**Attack 1 with Nmap Scan Alert**:

This alert will be triggered when there are Nmap scan logs identified by the network monitoring tool(zeek) and accordingly a custom alert is created.

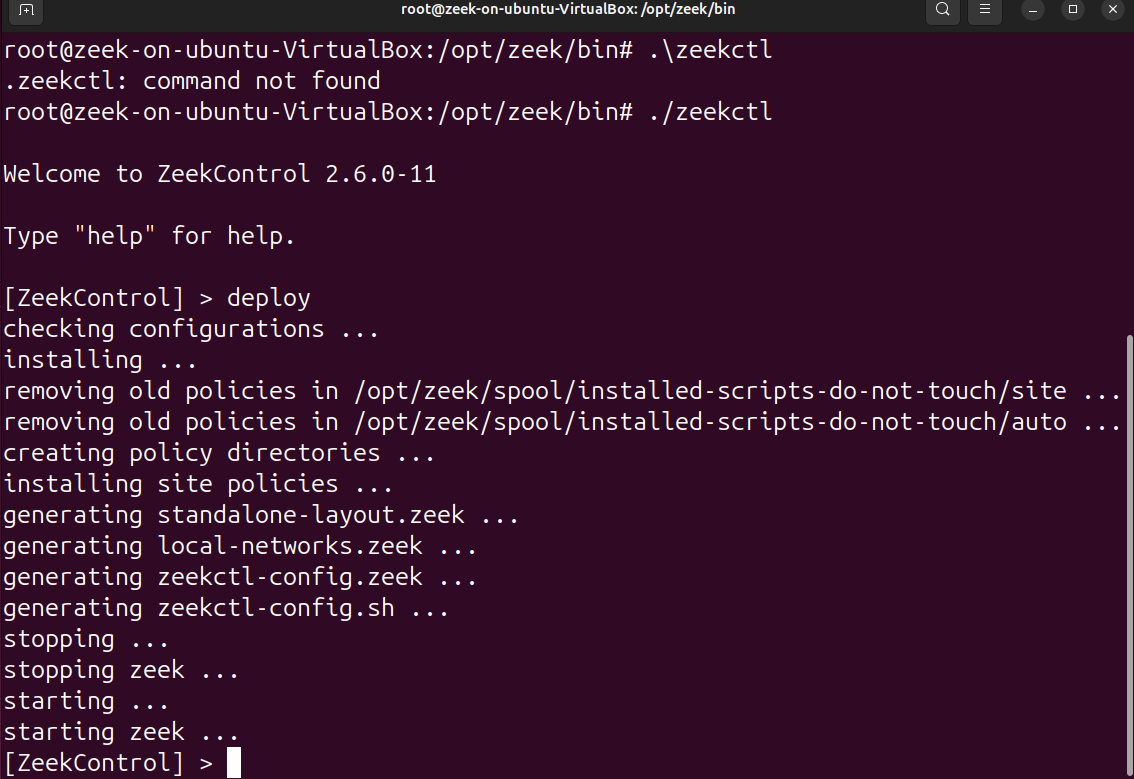
Created rules in elastic are in .ndjson format, those files for the alert is uploaded and the process and output screenshots are added in this page.

**Attack Scenario:**

This scenario is to run a nmap scanner in our attacker machine for the machines available in our network. Since I have the victim machine running in the same network , with web server on the victim machine up with python, we can see that our victim machine comes as the target in our nmap scan.

**Steps:**

First step is to make sure that the zeek is running.



Once we confirm that the zeek is running, we perform the nmap scan.

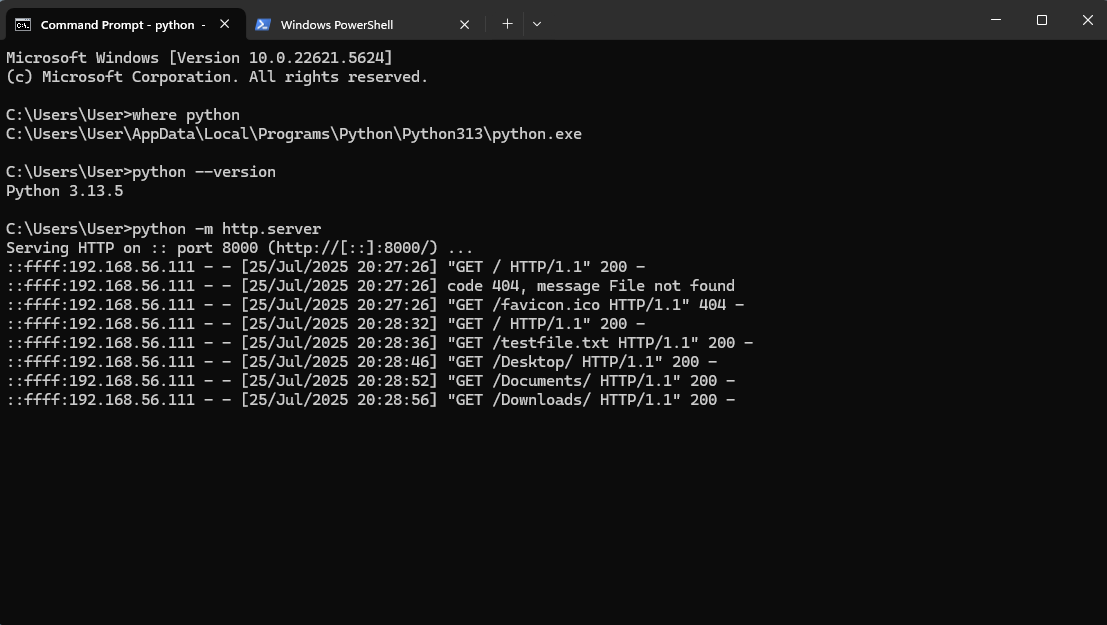
Nmap scan is done to know what are the machines available in our network, and any ports, services running on the machine etc.

**Syntax or command to run nmap scan:**

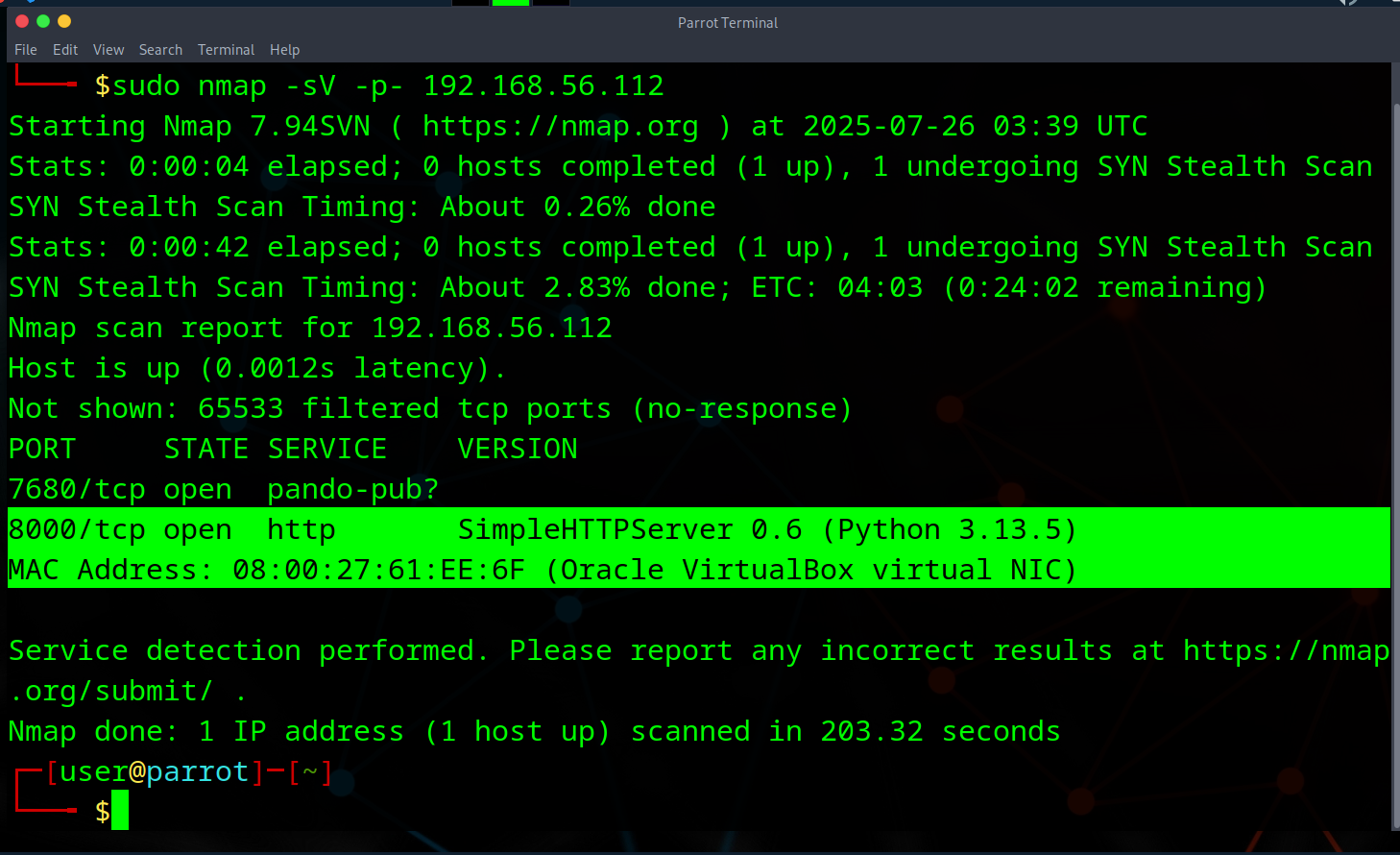
$ sudo nmap -sV -p- <target-machine-ip-addr>

In the command I did not mention to scan for specific ports, instead -p- scans all ports and -s scans the services and -v scan for the versions of the services.

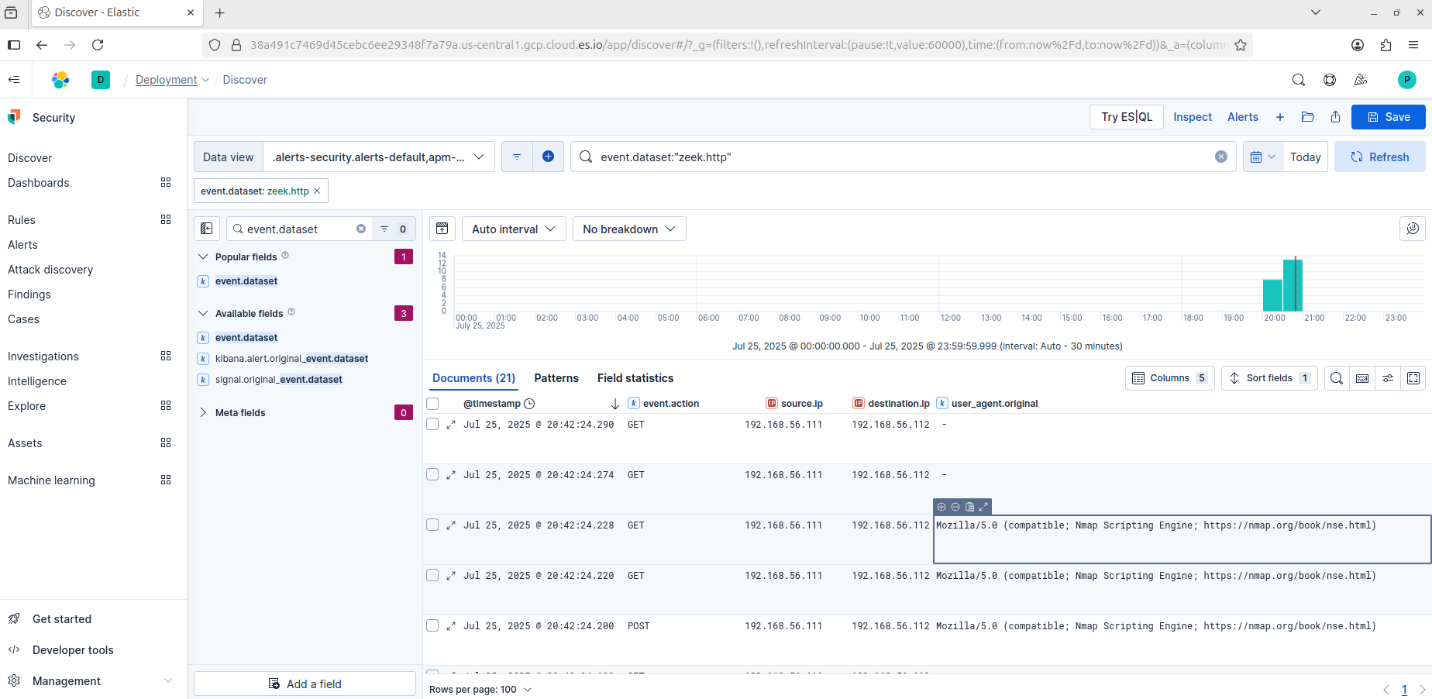
Since I am running this in a simulated lab environment, I made sure that the python server is running on my victim machine (windows machine) :

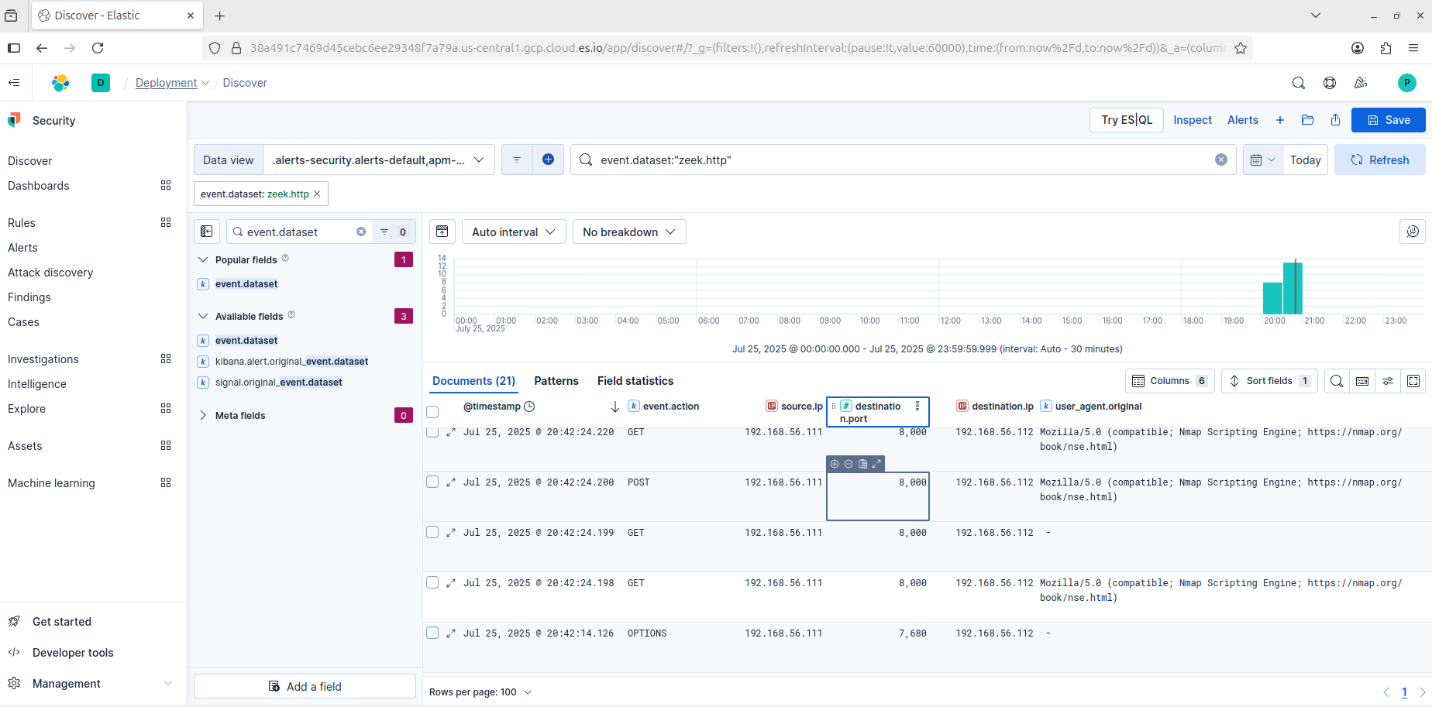


Later, on my attacker machine (parrot OS), I run the command to scan by using Nmap tool:



After the scan is done, we can log-in to our elastic and check the zeek logs in discover tab.





Nmap logs are generated by zeek and pushed into the SIEM.

We can see the logs are generated by name nmap script engine and we can see the destination and source ip addresses.

Next, a custom alert can be created for Nmap scan.

To do that, go to manage rules option, and click on create alert and fill in the details.

We can export this rule from kibana, this file will be stored in .ndjson format, which is uploaded, you can check for the alert in that file.

Below is the screenshot for the alert generated. We can see that 4 Nmap scan alerts were generated.

