Junior Security Analyst Intro | Tryhackme Writeup/Walkthrough | By Md Amiruddin

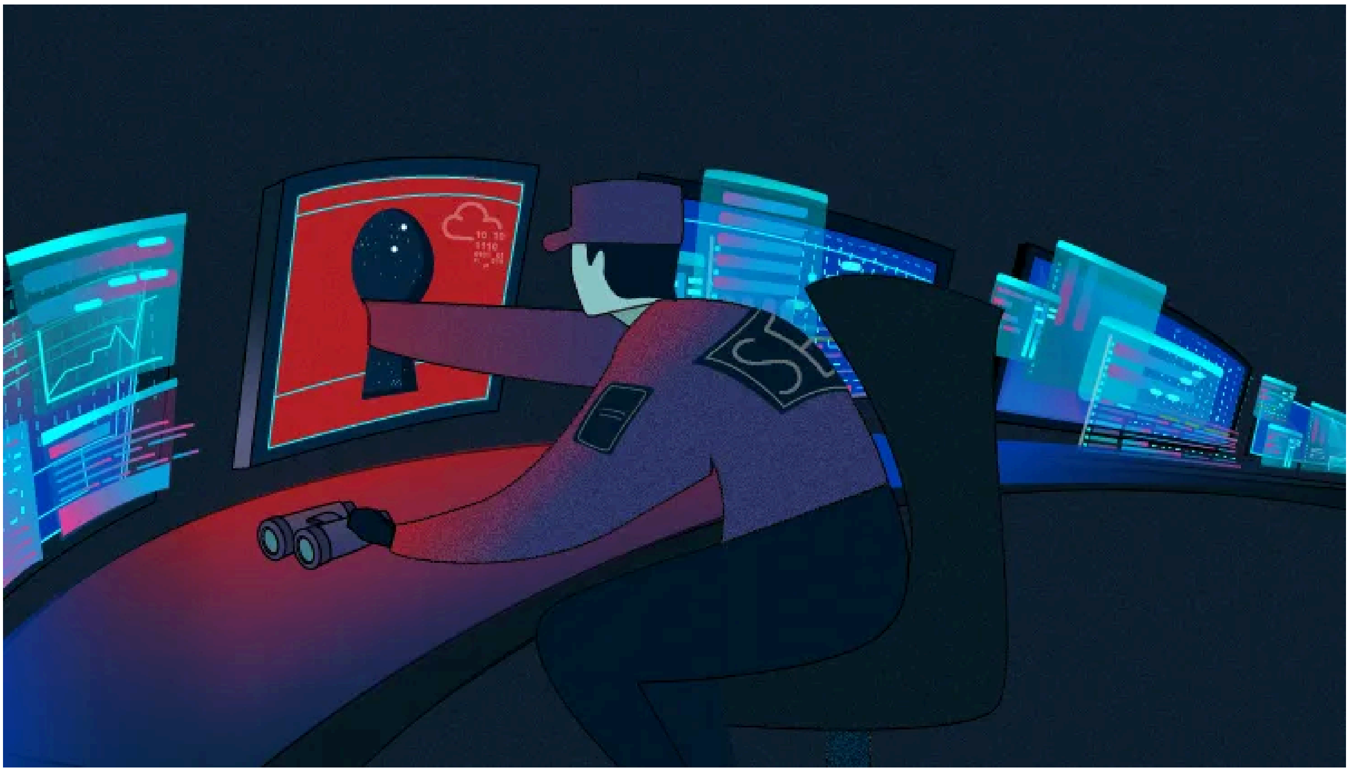
Md Amiruddin · Follow

6 min read · Feb 17, 2023

Listen Share More

Play through a day in the life of a Junior Security Analyst, their responsibilities and qualifications needed to land a role as an analyst.

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



In the Junior Security Analyst role, you will be a Triage Specialist. You will spend a lot of time triaging or monitoring the event logs and alerts.

The responsibilities for a Junior Security Analyst or Tier 1 SOC Analyst include:

- Monitor and investigate the alerts (most of the time, it's a 24x7 SOC operations environment)
- Configure and manage the security tools
- Develop and implement basic IDS (Intrusion Detection System) signatures
- Participate in SOC working groups, meetings
- Create tickets and escalate the security incidents to the Tier 2 and Team Lead if needed

Required qualifications (most common):

- 0–2 years of experience with Security Operations
- Basic understanding of Networking (OSI model (Open Systems Interconnection Model) or TCP/IP model (Transmission Control Protocol/Internet Protocol Model)), Operating Systems (Windows, Linux), Web applications. To further learn about OSI and TCP/IP models, please refer to the Introductory Networking Room.

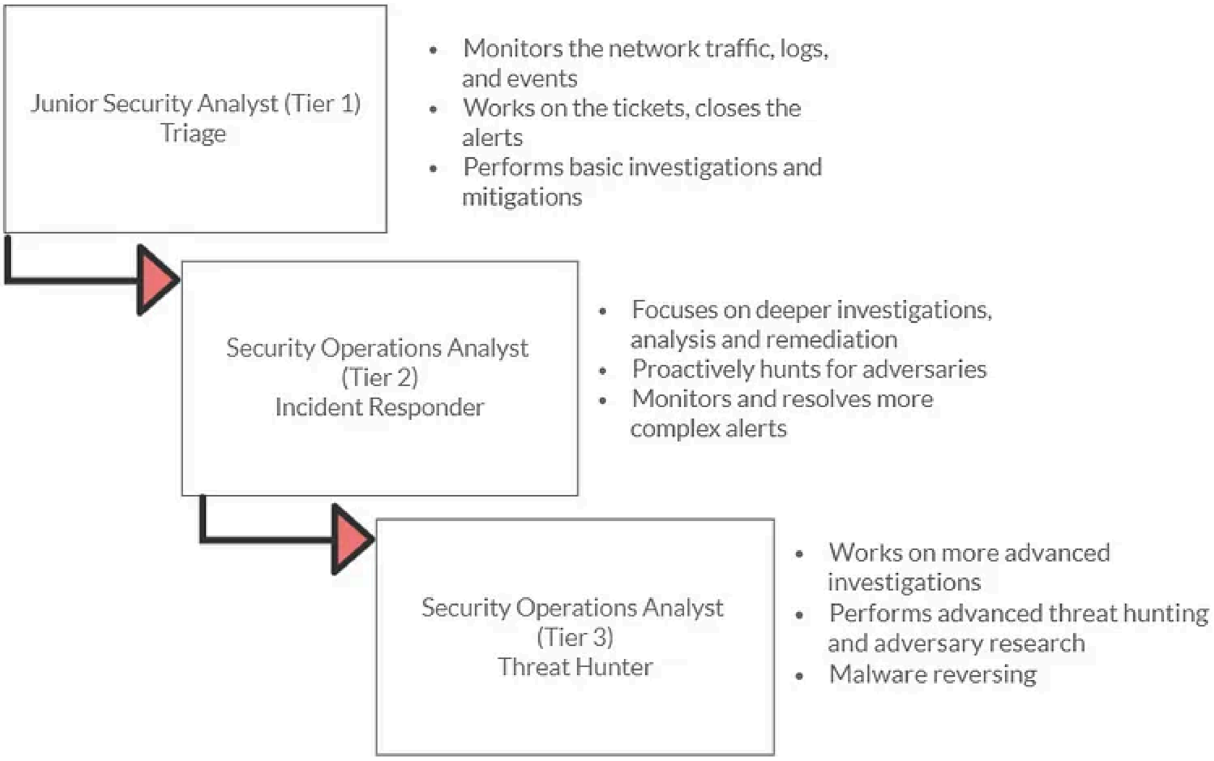
- Scripting/programming skills are a plus

Desired certification:

- CompTIA Security+

As you progress and advance your skills as a Junior Security Analyst, you will eventually move up to Tier 2 and Tier 3.

An overview of the Security Operations Center (SOC) Three-Tier Model:


Junior Security Analyst (Tier 1)
Triage
Monitors the network traffic, logs, and events
Works on the tickets, closes the alerts
Performs basic investigations and mitigations
Security Operations Analyst (Tier 2)
Incident Responder
Focuses on deeper investigations, analysis and remediation
Proactively hunts for adversaries
Monitors and resolves more complex alerts
Security Operations Analyst (Tier 3)
Threat Hunter
Works on more advanced investigations
Performs advanced threat hunting and adversary research
Malware reversing

Answer the questions below :

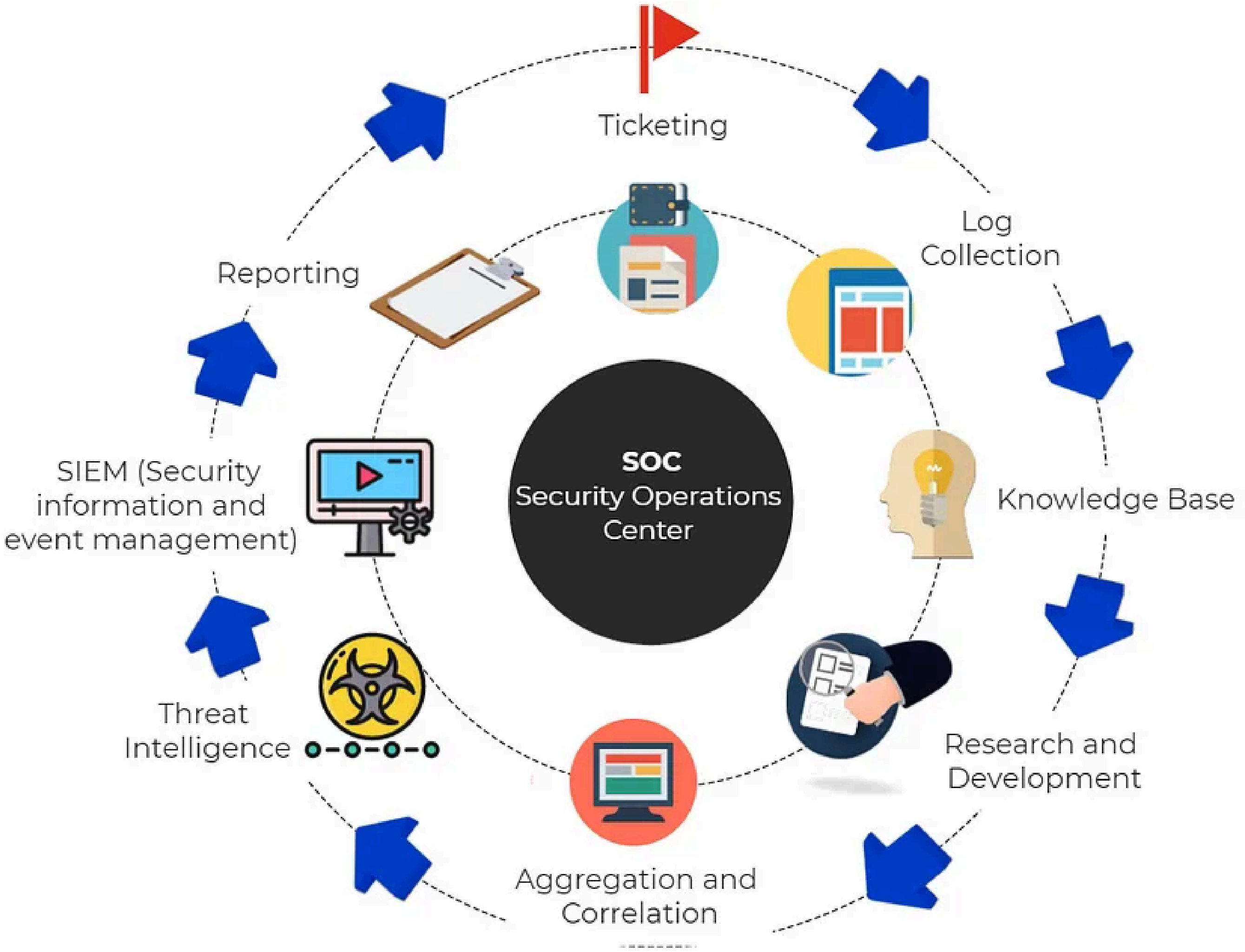
```
1. What will be your role as Junior Security Analyst?
A. Triage Specialist
```

Task 2 : Security Operations Center (SOC)

So, what exactly is a SOC?

The core function of a SOC (Security Operations Center) is to investigate, monitor, prevent, and respond to threats in the cyber realm 24/7 or around the clock. Per McAfee's definition of a SOC, "Security operations teams are charged with monitoring and protecting many assets, such as intellectual property, personnel data, business systems, and brand integrity. As the implementation component of an organization's overall cybersecurity framework, security operations teams act as the central point of collaboration in coordinated efforts to monitor, assess, and defend against cyberattacks". The number of people working in the SOC can vary depending on the size of the organization.

What is included in the responsibilities for the SOC?


Ticketing
Log Collection
Knowledge Base
Research and Development
Aggregation and Correlation
Threat Intelligence
SIEM (Security information and event management)
Reporting
SOC
Security Operations Center

Preparation and Prevention

As a Junior Security Analyst, you should stay informed of the current cybersecurity threats (Twitter and Feedly can be great resources to keep up with the news related to Cybersecurity). It's crucial to detect and hunt threats, work on a security roadmap to protect the organization, and be ready for the worst-case scenario

Prevention methods include gathering intelligence data on the latest threats, threat actors, and their TTPs (Tactics, Techniques, and Procedures). It also includes the maintenance procedures like updating the firewall signatures, patching the vulnerabilities in the existing systems, block-listing and safe-listing applications, email addresses, and IPs.

To better understand the TTPs, you should look into one of the CISA's (Cybersecurity & Infrastructure Security Agency) alerts on APT40 (Chinese Advanced Persistent Threat). Refer to the following link for more information, https://us-cert.cisa.gov/ncas/alerts/aa21-200a.

Monitoring and Investigation

A SOC team proactively uses SIEM (Security information and event management) and EDR (Endpoint Detection and Response) tools to monitor suspicious and malicious network activities. Imagine being a firefighter and having a multi-alarm fire — one-alarm fires, two-alarm fires, three-alarm fires; the categories classify the seriousness of the fire, which is a threat in our case. As a Security Analyst, you will learn how to prioritize the alerts based on their level: Low, Medium, High, and Critical. Of course, it is an easy guess that you will need to start from the highest level (Critical) and working towards the bottom — Low-level alert. Having properly configured security monitoring tools in place will give you the best chance to mitigate the threat.

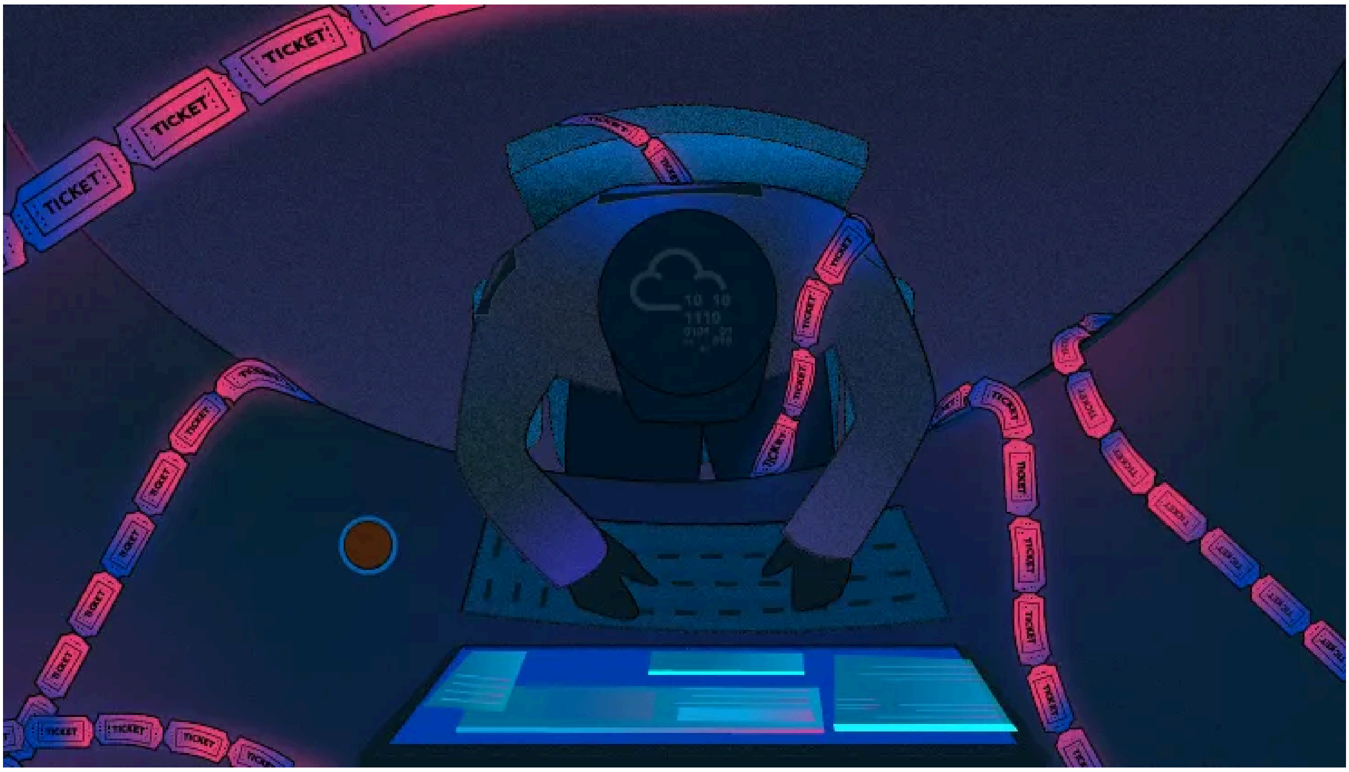
Junior Security Analysts play a crucial role in the investigation procedure. They perform triaging on the ongoing alerts by exploring and understanding how a certain attack works and preventing bad things from happening if they can. During the investigation, it's important to raise the question "How? When and why?". Security Analysts find the answers by drilling down on the data logs and alerts in combination with using the open-source tools, which we will have a chance to explore later in this path.

Response

After the investigation, the SOC team coordinates and takes actions on the compromised hosts, which involves isolating the hosts from the network, terminating the malicious processes, deleting files, and more.

```
Read Above.
```

Task 3 : A day In the life of a Junior (Associate) Security Analyst



To understand the job responsibilities for a Junior (Associate) Security Analyst, let us first show you what a day in the life of the Junior Security Analyst looks like and why this is an exciting career journey.

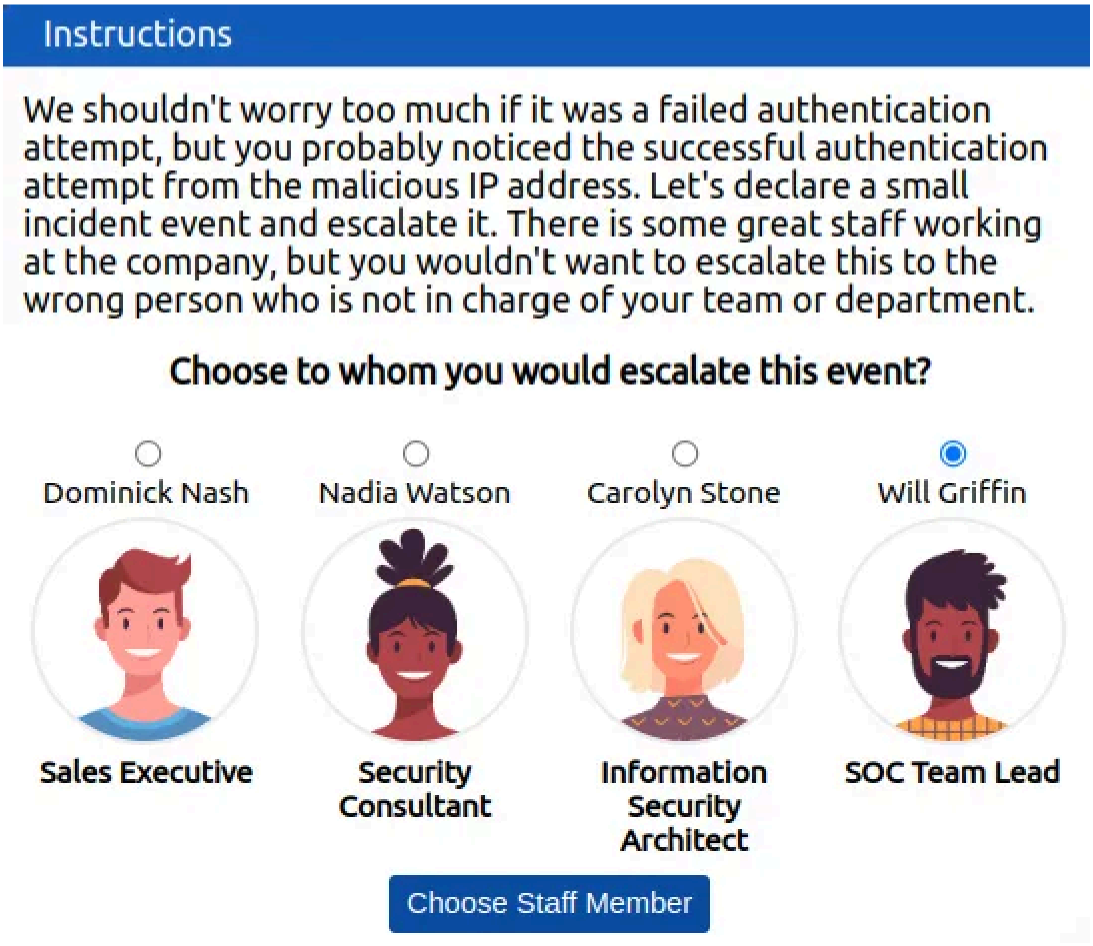
To be in the frontline is not always easy and can be very challenging as you will be working with various log sources from different tools that we will walk you through in this path. You will get a chance to monitor the network traffic, including IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) alerts, suspicious emails, extract the forensics data to analyze and detect the potential attacks, use open-source intelligence to help you make the appropriate decisions on the alerts.

One of the most exciting and rewarding things is when you are finished working on an incident and have managed to remediate the threat. Incident Response might take hours, days, or weeks; it all depends on the scale of the attack: did the attacker manage to exfiltrate the data? How much data does the attacker manage to exfiltrate? Did the attacker attempt to pivot into other hosts? There are many questions to ask and a lot of detection, containment, and remediation to do. We will walk you through some fundamental knowledge that every Junior (Associate) Security Analyst needs to know to become a successful Network Defender.

The first thing almost every Junior (Associate) Security Analyst does on their shift is to look at the tickets to see if any alerts got generated.

Are you ready to immerse yourself into the role of a Junior Security Analyst for a little bit?

Answer the questions below :



Instructions

We shouldn't worry too much if it was a failed authentication attempt, but you probably noticed the successful authentication attempt from the malicious IP address. Let's declare a small incident event and escalate it. There is some great staff working at the company, but you wouldn't want to escalate this to the wrong person who is not in charge of your team or department.

Choose to whom you would escalate this event?

○ Dominick Nash	○ Nadia Watson	○ Carolyn Stone	● Will Griffin
Sales Executive	Security Consultant	Information Security Architect	SOC Team Lead

```
1. Click on the green View Site button in this task to open the Static Site Lab
A. No answer needed

2. What was the malicious IP address in the alerts?
A. 221.181.185.159

3. To whom did you escalate the event associated with the malicious IP address?
A. Will Griffin

4. After blocking the malicious IP address on the firewall, what message did th
A. THM{UNTIL-WE-MEET-AGAIN}
```

Thankyou For Reading.

> *please Follow for more such amazing Content.*

Tryhackme Tryhackme Walkthrough Cybersecurity Security Infosec

Follow

Written by Md Amiruddin

155 Followers · 6 Following

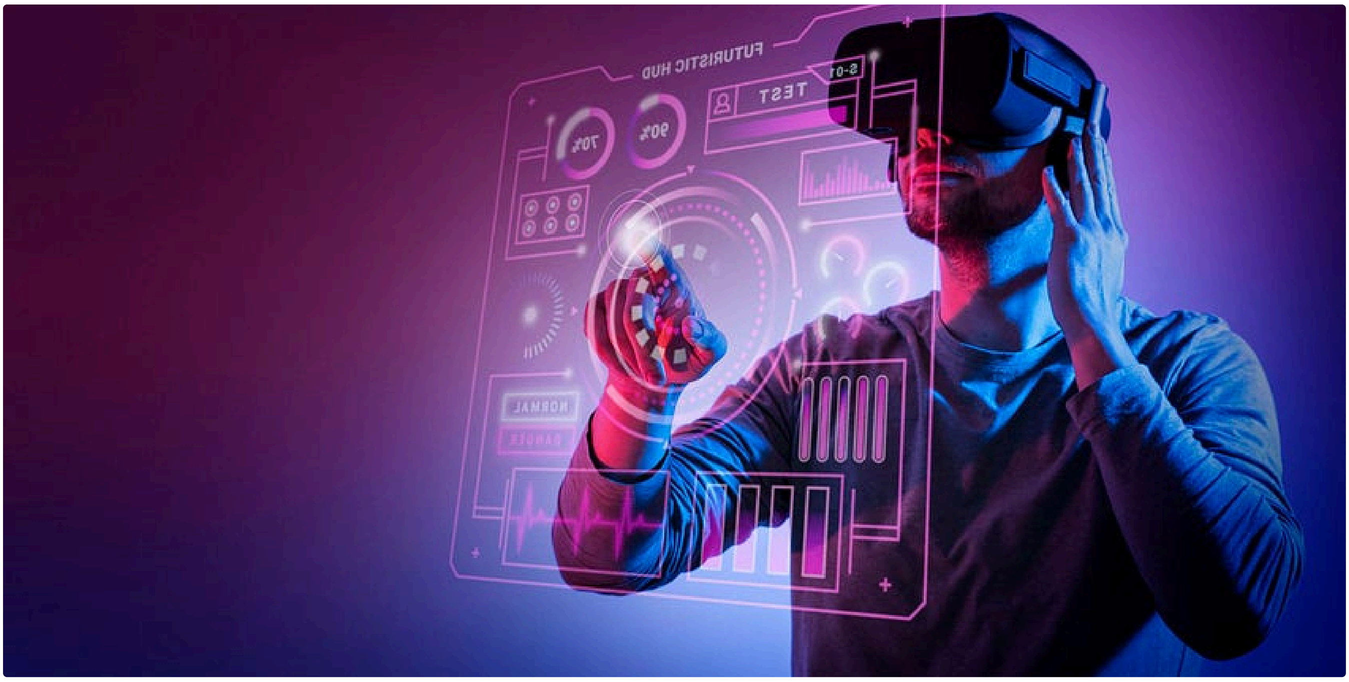
This is a profile of a cybersecurity enthusiast and CTF writer. He is an experi
professional and highly motivated individual.

No responses yet

What are your thoughts?

Respond

More from Md Amiruddin



In InfoSec Write-ups by Md Amiruddin

Vulnhub Writeup/Walkthrough SickOS 1.1 | By Md Amiruddin

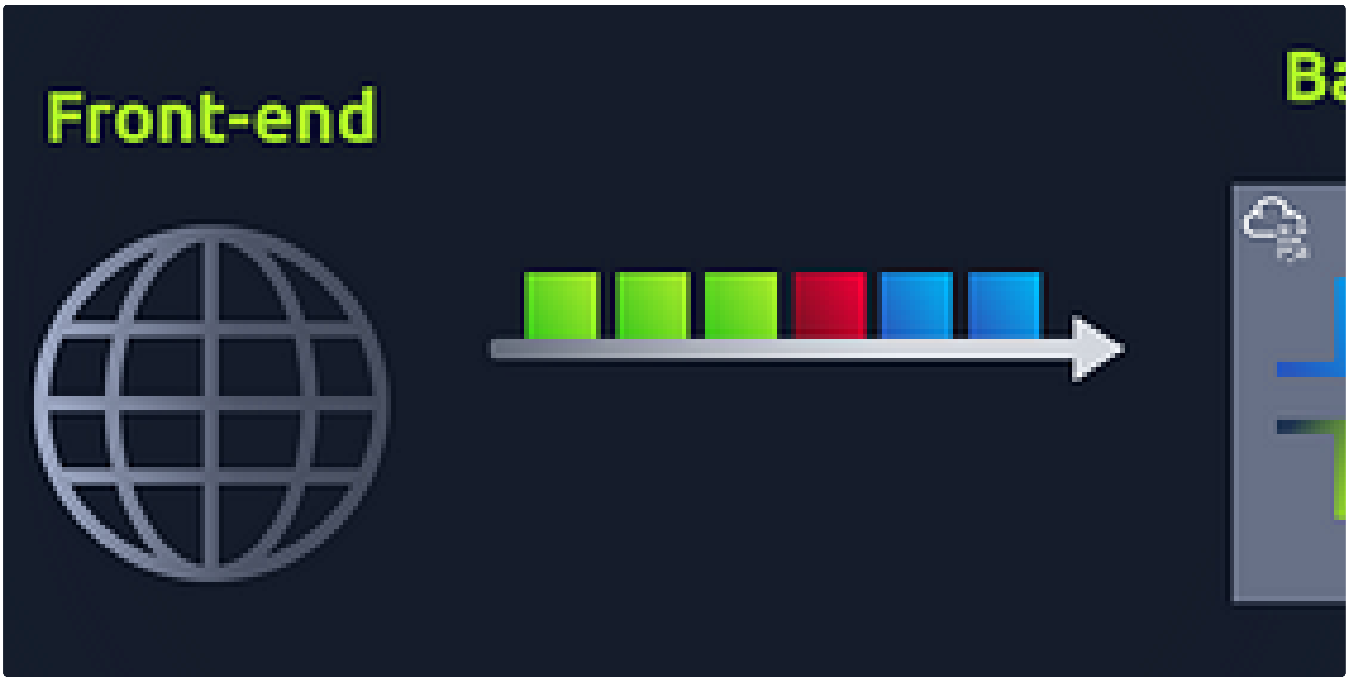
This CTF walkthrough is similar to the labs found in the OSCP exam course.

Dec 21, 2022

Open in app ↗

Medium Search

May 5, 2023 5



In InfoSec Write-ups by Md Amiruddin

HTTP Request Smuggling | Tryhackme Writeup/Walkthrough | By Md Amiruddin

Learn about HTTP Request Smuggling and its different techniques.

Jan 29, 2024 109 2

In InfoSec Write-ups by Md Amiruddin

MITRE | Tryhackme Room Writeup/Walkthrough | By Md Amiruddin

This room will discuss the various resources MITRE has made available for the cybersecurity community.

Mar 20, 2023 👏 2

See all from Md Amiruddin

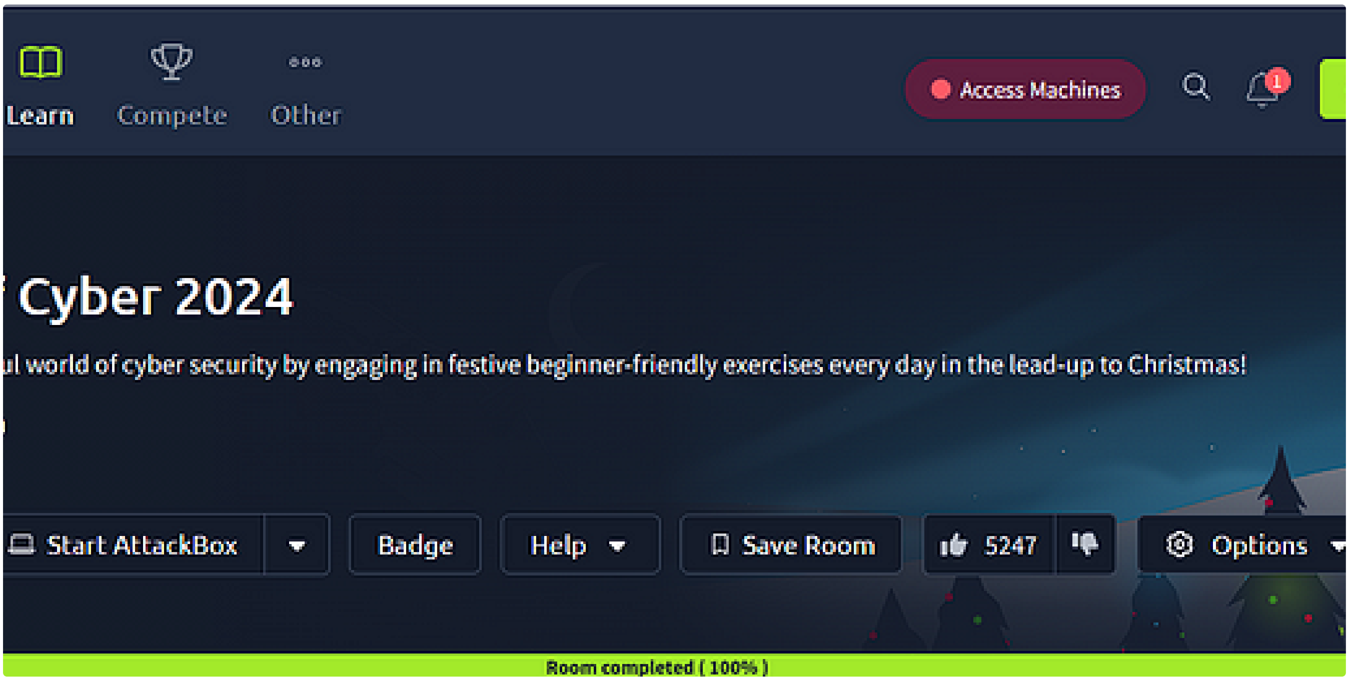
Recommended from Medium

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

✦ Sep 7, 2024 👏 10



Cyber 2024

ul world of cyber security by engaging in festive beginner-friendly exercises every day in the lead-up to Christmas!

In T3CH by TRedEye

Advent of Cyber 2024 {All Tasks Update daily}—Tryhackme walkthrough

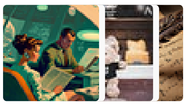
Advent of Cyber 2024 BY ::-> TRedEye

Dec 3, 2024 355 2

Lists

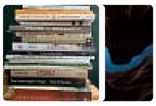
Tech & Tools

22 stories · 377 saves



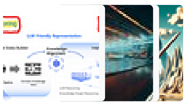
Medium's Huge List of Publications Accepting Submissions

377 stories · 4318 saves



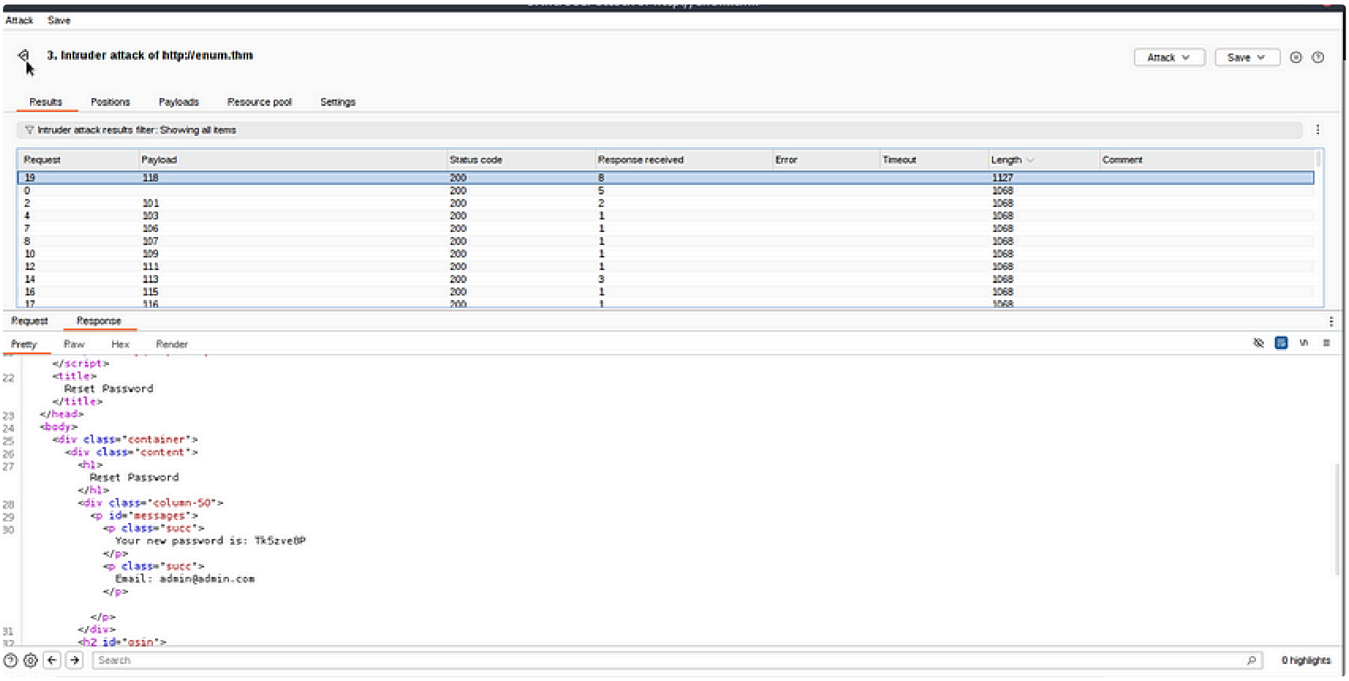
Staff picks

793 stories · 1548 saves



Natural Language Processing

1883 stories · 1521 saves



3. Intruder attack of http://enum.thm

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
19	118	200	8			1127	
0		200	5			1068	
2	101	200	2			1068	
4	103	200	1			1068	
7	106	200	1			1068	
8	107	200	1			1068	
10	109	200	1			1068	
12	111	200	1			1068	
14	113	200	3			1068	
16	115	200	1			1068	
17	116	200	1			1068	

```
    </script>
    <title>
      Reset Password
    </title>
  </head>
  <body>
    <div class="container">
      <div class="content">
        <h1>
          Reset Password
        </h1>
        <div class="column-50">
          <p id="messages">
            <p class="succ">
              Your new password is: Tk5zve8P
            </p>
            <p class="succ">
              Email: admin@admin.com
            </p>

          </p>
        </div>
        <h2 id="osin">
```

embossdotar

TryHackMe — Enumeration & Brute Force — Writeup

Key points: Enumeration | Brute Force | Exploring Authentication Mechanisms | Common Places to Enumerate | Verbose Errors | Password Reset...

Jul 31, 2024 26

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

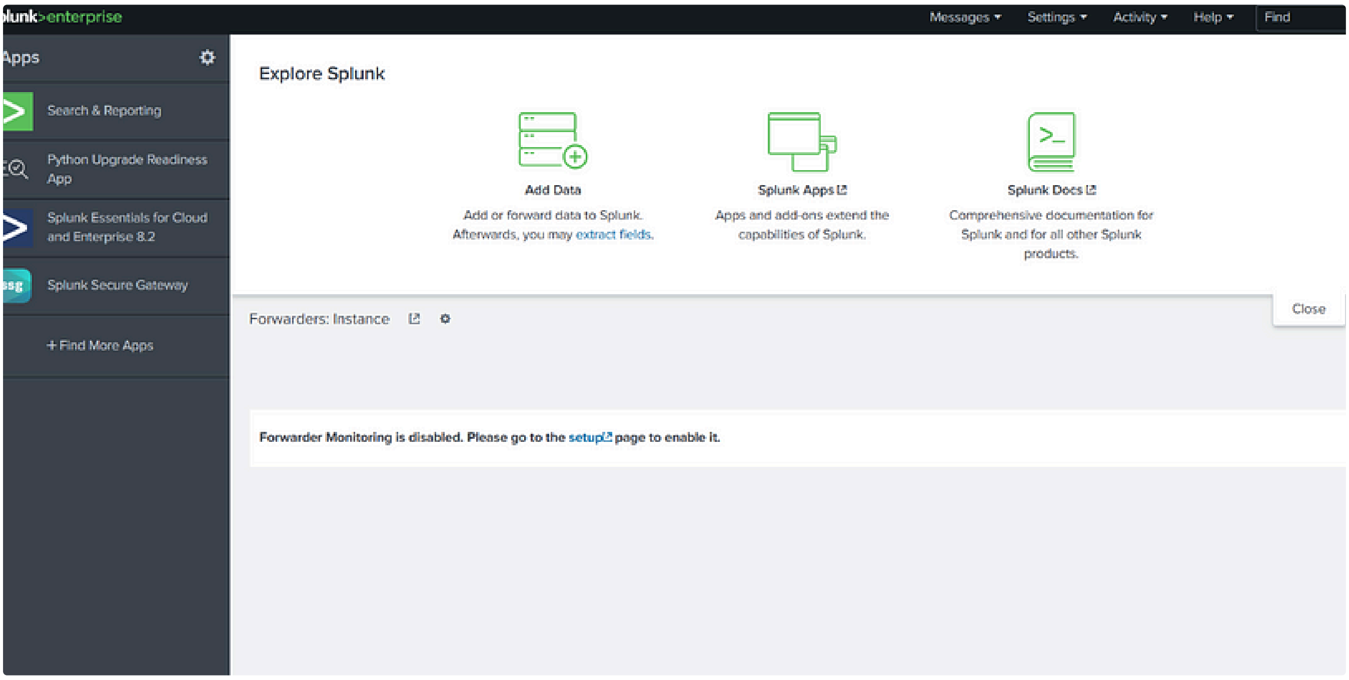
✦ Nov 28, 2024 50

Andrey Pautov

Mastering John the Ripper: A Complete Guide to Password Cracking

Unlock the power of John the Ripper, from basic setups to advanced password recovery strategies

Nov 15, 2024 7 1



Add or forward data to Splunk. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk.

Comprehensive documentation for Splunk and for all other Splunk products.

Forwarder Monitoring is disabled. Please go to the setup page to enable it.

Sudarshan Patel

📊 📈 Tryhackme | Splunk: Dashboards and Reports 🔒 📌

Creating Dashboards and Reports in Splunk.

Jul 27, 2024

See more recommendations