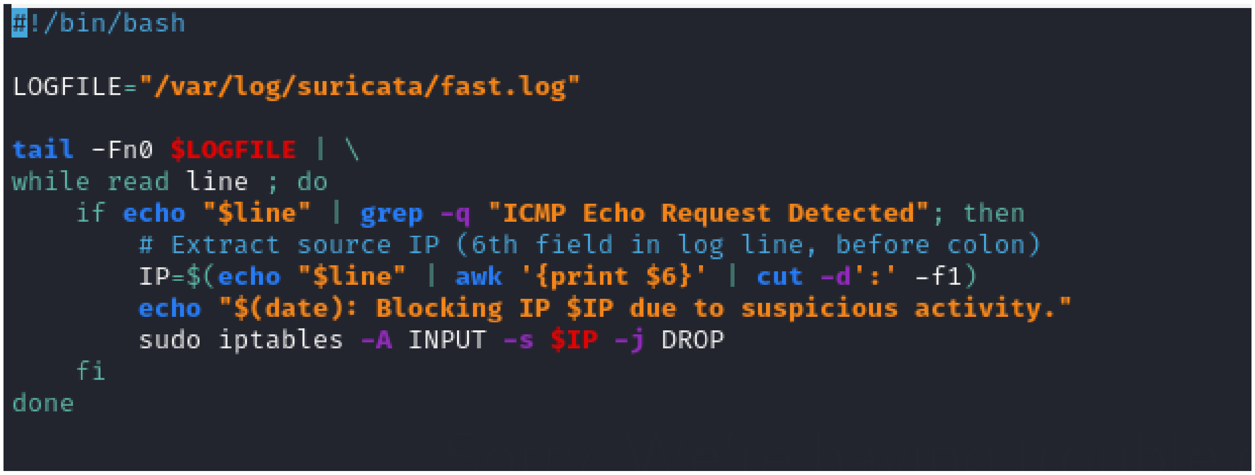
IDS Detection



```
05/21/2025-17:21:57.657211  [**] [1:1000001:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.56.1:8 → 192.168.56.102:0
05/21/2025-17:21:57.657311  [**] [1:1000001:1] ICMP Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.56.102:0 → 192.168.56.1:0
^C^X^C
```

The ICMP rule was generating alerts for all ICMP traffic, including benign network monitoring tools or legitimate pings.

Defense Automation Script



```bash
#!/bin/bash

LOGFILE="/var/log/suricata/fast.log"

tail -Fn0 $LOGFILE | \
while read line ; do
    if echo "$line" | grep -q "ICMP Echo Request Detected"; then
        # Extract source IP (6th field in log line, before colon)
        IP=$(echo "$line" | awk '{print $6}' | cut -d':' -f1)
        echo "$(date): Blocking IP $IP due to suspicious activity."
        sudo iptables -A INPUT -s $IP -j DROP
    fi
done
```

Advanced Network Architecture

Network Protocol & Traffic Analysis

Network Access & Authentication

Network Security Operations