**Command prompt usage alert**:

This alert will be generated when command prompt is used remotely.

**Attack Scenario:**

For the above alert to be generated I have made an attack in my simulated lab environment.

I have created a reverse tcp payload in my attacker machine(parrot OS) and the payload is hidden in a file named interesting.exe.

Next, in my attacker machine(parrot OS), I ran a simple http server to make the victim machine open and download the file on which our payload is hidden.

And in the attacker machine, I have opened a listener using msfconsole and set the Lhost(listening host) as attacker machine ip addr, and payload was set to the payload which was created and hidden in interesting.exe file, now my attacker machine is listening for any connections that can be made.

Generally it is difficult to make or trick the victims to click on the links or download a file.

Although tough in practical scenarios, but it is like a phishing attempt where people will click on the links or download the files on which the payloads will be hidden.

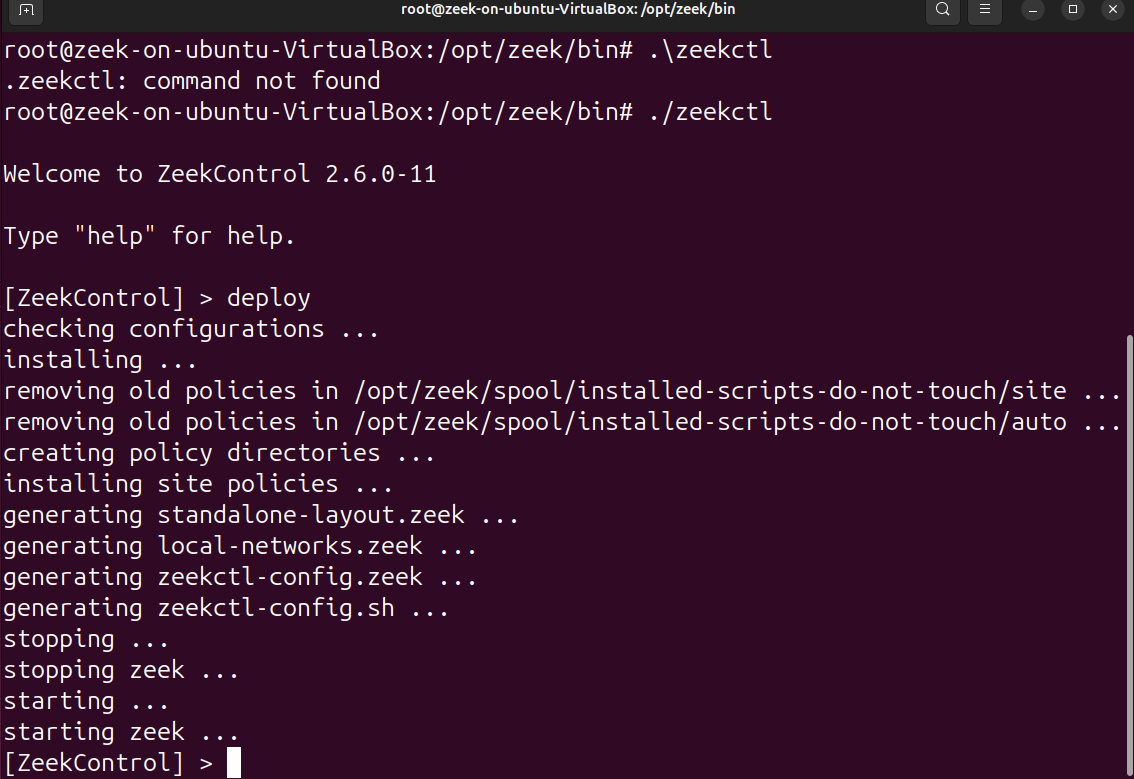
Since I am doing this in a simulated lab, and I have access to the victim machine I have opened up the http website on which the attacker is running. And I have downloaded the interesting.exe file.

Now upon opening the file interesting.exe, in my attacker machine a meterpreter will be opened and now I can acess the victim machines files and can do shell commands and download any files if I need any.

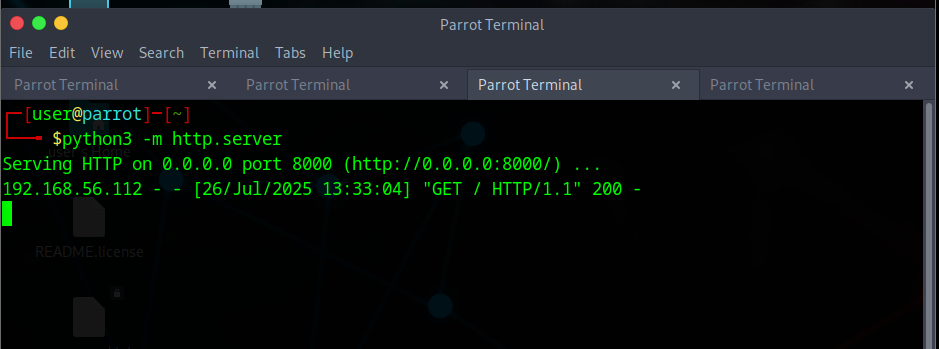
Whoami command is executed and the logs are generated and the alert for that is created.

**Steps:**

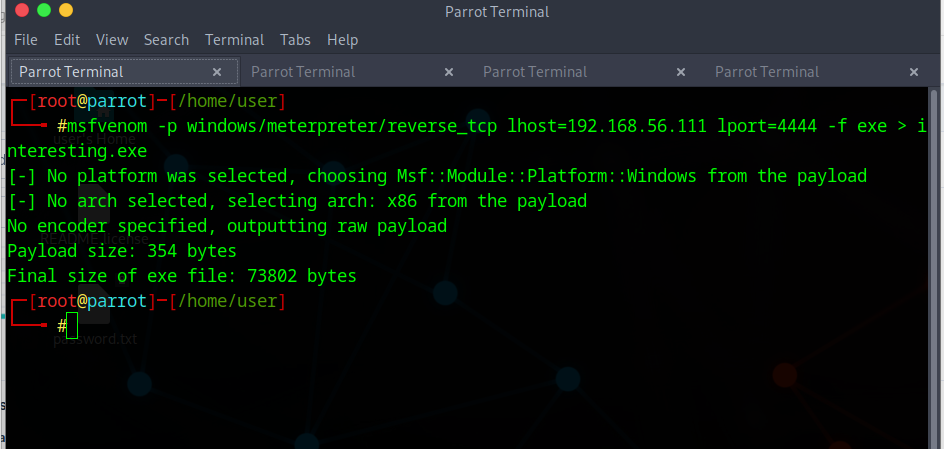
First step is to make sure that the zeek is running.



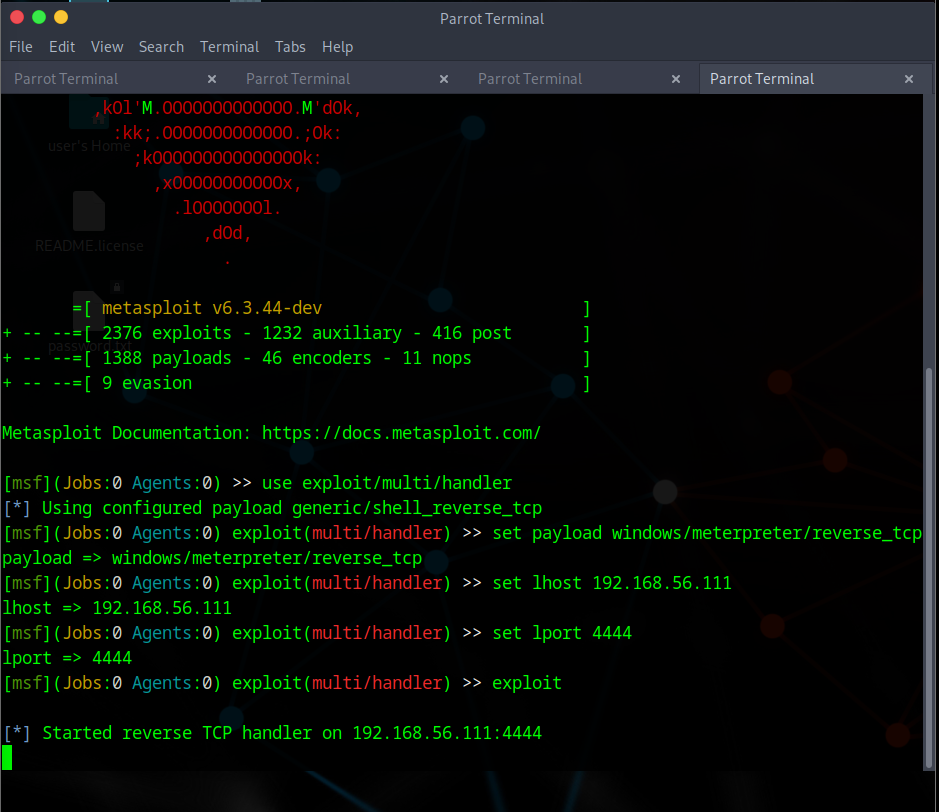
In this scenario, we will run http server on attacker machine(parrot OS)



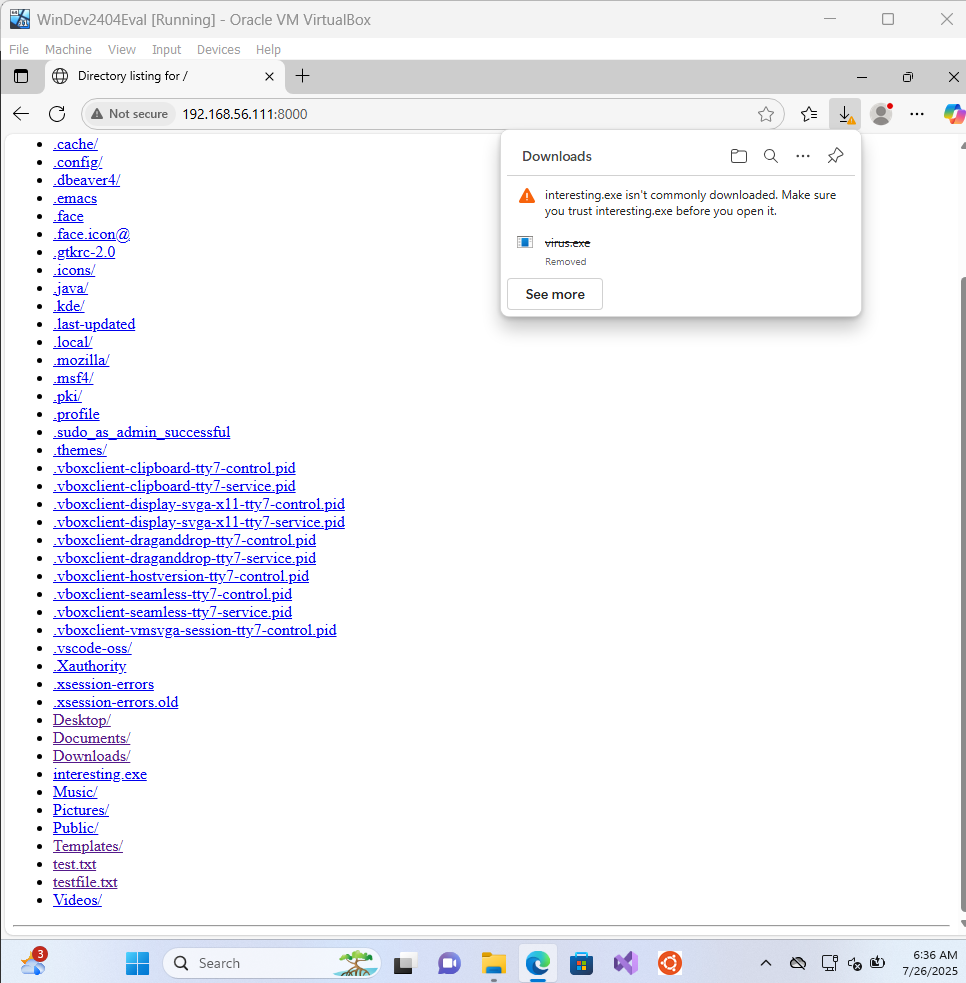
Next step is to create a payload in attacker machine:



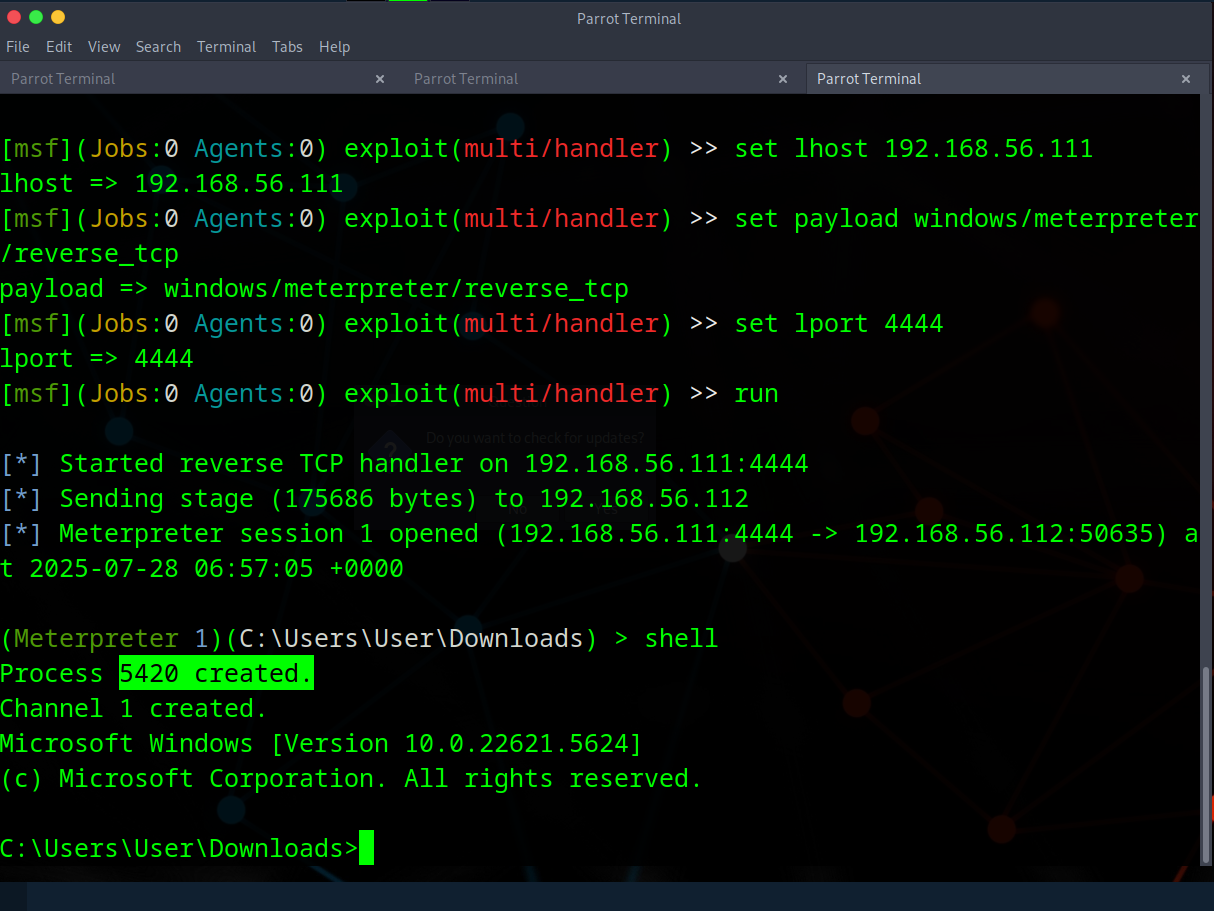
Next, we set up a listener in attacker machine(parrot OS):



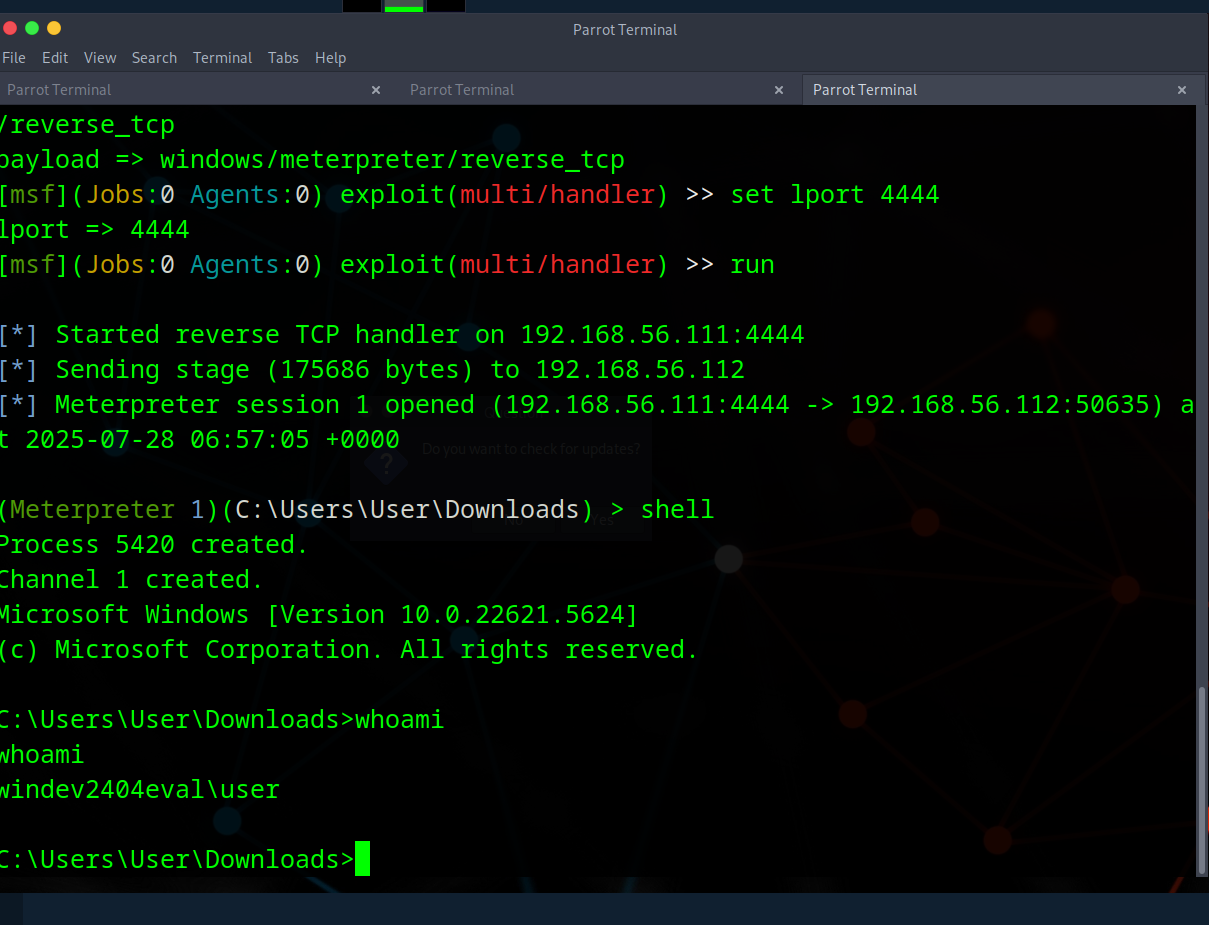
Now, on the victim machine, we acess the server and download the file named “interesting.exe”



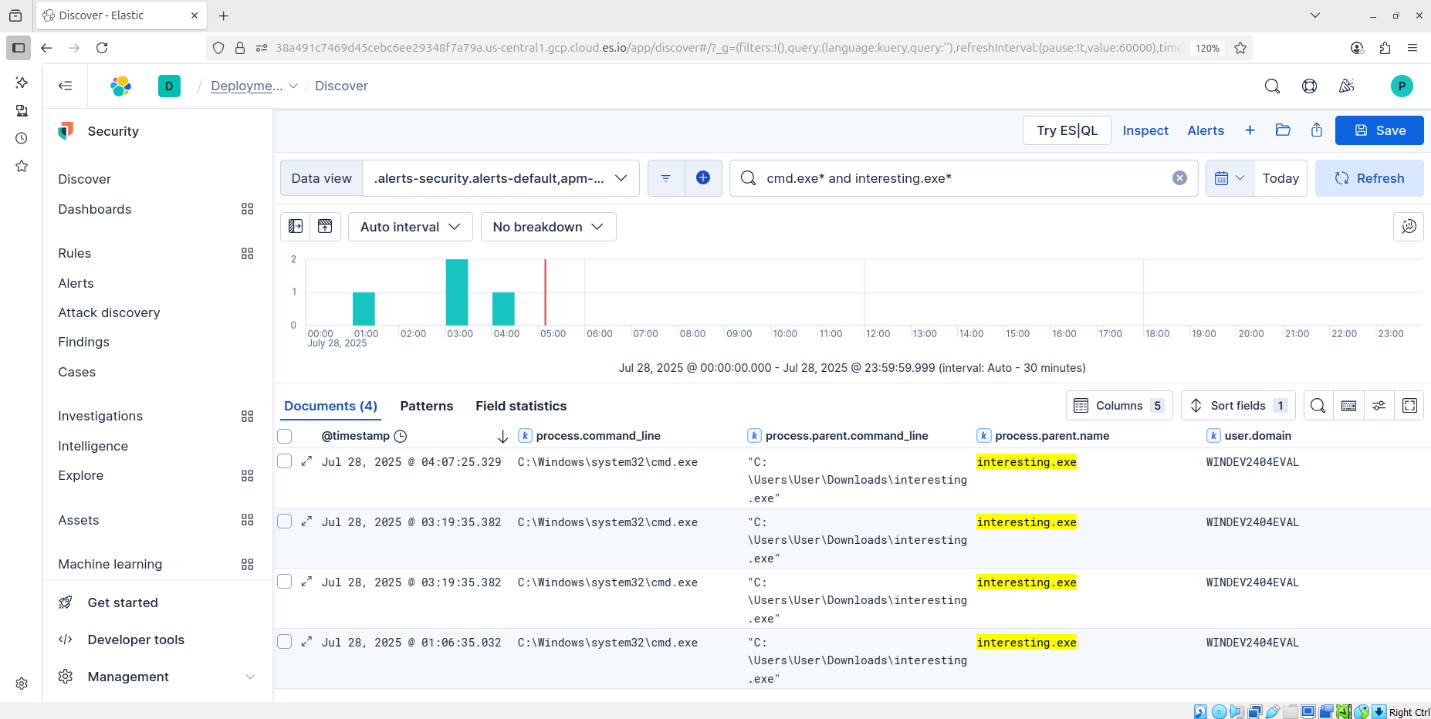
Upon opening the file in our victim machine, we can see a meterpreter session will be opened in our attacker machine. And now, we can type shell and the shell is created , now we can access the victims machine remotely and execute commands. In the below screenshot, we can see that a process is created upon opening the shell. This will be logged into the SIEM via Sysmon windows operational tool.

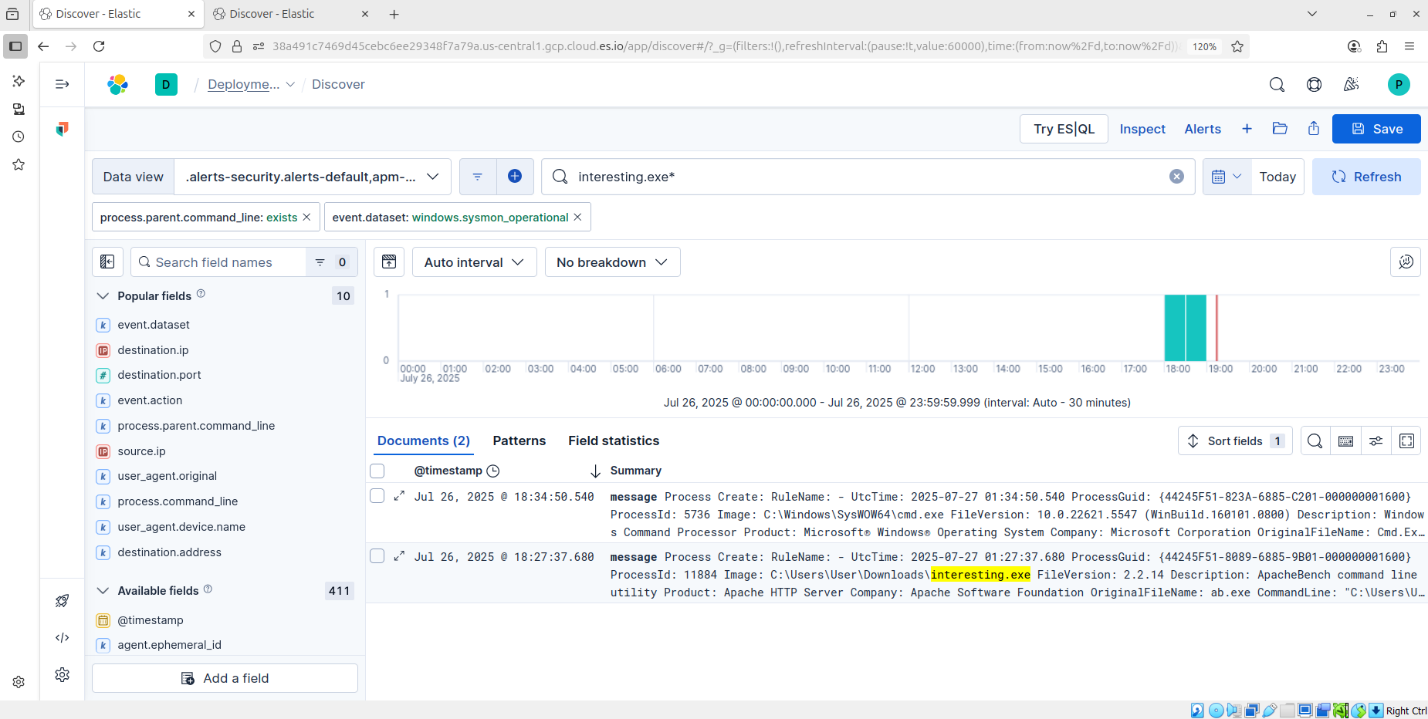


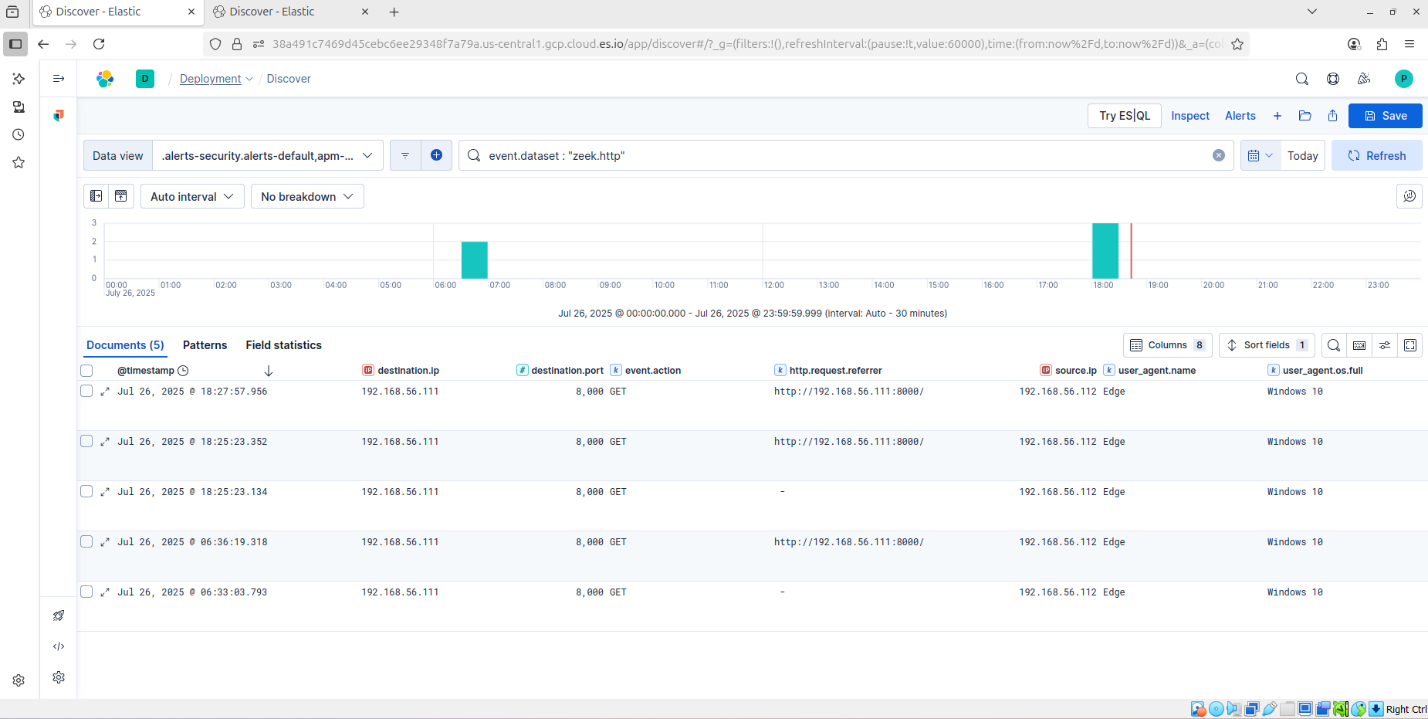
Now, In the below screenshot, we can see that upon executing the command “**whoami**” shows the machine name (victim machine name) as “**Windev2404eval**”

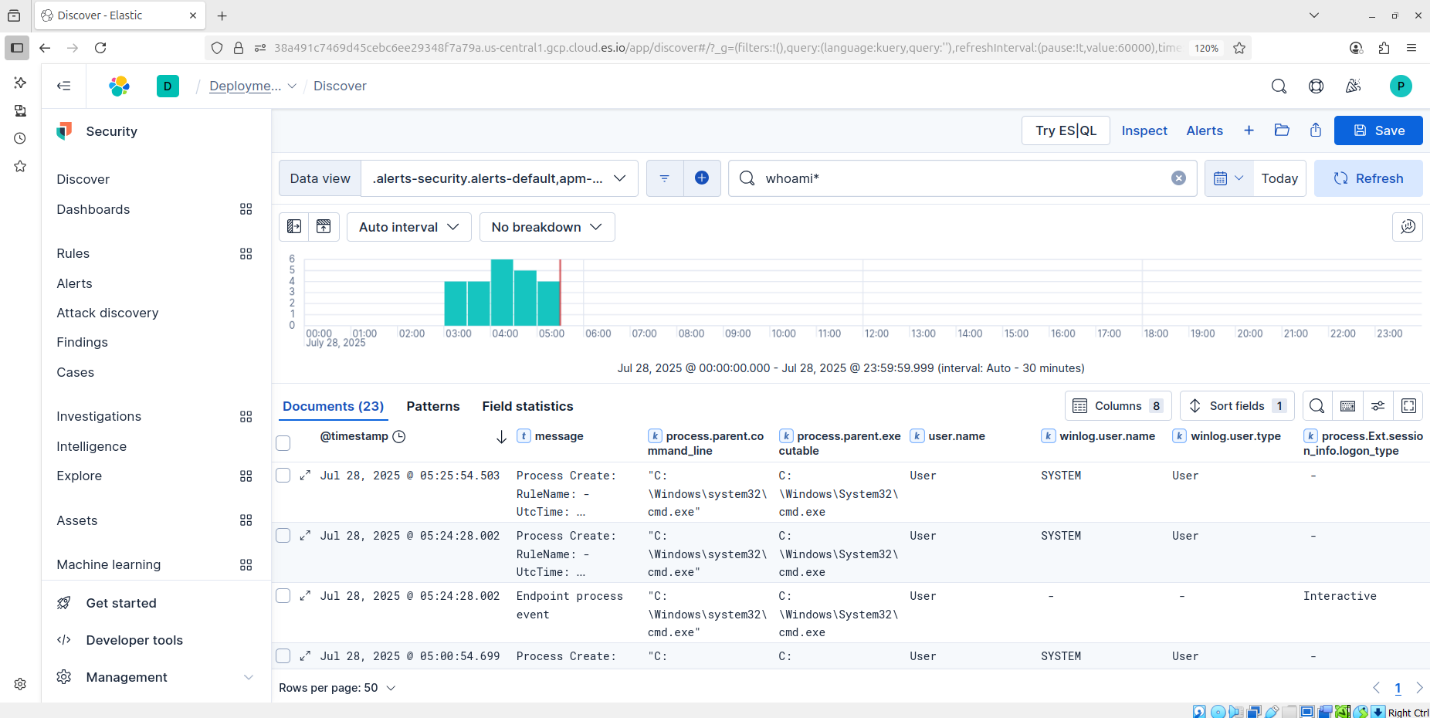


Now, we can check for logs in elastic discover tab.









In the above screenshot, we can see the logs for “whoami” command execution, I have generated logs from the remote meterpreter session and also by executing the whoami command in the windows powershell, the difference on logs can be clearly seen in the above screenshot.

The filed named “info\_logon\_type” shows interactive when the command is executed from a remote machine, and also we can see that the message for the log is shown as endpoint process event, a process is created remotely , and we do not get user name in the logs. So this is how we can identify if someone else remotely accessed our machine.

Next, a custom alert can be created when command prompt is accessed remotely.

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 1 alert is generated.

