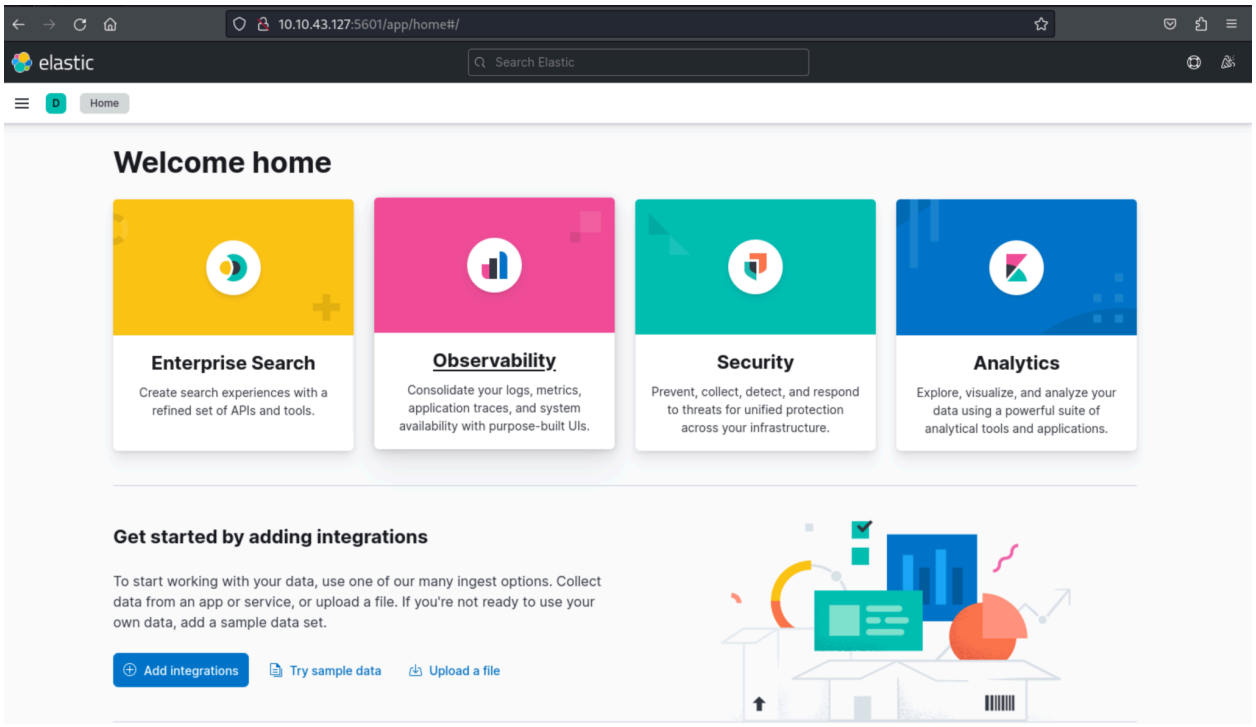
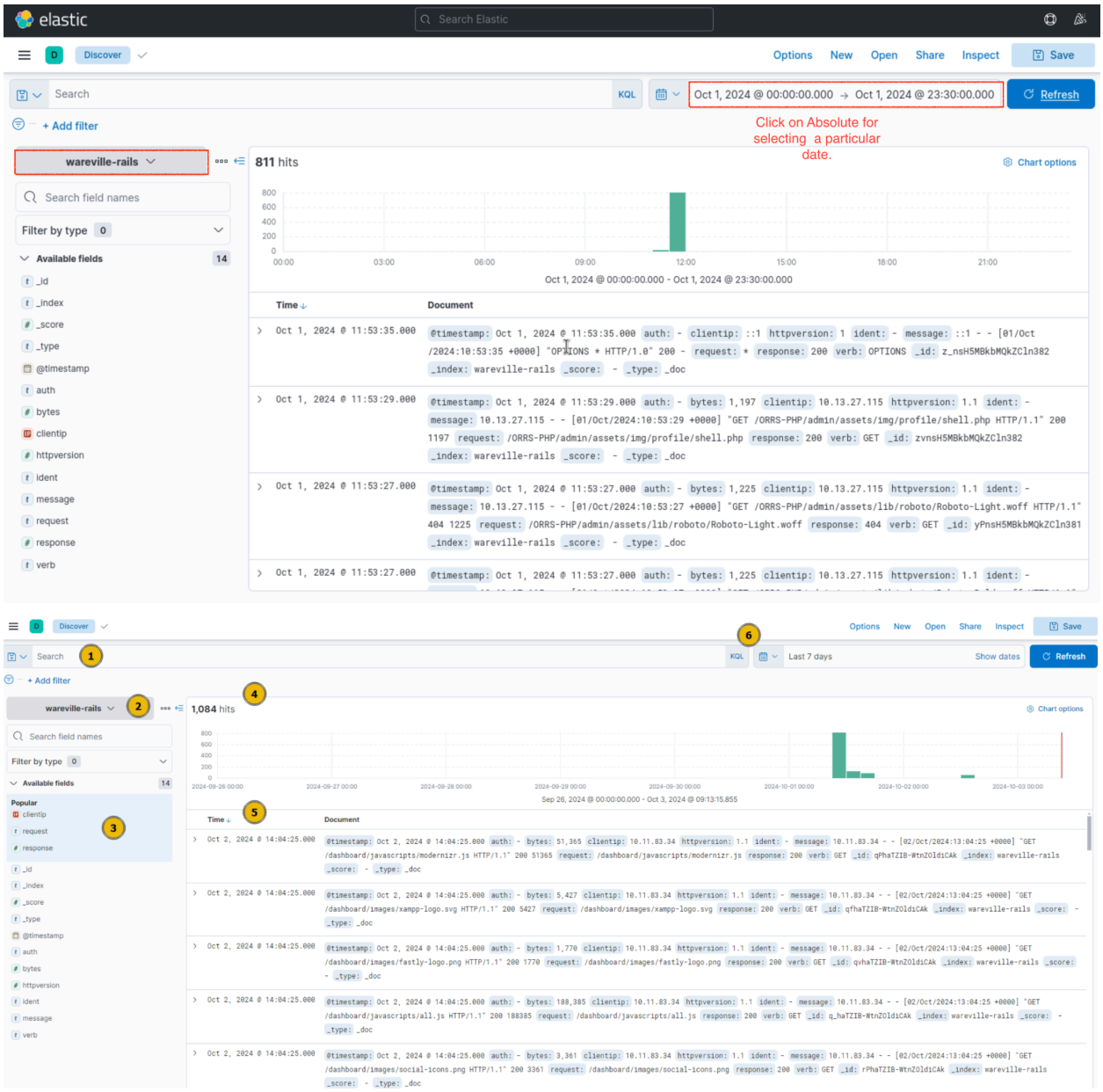
Day 3
Advent of Cyber 2024
Log Analysis

Log analysis can be a tedious process if you have a lot of endpoints and continuously generate a lot of logs. But tools like ELK which is a data analysis tool will make SOC engineer life easy. We will discuss more on analysing the logs in this document.

Opening up the website through the attackbox or your own VM via VPN (in my case).



Go to Kibana Discover on selecting the side menu and add the following option for seeing the logs.

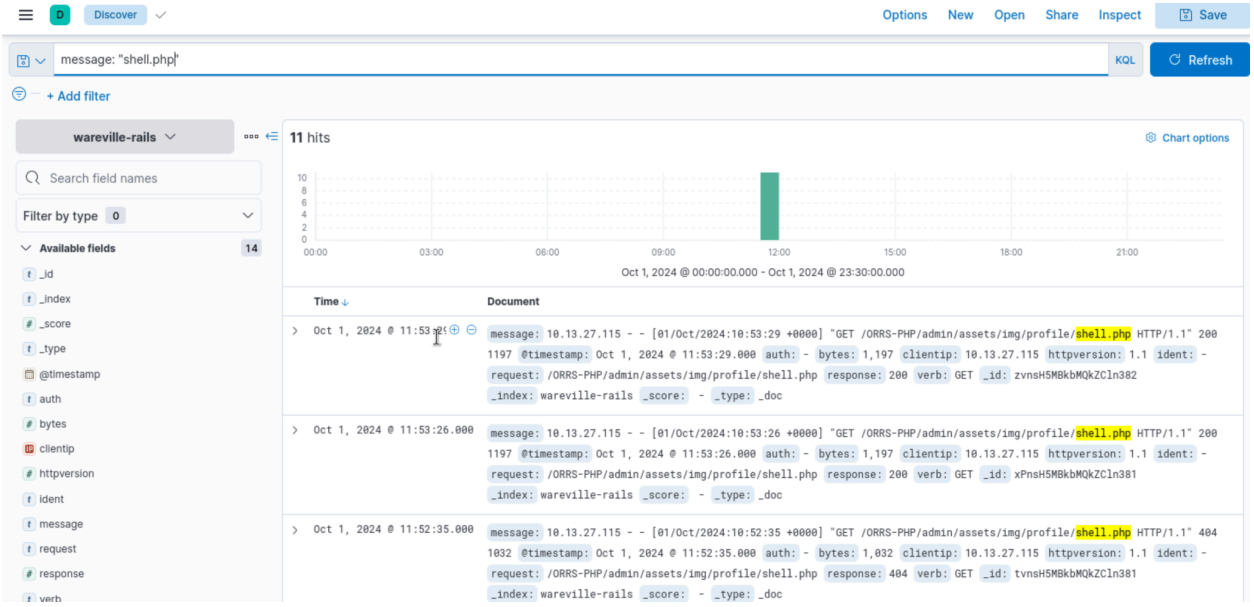


Important variables on this page

1. **Search Bar:** Here, we can place our search queries using KQL
2. **Index Pattern:** An index pattern is a collection of logs. This can be from a specific host or, for example, multiple hosts with a similar purpose (such as multiple web servers). In this case, the index pattern is all logs relating to "wareville-rails"
3. **Fields:** This pane shows us the fields that Elasticsearch has parsed from the logs. For example, timestamp, response type, and IP address.
4. **Timeline:** This visualisation displays the event count over a period of time
5. **Documents (Logs):** These entries are the specific entries in the log file

6. **Time Filter:** We can use this to narrow down a specific time frame (absolute). Alternatively, we can search for logs based on relativity. I.e. "Last 7 days".

From the screenshot below we can see that shell.php has been executed which we found through Kibana Query Language.



We can find useful information like this through choosing right IP options and other column variables.

Restricted file uploads
Having a weak username and passwords for servers allow attackers to upload malicious files. Having an input validation is very important for avoiding the .php and other scripts including javascript.

What is remote code execution (RCE)?
Remote code execution (RCE) happens when an attacker finds a way to run their own code on a system. This is a highly dangerous vulnerability because it can allow the attacker to take control of the system, exfiltrate sensitive data, or compromise other connected systems.

Chance of privilege escalation, total control of the system, even changing the user setting to steal company resources.

Web Shell
A web shell is a script that attackers upload to a vulnerable server, giving them remote control over it. Once a web shell is in place, attackers can run commands, manipulate files, and essentially use the compromised server as their own. They can even use it to launch attacks on other systems.

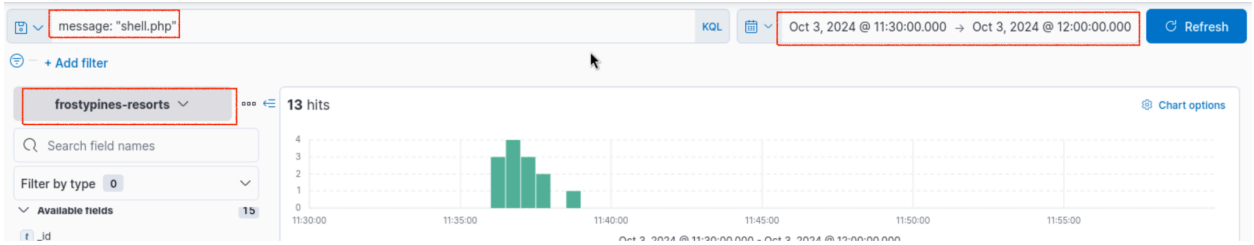
Remote code execution

1. Sending a script
2. Script has a reverse TCP or protocol for reverse connection
3. Privilege escalation.
4. Lateral movement.
5. Full Control of the system.

Below is the screenshot of the reverse script which is going to be executed on the malicious website which allows unrestricted upload.

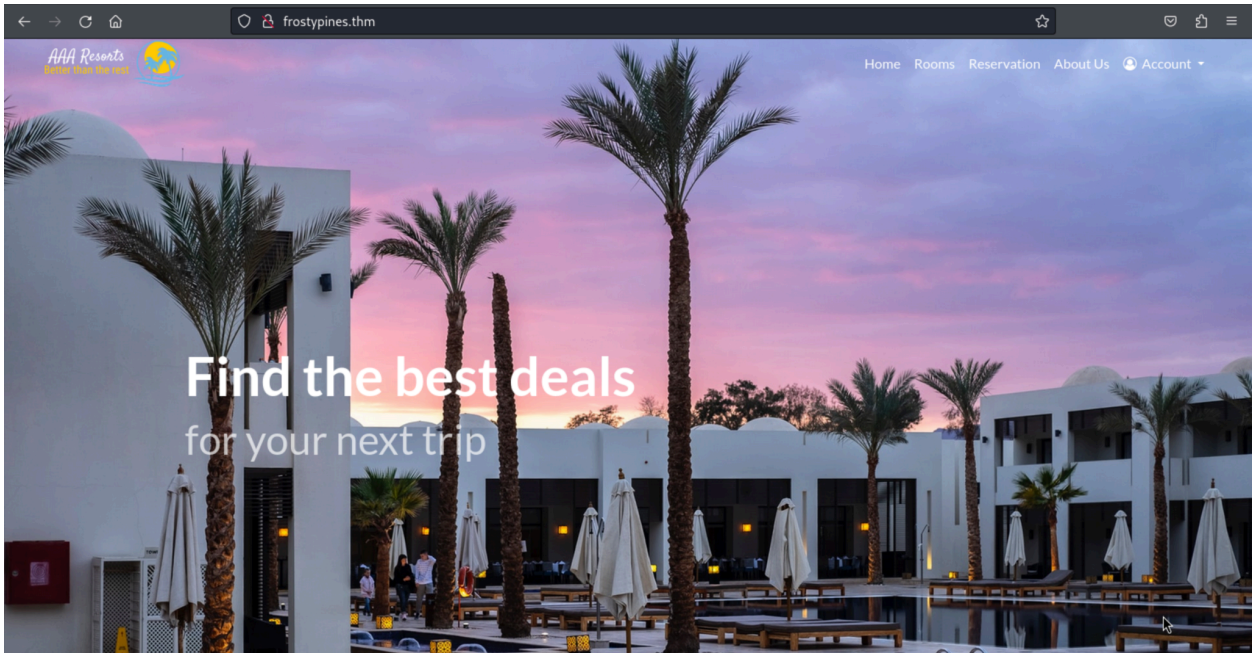
We are going to upload this malicious script on this website.

Before doing this task let's complete two questions which should be filled through the blue team part. We need to investigate the shell script on the day Oct 3 from 11.30 to 12.30.
Hint: use the following setting below.
Once the hint is used you can answer the first two questions.



For getting the flag, open the website, if it's not opening in the first attempt try to run this command on your terminal with root privileges.

```
echo "10.10.43.127 frostypines.thm" >> /etc/hosts
```

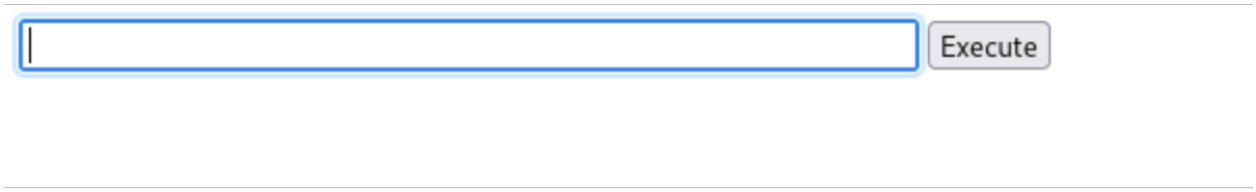


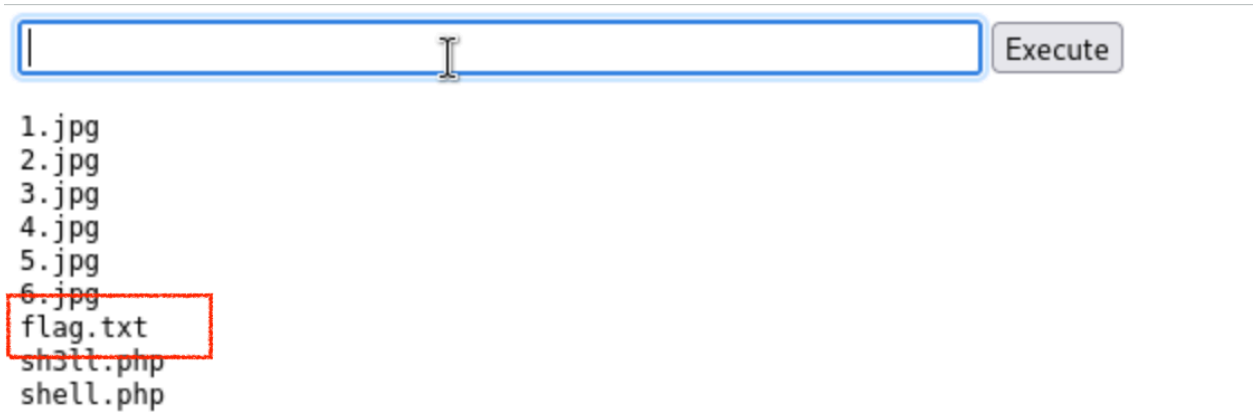
Above '**echo'** command will help to map the ip address to the following domain.

Brainstorm and think of the previous analysis from the blue team to know the possible location of the shell.php file.

Above image is the first hint, next try to look more into the logs of the blue team. Now again try to verify which path may be used.

Second hint:
Use admin privileges, look for ways how you can gain admin privilege for that website.
Look for pages that have upload options. Open the shell on new page.
Boom you will get the shell.





That’s all the lab is complete for today.
Take a rest and treat yourself for tomorrow.
Learning day by day is a good progress.