

# ***Project: Using a SIEM to monitor Ubuntu traffic and generate alerts***

Clay Jones

## **Objective:**

Connect a Ubuntu virtual machine to a SIEM and monitor the traffic. Run some Nmap scans to generate network traffic. Analyze the traffic and find the commands that were run. Create a chart monitoring based on the traffic. Create an alert that sends an email and triggers when a specific command is run.

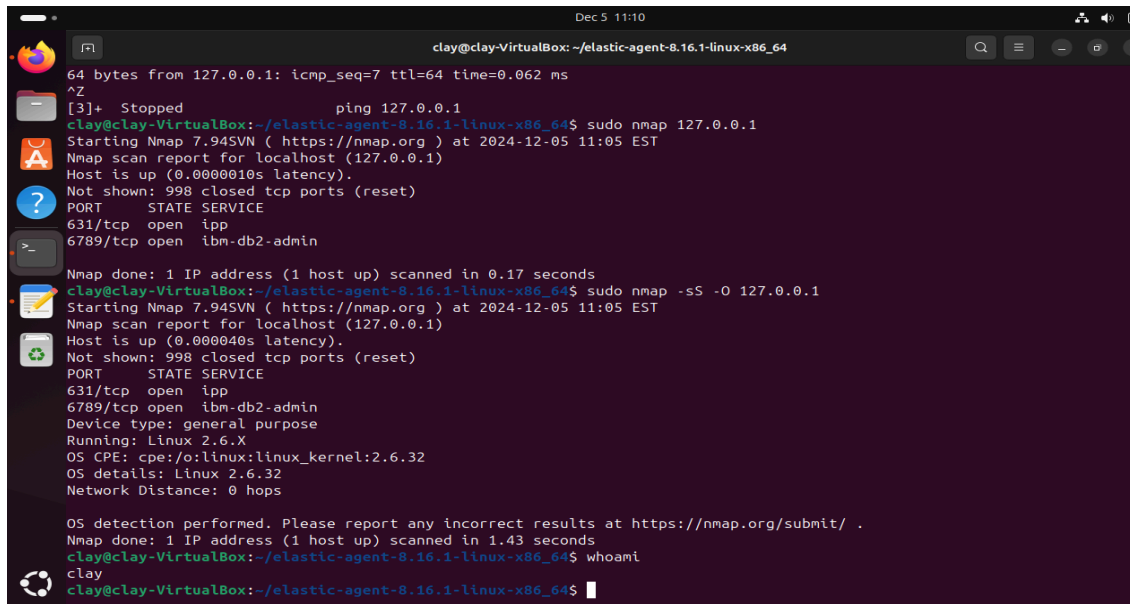
## **Connecting the VM with Elastic Stack:**

```
{
  "log.level": "info",
  "@timestamp": "2024-12-05T11:01:05.270-0500",
  "log.origin": {
    "function": "github.com/elastic/elastic-agent/pkg/agent/cmd.(*enrollCmd).Execute",
    "file.name": "cmd/enroll_cmd.go",
    "file.line": 301,
    "message": "Successfully triggered restart on running Elastic Agent.",
    "ecs.version": "1.6.0"
  }
}
Successfully enrolled the Elastic Agent.
[= ] Done [26s]
Elastic Agent has been successfully installed.
clay@clay-VirtualBox: ~/elastic-agent-8.16.1-linux-x86_64$ sudo systemctl status elastic-agent.service
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor >
   Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset>
   Active: active (running) since Thu 2024-12-05 11:01:01 EST; 2min 25s ago
 Main PID: 7877 (elastic-agent)
   Tasks: 71 (limit: 2278)
  Memory: 705.7M (peak: 774.6M swap: 35.0M swap peak: 49.2M)
    CPU: 18.269s
 CGroup: /system.slice/elastic-agent.service
          └─7877 elastic-agent
              └─7955 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compon>
              └─7964 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compon>
              └─7976 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compon>
              └─7986 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compon>
              └─8151 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compon>
              └─8675 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compon>

Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level": "info", "@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level": "info", "@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level": "info", "@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level": "info", "@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level": "info", "@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level": "info", "@time>
Dec 05 11:01:04 clay-VirtualBox elastic-agent[7877]: {"log.level": "info", "@time>
lines 1-23
clay@clay-VirtualBox: ~/elastic-agent-8.16.1-linux-x86_64$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 ndisc queue state UNKNOWN group default qlen 1000
```

Create an integration and connected Ubuntu to elastic.

## Generating Traffic using Nmap:

A terminal window titled 'clay@clay-VirtualBox: ~/elastic-agent-8.16.1-linux-x86\_64' with a timestamp of 'Dec 5 11:10'. The terminal shows a series of commands and their outputs. It starts with a ping to 127.0.0.1, followed by a standard Nmap scan of 127.0.0.1. The output shows the host is up and lists open ports 631/tcp (ipp) and 6789/tcp (ibm-db2-admin). Then, a silent Nmap scan (-sS -O) is performed on 127.0.0.1, which includes OS detection. The OS is identified as Linux 2.6.32. The terminal also shows the output of the 'whoami' command, which is 'clay'.

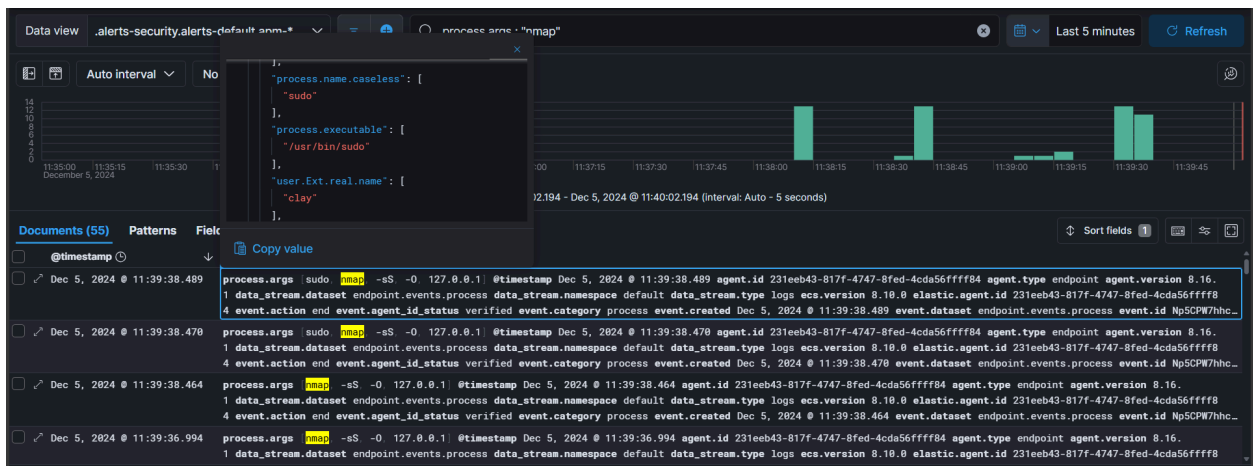
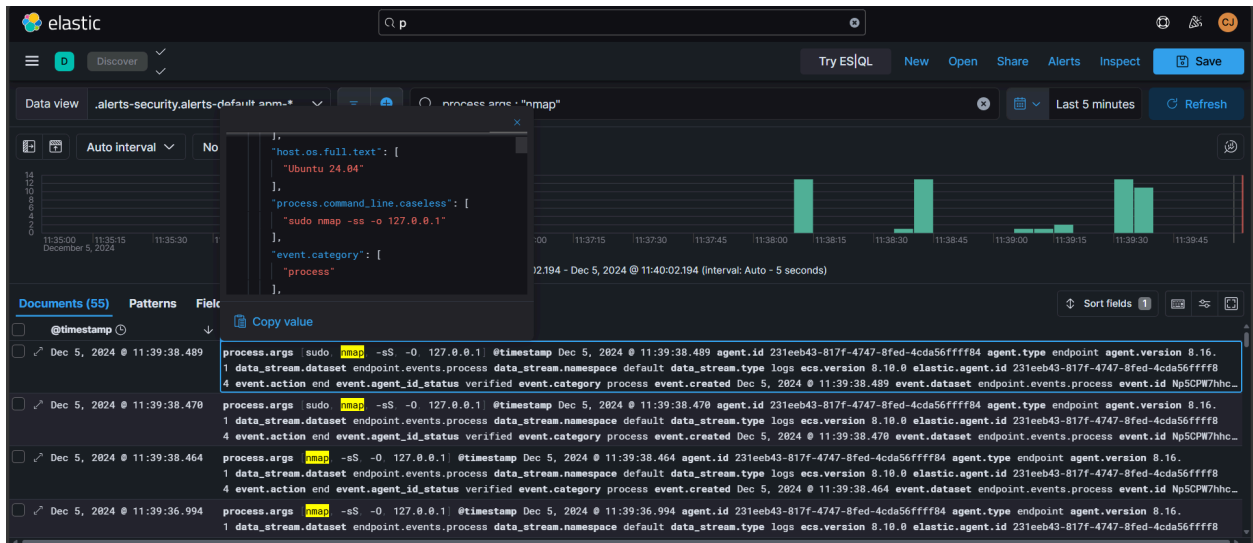
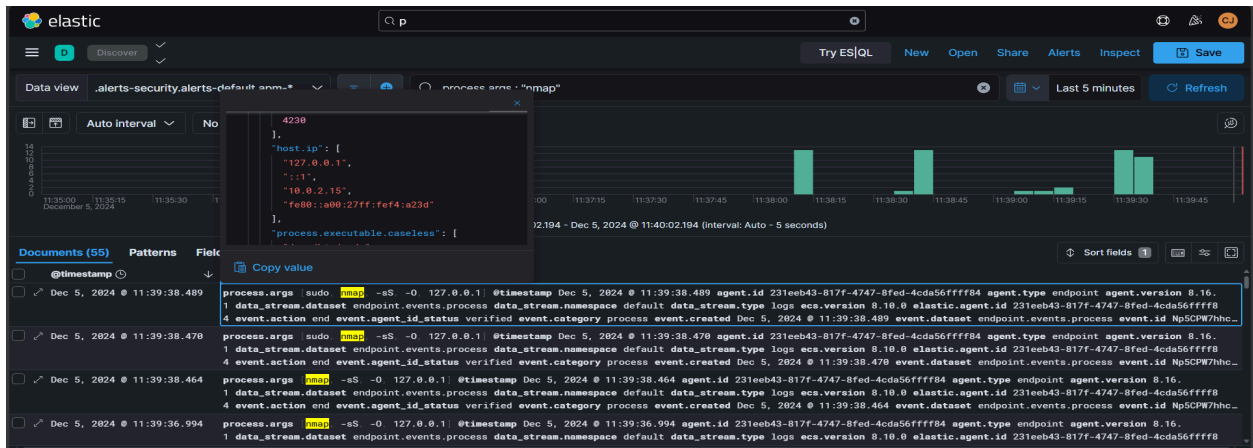
```
clay@clay-VirtualBox: ~/elastic-agent-8.16.1-linux-x86_64
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.062 ms
^Z
[3]+  Stopped                  ping 127.0.0.1
clay@clay-VirtualBox:~/elastic-agent-8.16.1-linux-x86_64$ sudo nmap 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-05 11:05 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
631/tcp   open  ipp
6789/tcp  open  ibm-db2-admin

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
clay@clay-VirtualBox:~/elastic-agent-8.16.1-linux-x86_64$ sudo nmap -sS -O 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-05 11:05 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
631/tcp   open  ipp
6789/tcp  open  ibm-db2-admin
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
clay@clay-VirtualBox:~/elastic-agent-8.16.1-linux-x86_64$ whoami
clay
clay@clay-VirtualBox:~/elastic-agent-8.16.1-linux-x86_64$
```

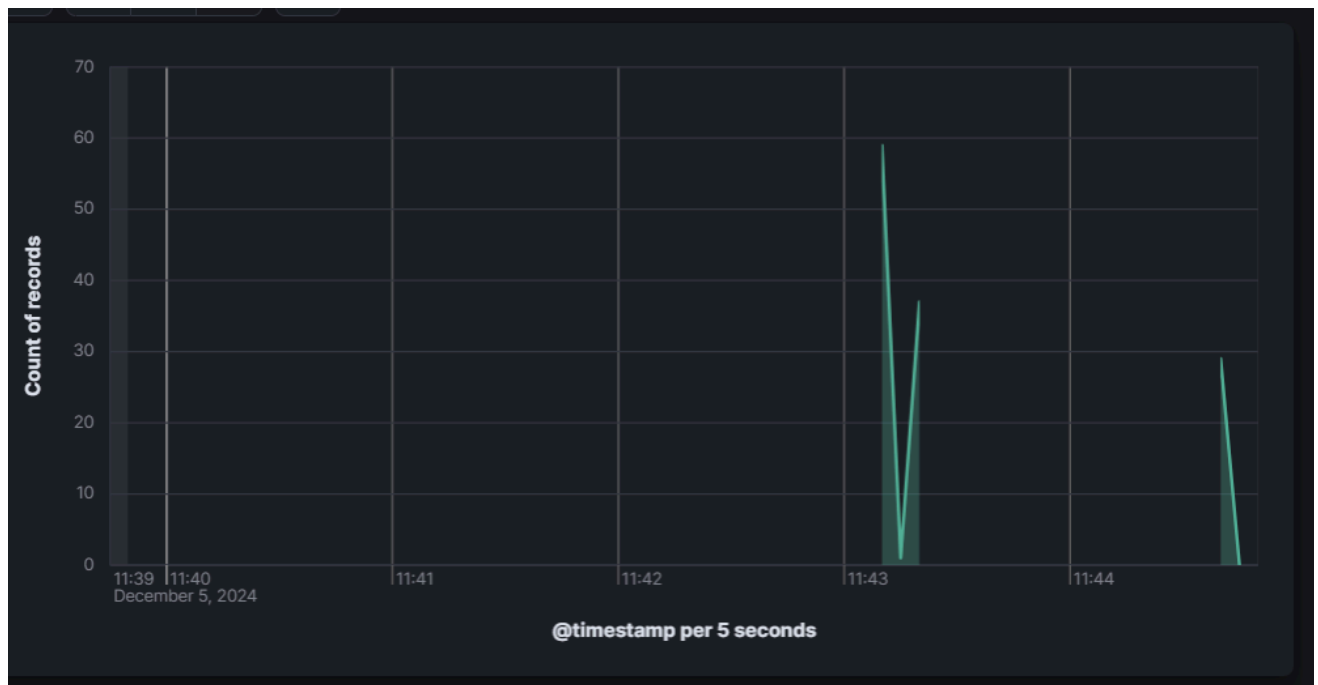
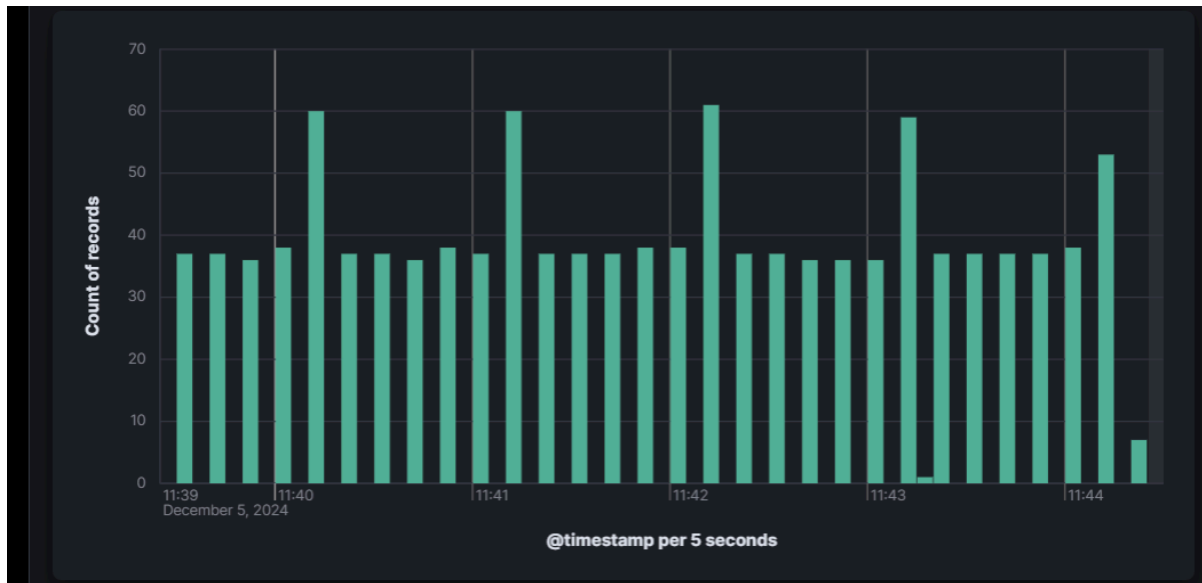
I ran several Nmap scans on the host to generate network traffic.

## Nmap scans found in elastic logs:



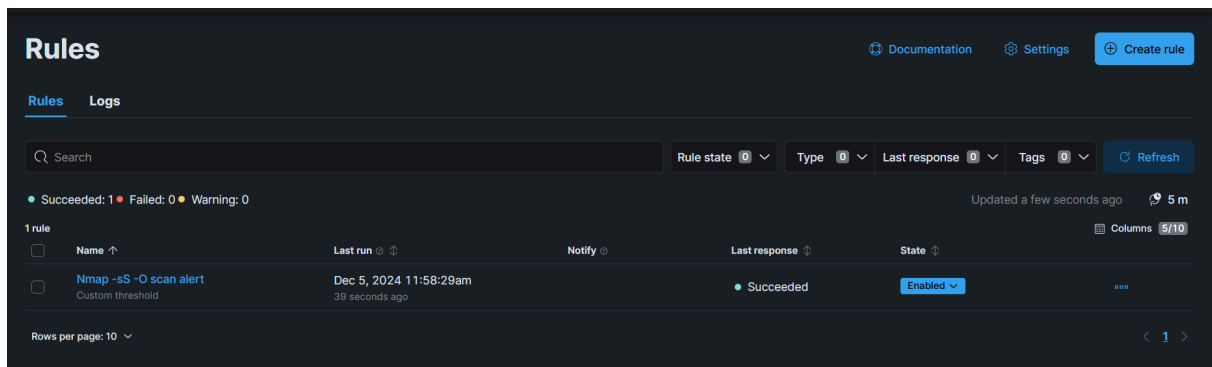
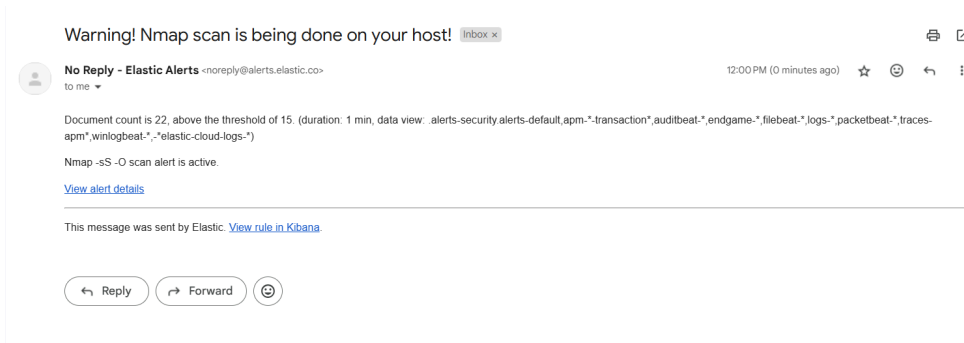
The scans that I ran were shown in the logs. The command that generated the most traffic was “sudo nmap -sS -O localhost.” This also shows metadata off the host that generated this traffic.

### Charts based on traffic:



These charts were created based on the time and count of records.

## Creating an alert



I created an alert that sends an email every time the “sudo nmap -sS -O localhost” command is run on the host.

## Isolation and Response:

The screenshot displays the Elastic Endpoints management console. The left sidebar shows navigation options under 'Security' and 'Manage'. The main panel, titled 'Endpoints', shows 'Hosts running Elastic Defend'. A single endpoint is listed in a table with columns for Endpoint, Agent status, Policy, Policy status, OS, IP address, and Version. The endpoint 'clay-VirtualBox' is shown as 'Offline'. A context menu is open over the endpoint, offering actions: 'Isolate host', '>\_ Respond', 'View response actions history', 'View host details', 'View agent policy', 'View agent details', and 'Reassign agent policy'. The bottom of the screen shows a Windows taskbar with the date and time as 12:16 PM on 12/5/2024.

Endpoint	Agent status	Policy	Policy status	OS	IP address	Version
clay-VirtualBox	Offline	ubuntu rev. 1	Success	Linux	127.0.0.1, ::1, 10.0.2.15, f...	8.16.1

I have the option of isolating the host or responding to the incident in the endpoint manager.