Introduction:

- The role of a Junior Security Analyst is critical in maintaining the security posture of an organization. This report provides an overview of the responsibilities of a Junior Security Analyst, the functions of a Security Operations Centre (SOC), and a typical day in the life of a Junior Security Analyst.

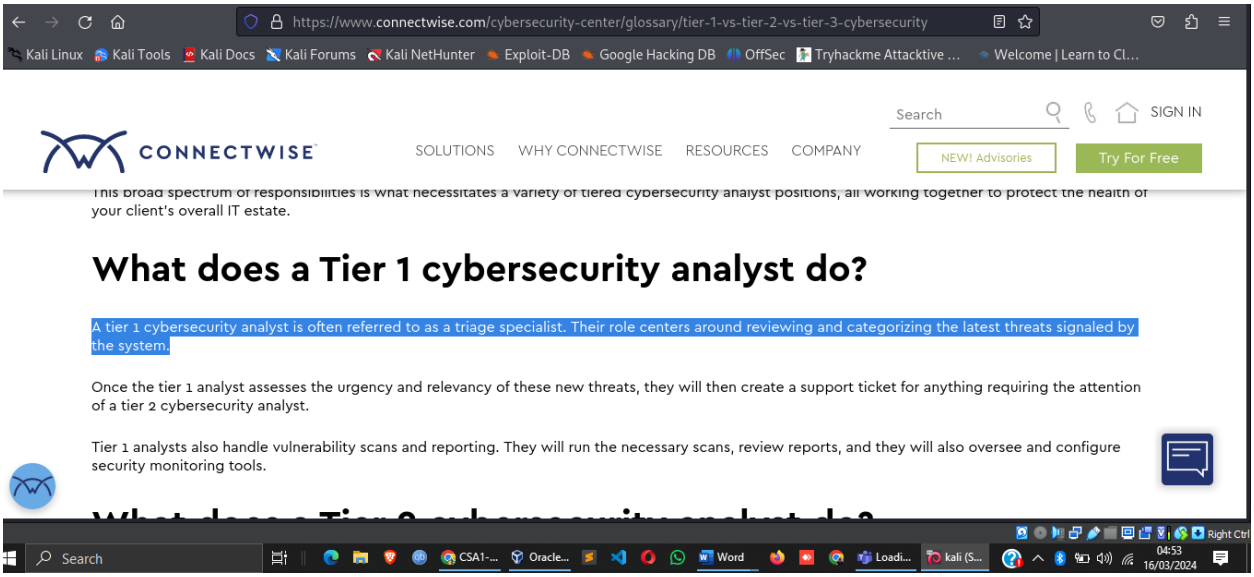
  https://tryhackme.com/p/Damiano254

Task 1: A Career as a Junior (Associate) Security Analyst

- Role: Triage Specialist
- Responsibilities:
  - Monitor and investigate alerts
  - Configure and manage security tools
  - Develop and implement basic IDS signatures
  - Participate in SOC working groups and meetings
  - Escalate security incidents to Tier 2 and Team Lead if needed
- Required qualifications:
  - 0-2 years of Security Operations experience
  - Basic understanding of Networking and Operating Systems
  - Scripting/programming skills are a plus
- Desired certification: CompTIA Security+
- Career progression: Move up to Tier 2 and Tier 3 roles.

  Questions:

  - What will be your role as a Junior Security Analyst?
    Triage Specialist



Task 2: Security Operations Centre (SOC)

- Core functions of a SOC:
    - Preparation and prevention
    - Monitoring and investigation
    - Response
- Preparation involves staying informed of current cybersecurity threats, gathering intelligence data, and maintaining security tools.
- Monitoring and investigation are conducted using SIEM and EDR tools, prioritizing alerts, and conducting thorough investigations.
- Response includes coordinating and taking action on compromised hosts.

Task 3: A Day in the Life of a Junior (Associate) Security Analyst

- Daily tasks include:
    - Working with various log sources
    - Monitoring network traffic
    - Analyzing IPS and IDS alerts
    - Investigating suspicious emails
    - Extracting forensics data
- Incident Response tasks may involve detecting, containing, and remediating potential attacks.

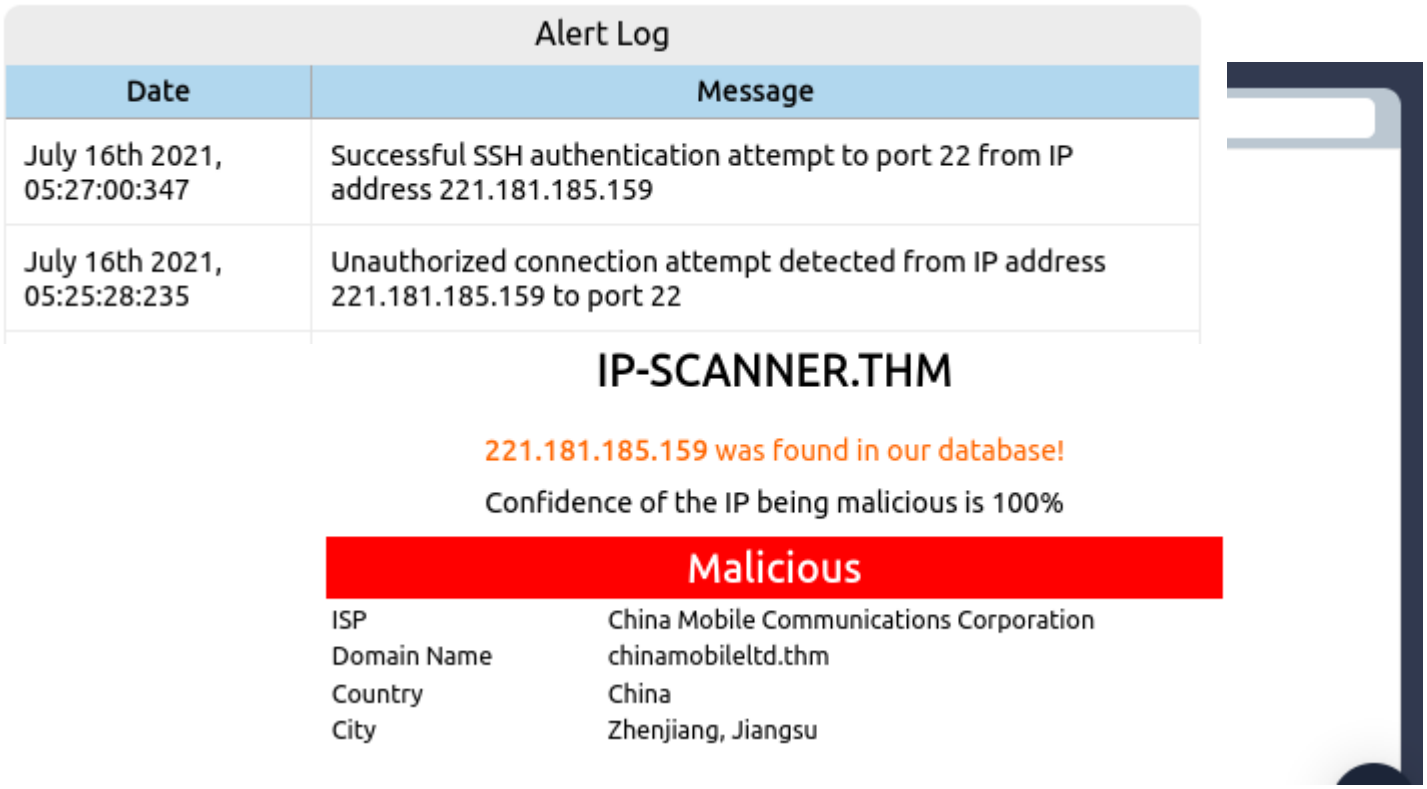
Answer the questions below

- 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.

  No answer needed

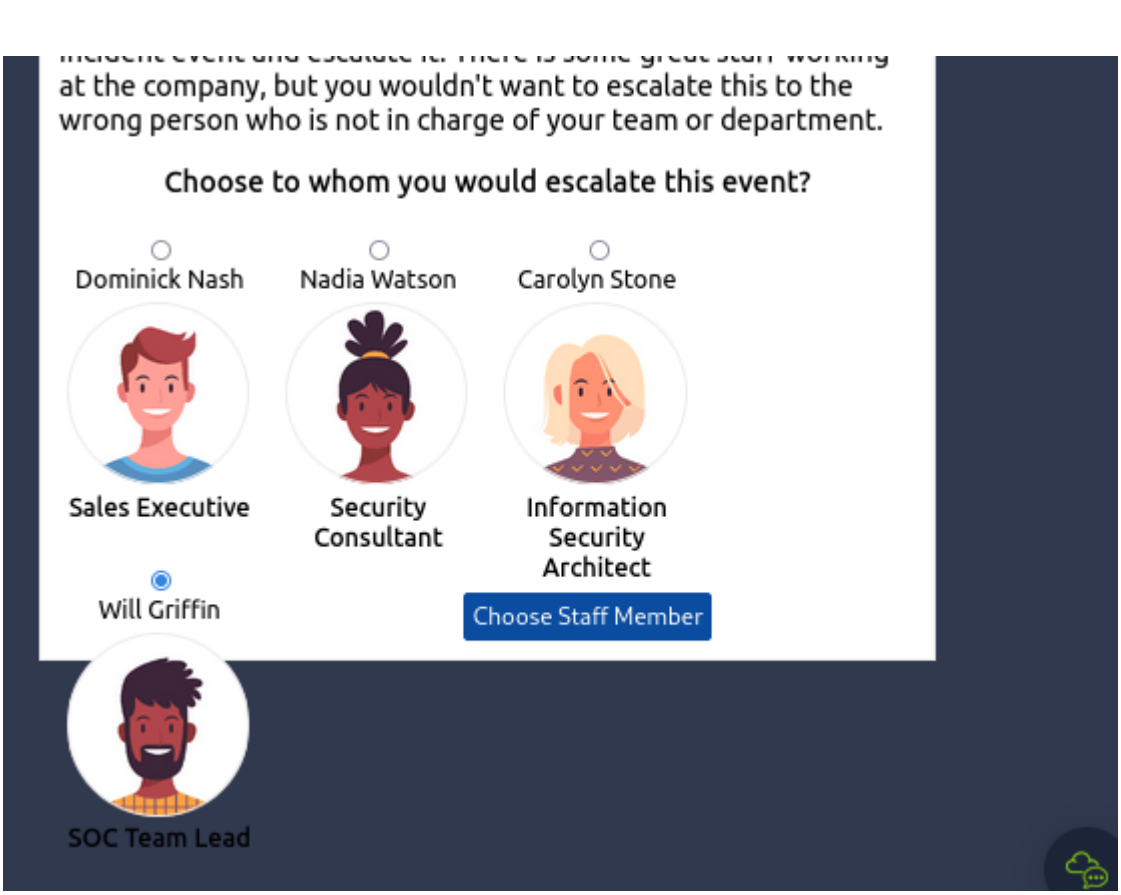
- What was the malicious IP address in the alerts?

  221.181.185.159



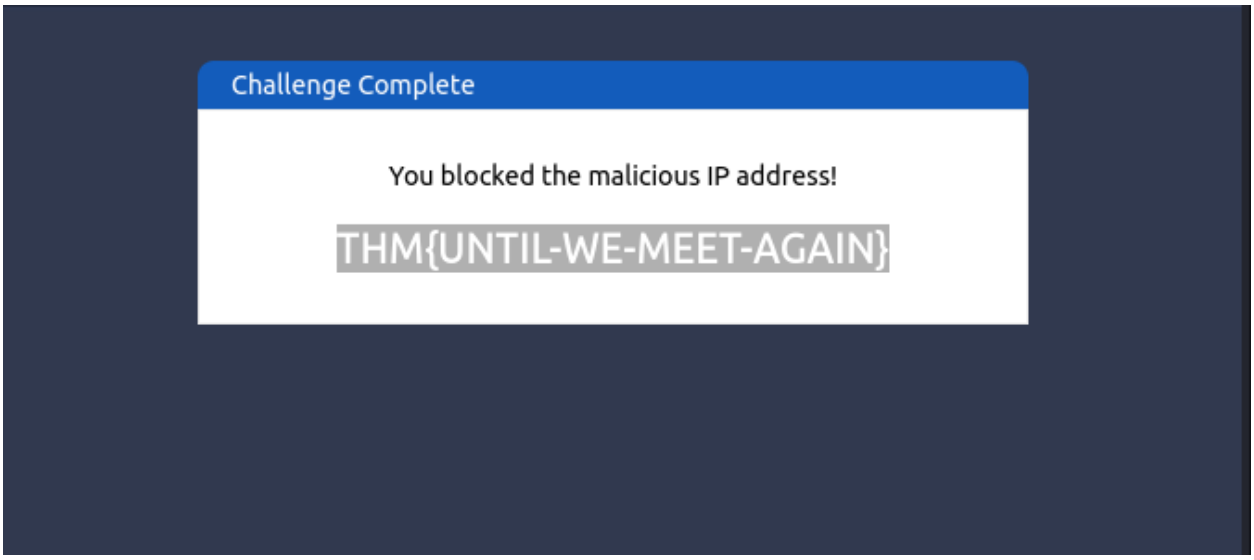
- To whom did you escalate the event associated with the malicious IP address?

  Will Griffin



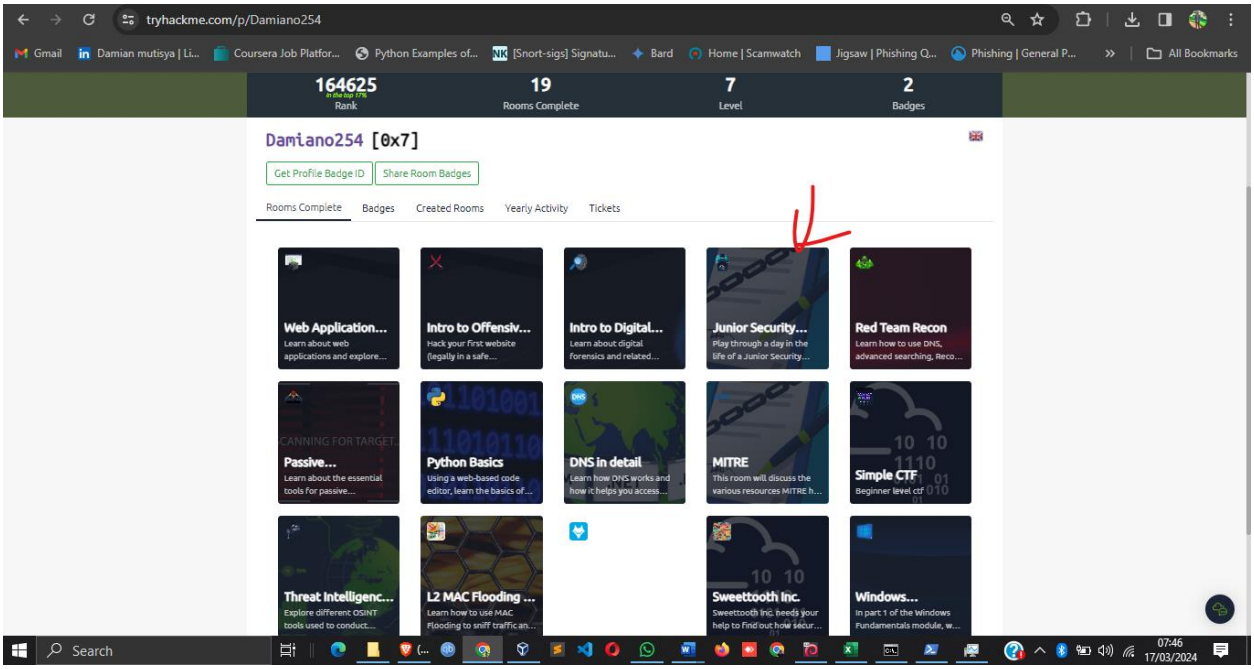
- After blocking the malicious IP address on the firewall, what message did the malicious actor leave for you?

  THM{UNTIL-WE-MEET-AGAIN}



Conclusion:

A Junior Security Analyst's job responsibilities are diverse, encompassing tasks such as monitoring for cybersecurity threats, investigating potential security incidents, and responding to confirmed threats. Through active participation in Security Operations Centre (SOC) activities, Junior Security Analysts contribute significantly to preserving an organization's security posture. Their skills and expertise are vital in detecting and mitigating cyber threats, thereby safeguarding the organization's assets and data.


tryhackme.com/p/Damiano254
Gmail
Damian mutisya | Li...
Coursera Job Platfor...
Python Examples of...
[Snort-sigs] Signatu...
Bard
Home | Scamwatch
Jigsaw | Phishing Q...
Phishing | General P...
All Bookmarks
164625
Rank
19
Rooms Complete
7
Level
2
Badges
Damiano254 [0x7]
Get Profile Badge ID
Share Room Badges
Rooms Complete
Badges
Created Rooms
Yearly Activity
Tickets
Web Application...
Learn about web applications and explore...
Intro to Offensiv...
Hack your first website (legally in a safe...
Intro to Digital...
Learn about digital forensics and related...
Junior Security...
Play through a day in the life of a Junior Security...
Red Team Recon
Learn how to use DNS, advanced searching, Reco...
Passive...
Learn about the essential tools for passive...
Python Basics
Using a web-based code editor, learn the basics of...
DNS in detail
Learn how DNS works and how it helps you access...
MITRE
This room will discuss the various resources MITRE h...
Simple CTF
Beginner level ctf
Threat Intelligenc...
Explore different OSINT tools used to conduct...
L2 MAC Flooding ...
Learn how to use MAC Flooding to sniff traffic an...
Sweettooth Inc.
Sweettooth Inc. needs your help to find out how secur...
Windows...
In part 1 of the Windows Fundamentals module, w...
Search
07:46
17/03/2024