

ISSACK WAITHAKA
cs-sa07-24085

Junior Security Analyst Intro

- Most work of a Junior Security Analyst is to triage or monitor event logs and alert
- His roles are mostly to monitor and investigate alerts, configure and manage security tools, participate in SOC working groups etc.

Questions

1.

Answer the questions below

What will be your role as a Junior Security Analyst?

Triage Specialist

✓ Correct Answer

Security Operations Center(soc)

- The main function of SOC is to investigate, monitor, prevent and respond to threats

24/7

- Their activities include Ticketing, log collection, knowledge base, research, reporting etc.

A day in the life of a junior (associate) security Analyst

Questions

1.

Answer the questions below

Click on the green View Site button in this task to open the Static Site Lab and navigate to the security monitoring tool on the right panel to try to identify the suspicious activity.

 View Site

No answer needed

✓ Correct Answer

What was the malicious IP address in the alerts?

221.181.185.159

✓ Correct Answer

💡 Hint

20:08

OWASP Top 10 V x | Internet Speed T x | triaging meaning x | +

3

30% 30% 30%

50

UK US Brazil China Russia N. Korea

Operations: Information 1/3

✓ Woop woop! Your answer is correct

Alert Log

Date	Message
April 16th 2024, 05:27:00:347	Successful SSH authentication attempt to port 22 from IP address 221.181.185.159
April 16th 2024, 05:25:28:235	Unauthorized connection attempt detected from IP address 221.181.185.159 to port 22
April 16th 2024, 02:43:22:456	The user John Doe logged in successfully (Event ID 4624)
April 16th 2024, 02:43:20:658	Multiple failed login attempts from John Doe
April 16th 2024, 02:30:20:215	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

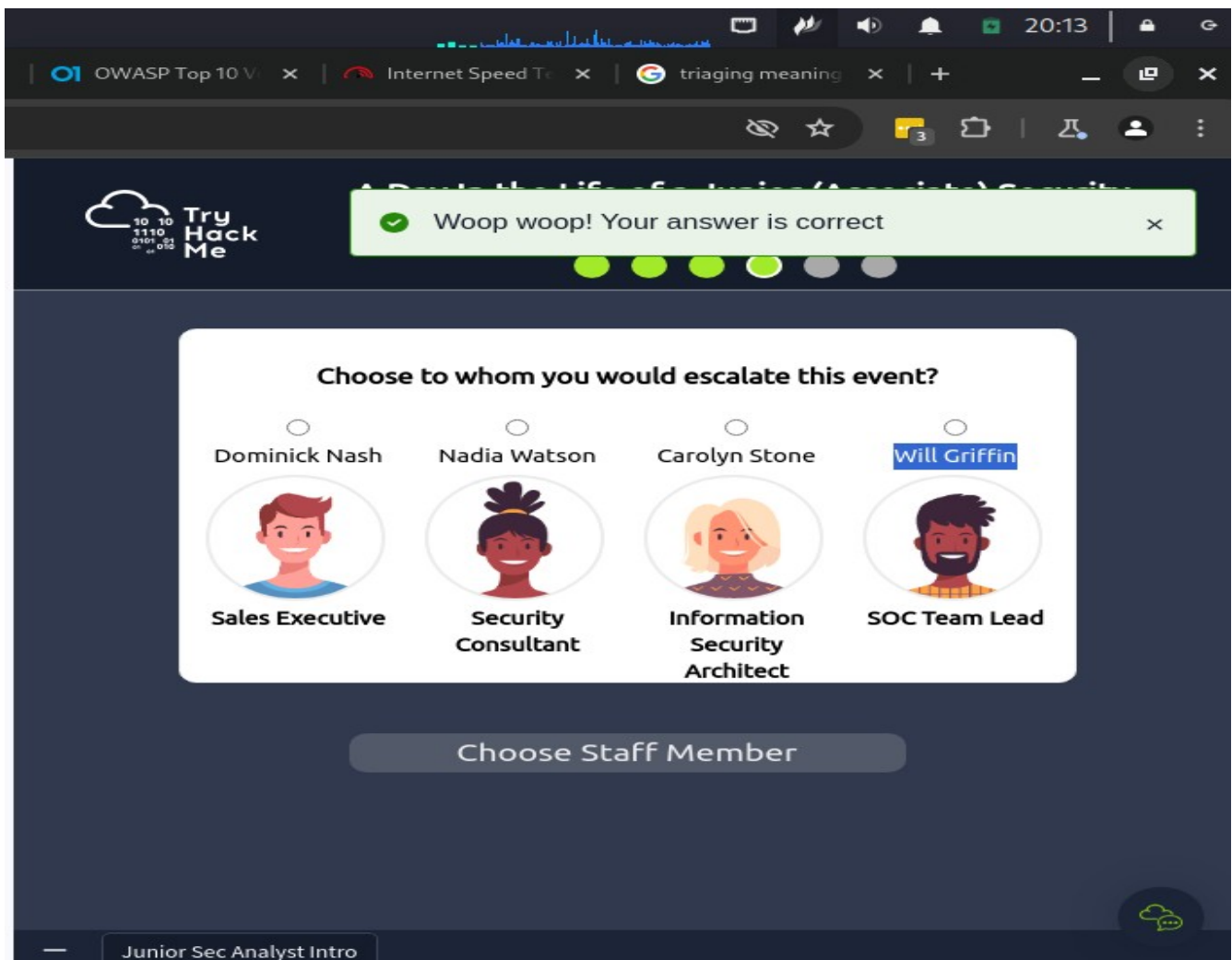
Junior Sec Analyst Intro

3.

To whom did you escalate the event associated with the malicious IP address?

Will Griffin

✓ Correct Answer

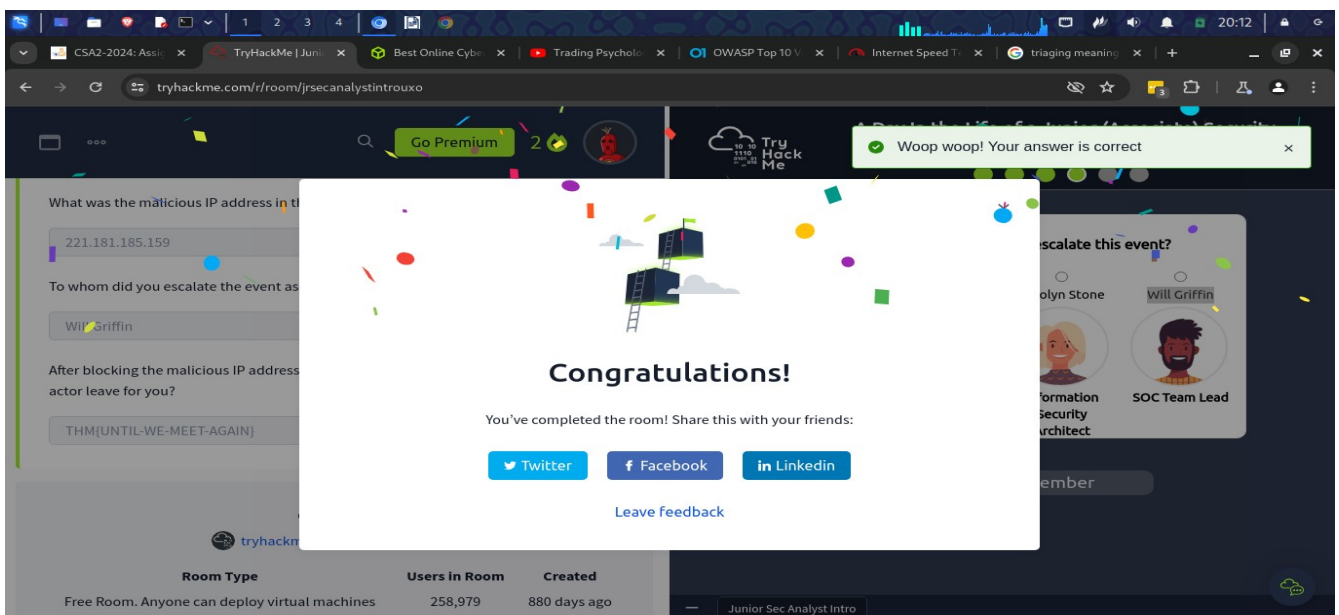
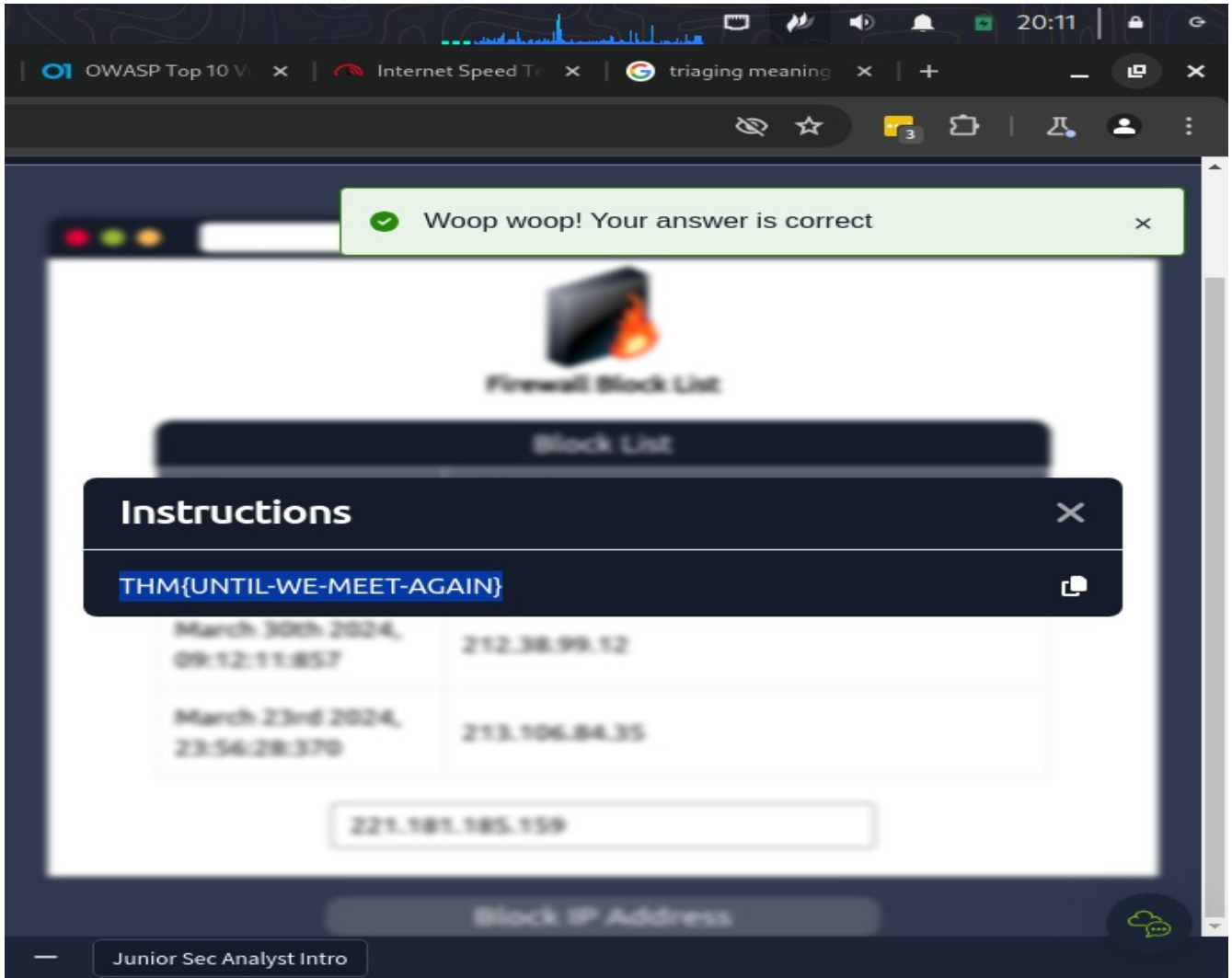


4.

After blocking the malicious IP address on the firewall, what message did the malicious actor leave for you?

THM{UNTIL-WE-MEET-AGAIN}

✓ Correct Answer



Conclusion

In this room I got the chance to be a junior security analyst. I have learn what a junior analyst mainly do. I was able to do some of the activities the junior security analyst does. I cant wait to be one. It seems fun.