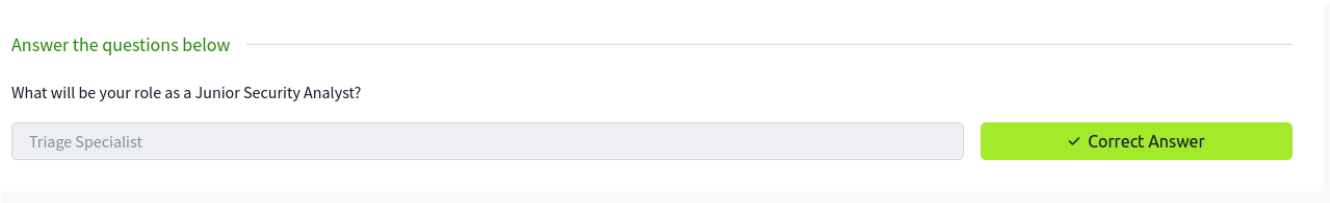
ISSACK WAITHAKA
cs-sa07-24085

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.



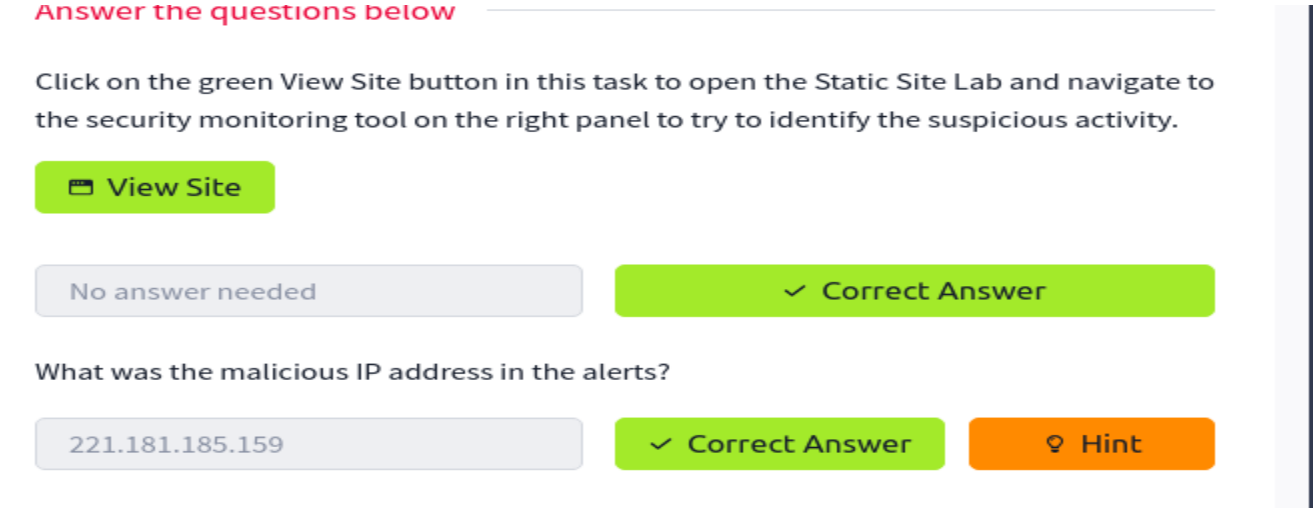
Security Operations Center(soc)

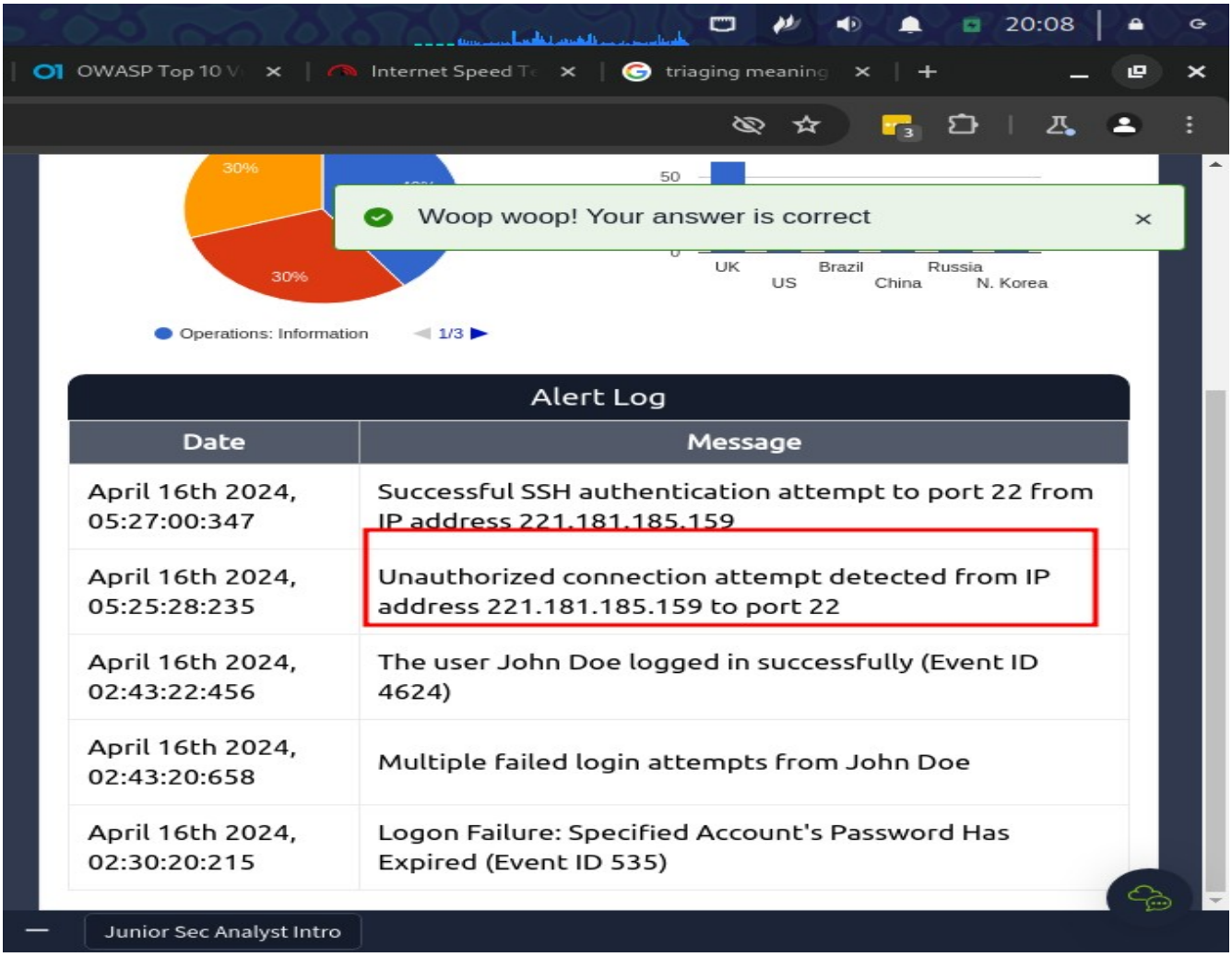
- The main function of SOC is to investigate, monitor, prevent and respond to threats 24/7
- Their activities include Ticketing, log collection, knowledge base, research, reporting etc.

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

Questions

1.



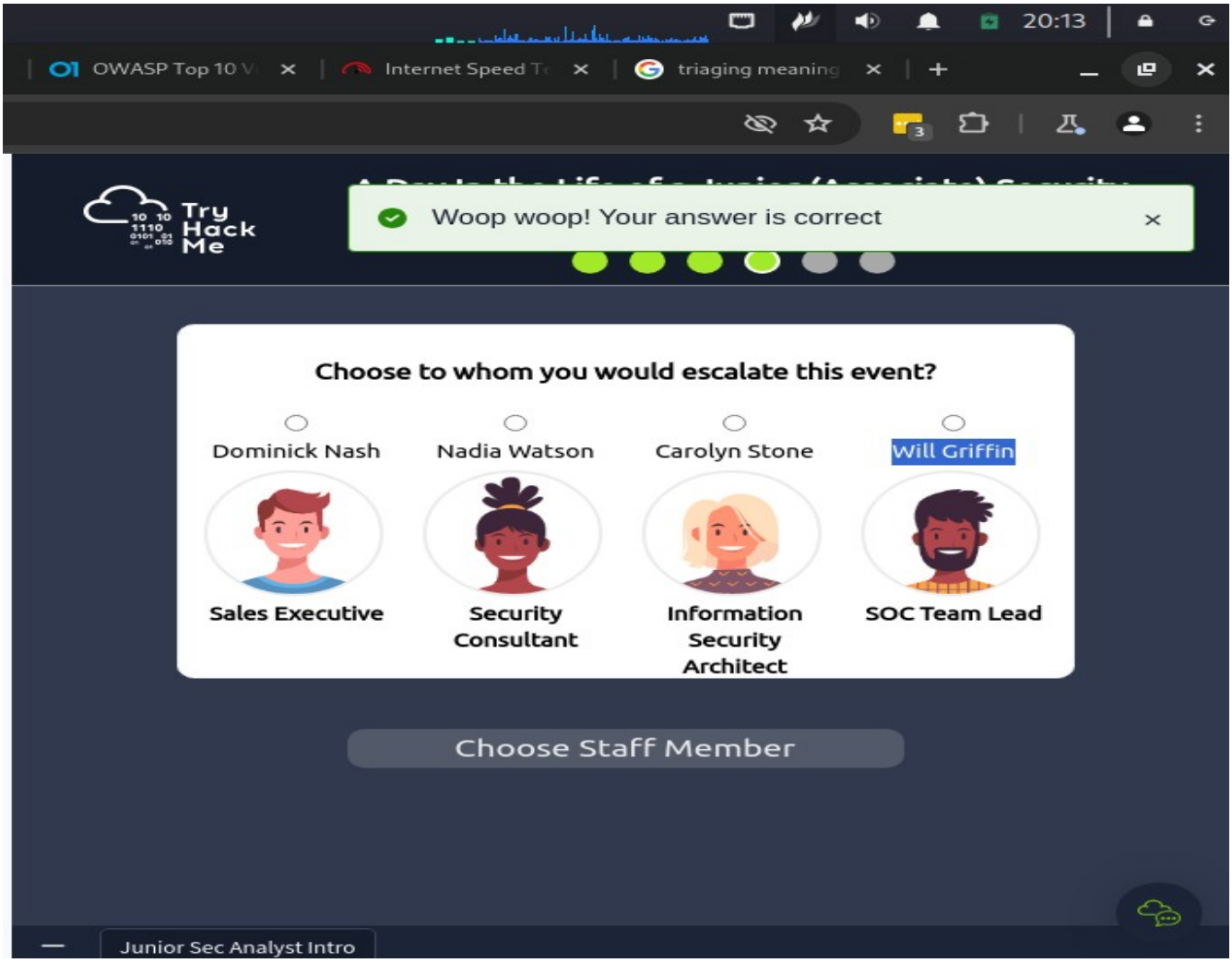


3.

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

Will Griffin

✓ Correct Answer

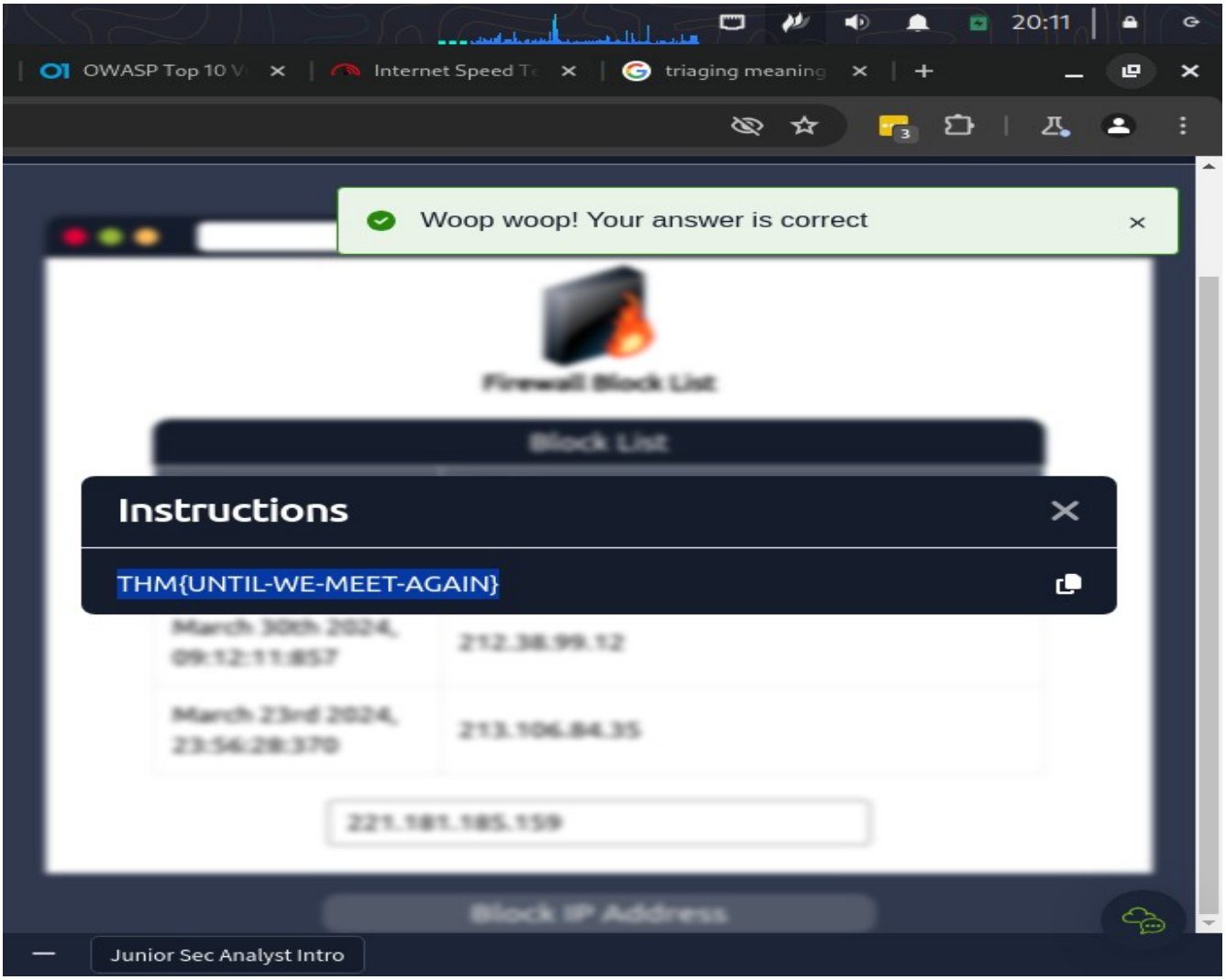


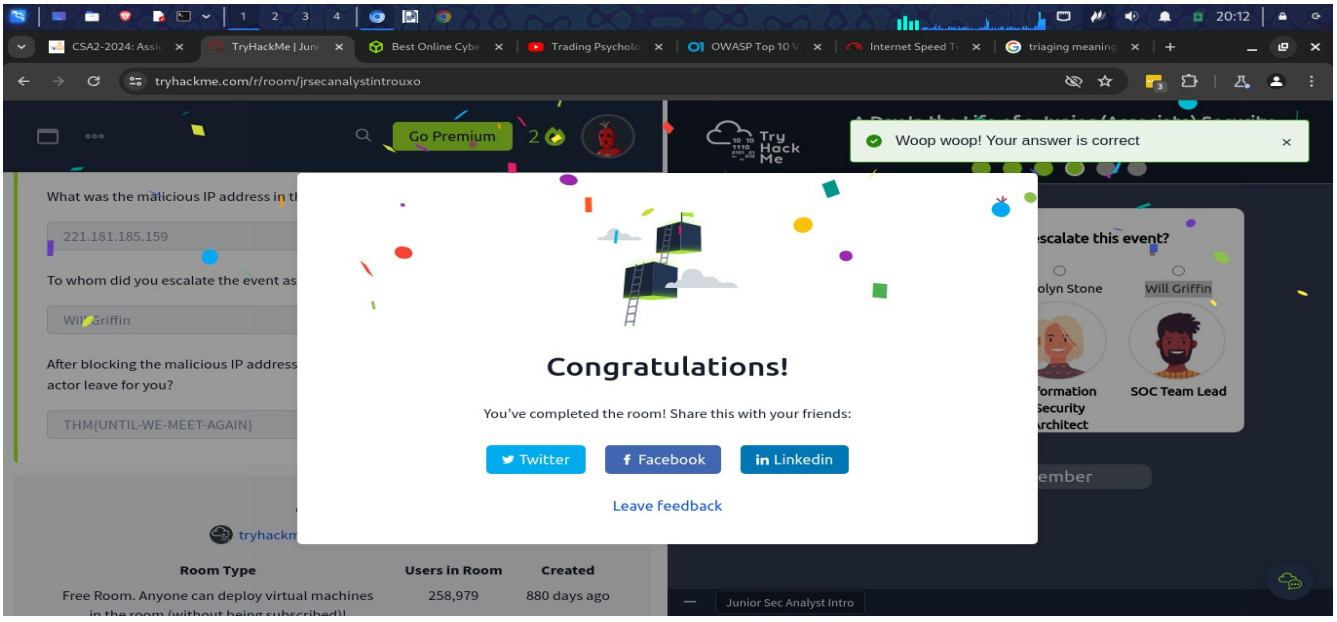
4.

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


Woop woop! Your answer is correct
Instructions
THM{UNTIL-WE-MEET-AGAIN}
Junior Sec Analyst Intro


tryhackme.com/r/room/jrsecanalystintrouxo
Go Premium
Woop woop! Your answer is correct
Congratulations!
You've completed the room! Share this with your friends:
Twitter
Facebook
Linkedin
Leave feedback
Room Type
Users in Room
Created
Free Room. Anyone can deploy virtual machines
258,979
880 days ago
Junior Sec Analyst Intro

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.