**Attack 2 with Nikto Scan Alert**:

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

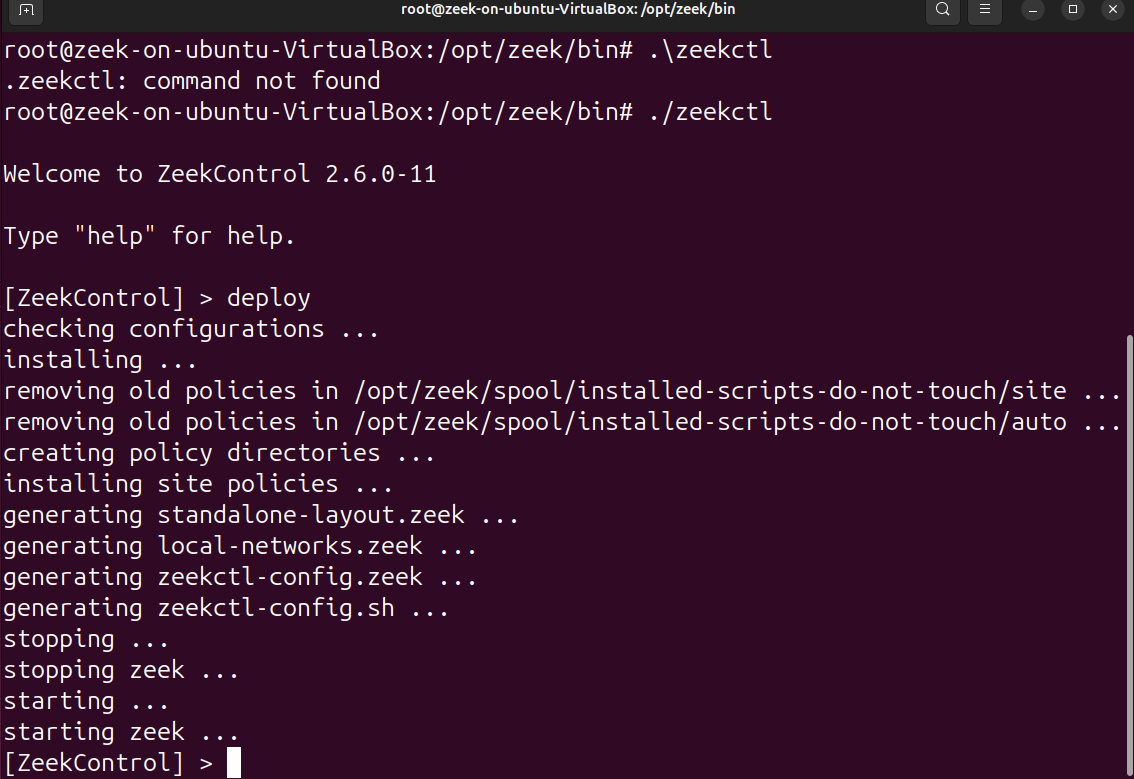
Created rules in elastic are in .ndjson format, those files for the alert is uploaded and the process and output screenshots are added in this page.

Attack scenario:

This scenario is to run a nikto scanner in our attacker machine to check for web vulnerabilities, and identify a way to go into the machine using those web vulnerabilities.

**Steps:**

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



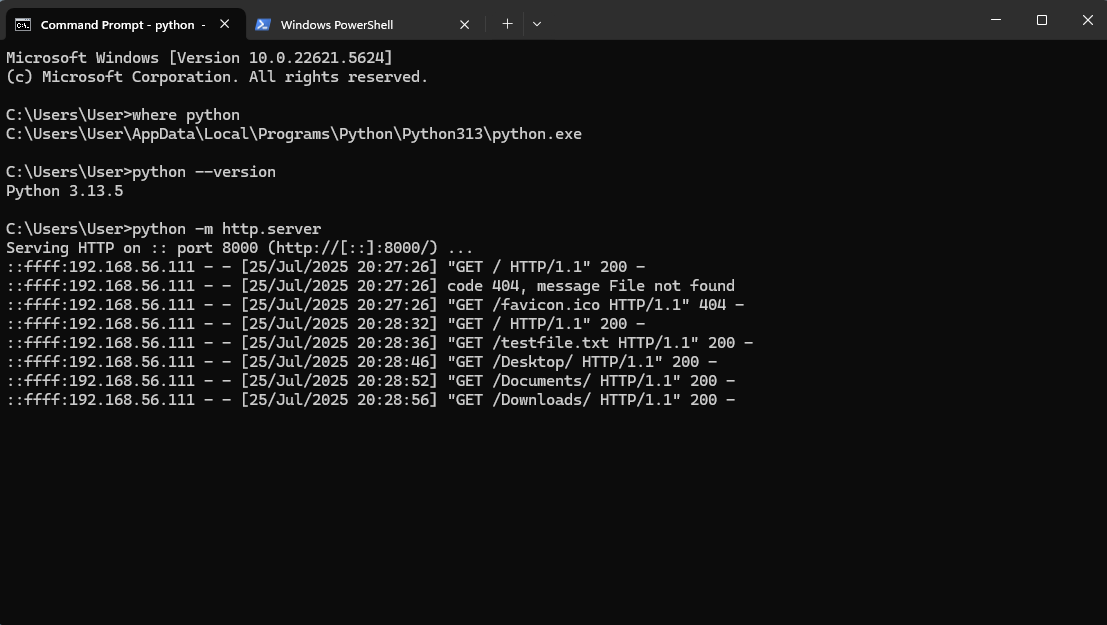
Once we confirm that the zeek is running, we perform the nikto scan to for web vulnerabiblities.

This scan is done after the nmap scan, once we know what are the services and ports running from nmap scan, we do nikto scan for deep web vulnerabilities scan on specific poer which is identified in nmap scanning.

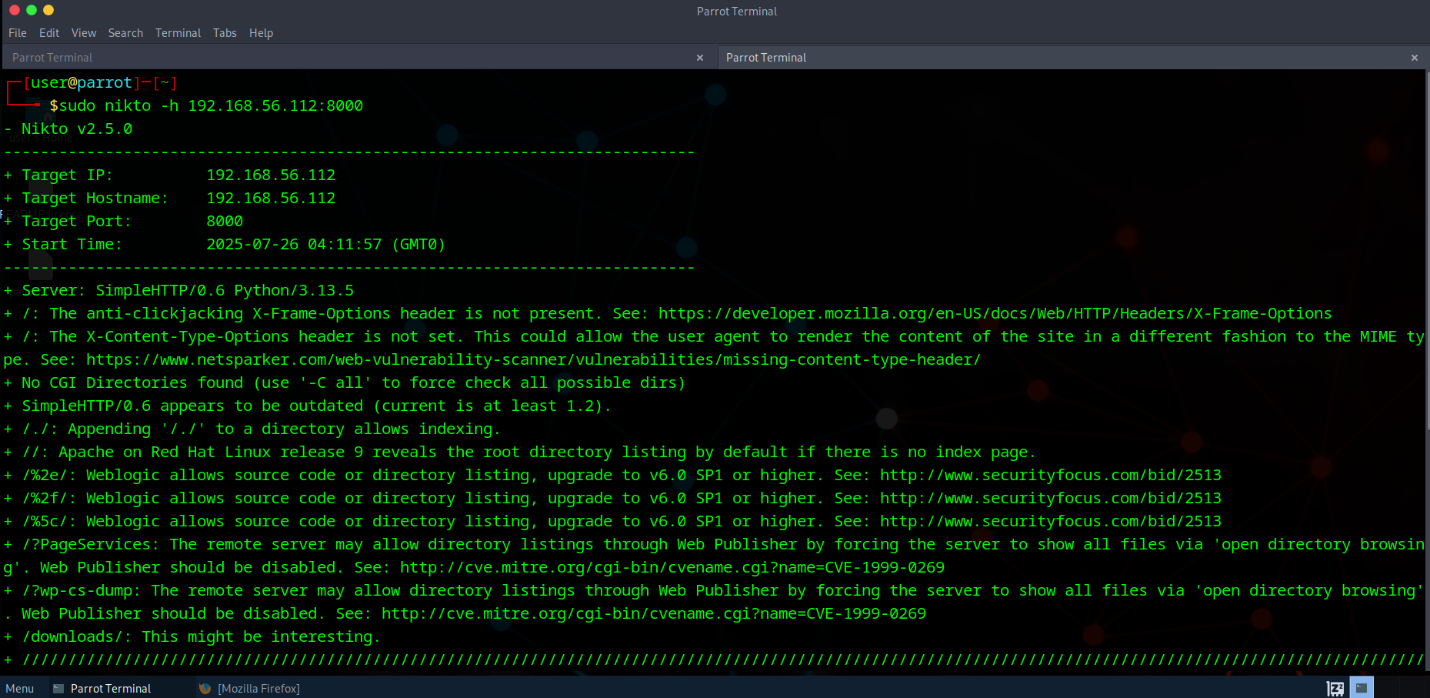
**Syntax or command to run nikto scan:**

$ sudo nikto -h <target-machine-ip-addr>:<port no.>

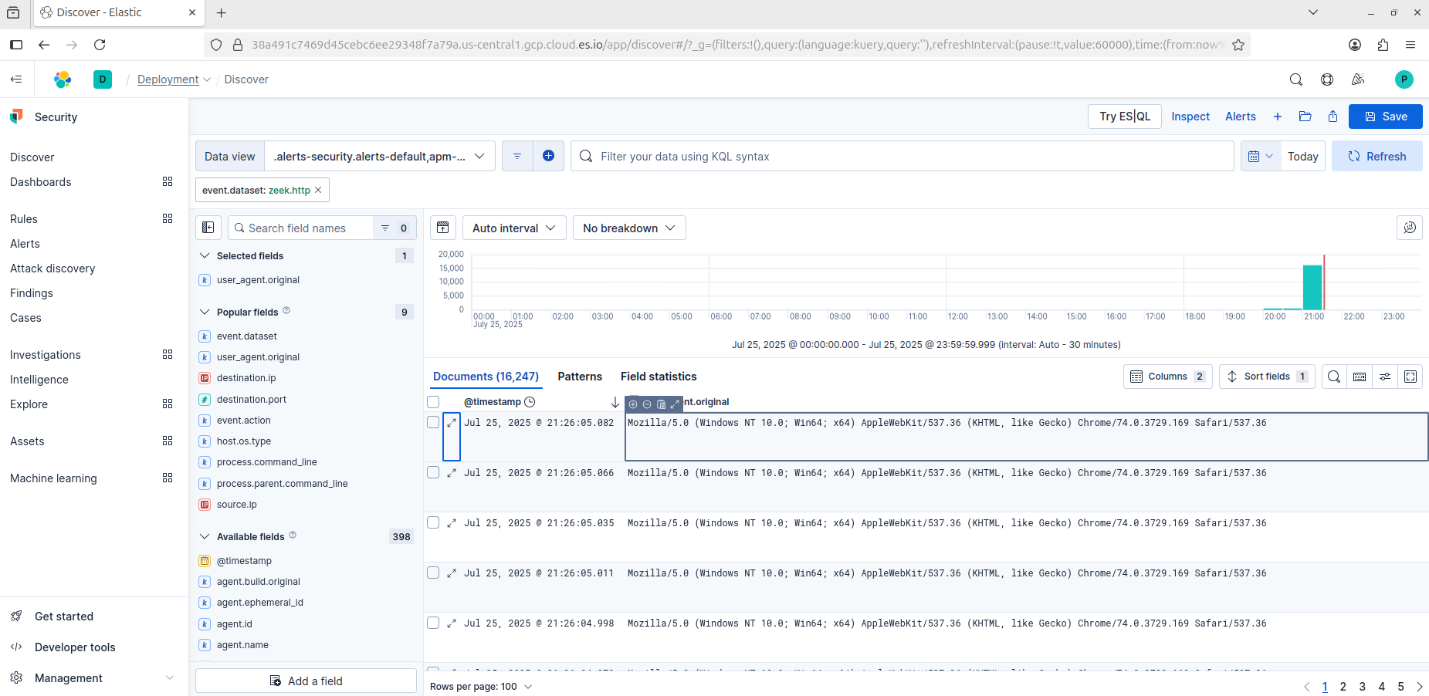
Since I am running this in a simulated lab environment, I made sure that the python server is running on my victim machine (windows machine) :



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



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



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

By default in some of the browsers like mozilla, nikto uses Aplewebkit as user\_agent\_name to get into logs to look less suspicious on the network, which helps to avoid WAFs (Web Application Firewalls) or IDS/IPS systems that might block Nikto if it used its default signature.

Next, a custom alert can be created for Nikto 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.

