

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



TryHackMe - Red Team OPSEC



Vyshakhari · [Follow](#)

Published in Techiepedia

3 min read · May 11, 2022



Listen



Share



More

Hello Everyone. In this blog let's see how to solve Red Team OPSEC room in TryHackMe.

TryHackMe | Cyber Security Training

TryHackMe is a free online platform for learning cyber security, using hands-on exercises and labs, all through your...

tryhackme.com

Task 1:

Aim to memorize the five steps of the OPSEC process as we explain each one in its own task.

Task 2:

Mark the critical information to get the flag. after you selected the right ones, the page automatically redirects to the flag.

Mark Critical Information

- ☐ Your team uses Firefox exclusively to browse the Internet. Is this critical information?
- ☐ Your team prefers to browse the Internet using Lynx text-based web browser. Is this critical information?
- ☐ Your team uses MS Windows 10 as their primary operating system. Is this critical information?
- ☐ Your team uses offensive Linux distributions hosted on cloud provider X. Would you consider this critical information?
- ☐ Your team has registered the domain name `webmai1.thm` to host phishing sites. Would you consider this critical information?

The critical information are 2,4 and 5. which provides the flag.

[Open in app](#) ↗

Medium

 Search



Task 3:

Try to think of at least one adversary who is not a threat and one who is a threat.

Task 4:

Your red team uses THC-Hydra to find the password for a specific login page. Moreover, they are using the Metasploit framework on the same system as THC-Hydra. Would you consider this an OPSEC vulnerability? (Y/N)

Y

One of the red team members posts a photo of his cat every day. Would this be considered an OPSEC vulnerability? (Y/N)

N

Your red team went for dinner, took a photo, and tagged every team member on a popular social media platform. Would you consider this an OPSEC vulnerability? (Y/N)

Y

Your red team posts on its website a list of clients you regularly conduct red team exercises with. Would you consider this an OPSEC vulnerability? (Y/N)

Y

One of your red team members posted a photo of her morning coffee. Would you consider this an OPSEC vulnerability? (Y/N)

N

Task 5:

Your red team uses THC-Hydra to find the password for a specific login page. Moreover, they are using the Metasploit framework on the same system as THC-Hydra. Knowing that your target uses a properly configured Intrusion Detection System (IDS), would you consider this vulnerability as high risk? (Y/N)

Y

Task 6:

This concludes the fifth element in the OPSEC process. Let's get ready before we apply all five elements to other instances of critical information.

Task 7:

Click on View Site and follow through till you get the flag.

(Please note that some browser extensions, such as NoScript, might prevent the site from loading correctly.)

What is the right order?

- Knowing that their company has assigned a red team will alert the blue team to the incoming attack. The alert happens if the red team is outsourced; however, this won't be new information for the blue team if the red team is part of the company staff. If the blue team anticipates you, it might affect their alert level, which in turn might affect the accuracy of the results.
- This will depend on the company and the blue team.
- We would consider the name of the client as critical information.
- We realise that we prefer to keep this piece of information hidden from the blue team. This way, we can attack while they are going on with their usual routine.
- Client name

4 5 ? ? ?

Submit

- 1 for Critical Information
- 2 for Threats
- 3 for Vulnerabilities
- 4 for Risks
- 5 for Coustermeasures

This one is quite tricky to understand. We must read the sentences and find which element of OPSEC does that refers. After the right order, the page redirects to next set of questions. There are four sets after which you get the flag.

The solution is given below.

- 4 5 2 3 1
- 1 5 4 3 2
- 5 2 4 3 1

- 2 3 1 5 4

After solving, you get the flag for task 7. Make sure to use spaces.

Task 8:

Memorise the five elements of the OPSEC process and learn how to apply them to the different aspects of your cybersecurity work.

Hope this blog helps you. Make sure to follow my socials for more cybersecurity content. See you in next blog 🕒 🙌

- **Instagram:** https://www.instagram.com/vyshak_sec/
- **Twitter:** https://twitter.com/vyshak_sec
- **LinkedIn:** <https://www.linkedin.com/in/vyshak-haridasan/>
- **YouTube:** <https://www.youtube.com/channel/UChyEYoBb60jfsHiIpLVNSBw>

Do Follow [Techiepedia](#) for more Interesting write-ups!

Cybersecurity

Red Team

Red Team Security

Tryhackme Walkthrough

Tryhackme



Follow

Published in Techiepedia

526 Followers · Last published Dec 16, 2024

Where Innovation is Composed



Follow

Written by Vyshakhari

38 Followers · 30 Following

Hacker || CTF Player || Cybersecurity analyst ||

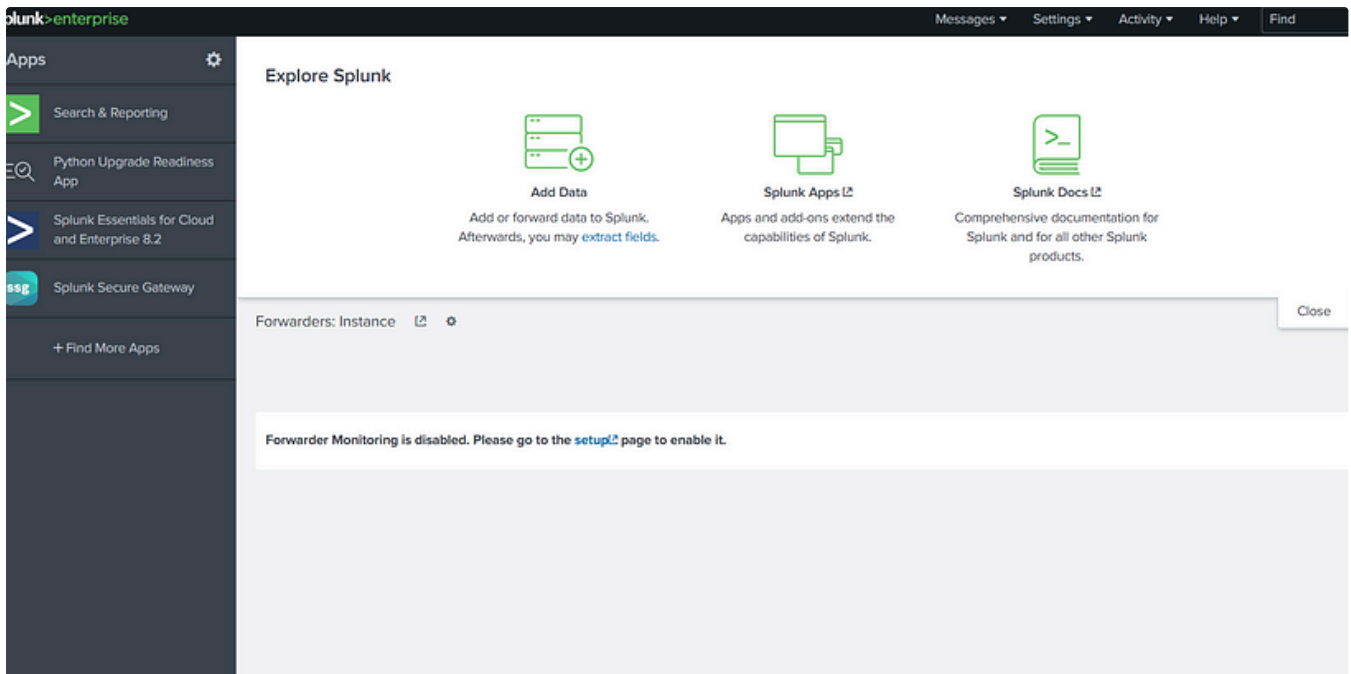
No responses yet




What are your thoughts?

Respond

More from Vyshakhari and Techiepedia



 Vyshakhari

“Splunk: Dashboards and Reports” by TryHackMe

TryHackMe Link: <https://tryhackme.com/room/splunkdashboardsandreports>

Oct 16, 2023  6  1



EC-Council



 In Techiepedia by C M UPPIN

Certified Ethical Hacker Practical Exam Guide

Hola Hackers, Today I'm going to share my experience about the CEH Practical Exam, which i have cleared recently and scored 19/20, in this...

Jun 10, 2022 🖱️ 309 💬 5



Status

Unresolved

This submission has been accepted as a valid issue.
Congratulations!

Reward

 In Techiepedia by Prajit Sindhkar

How to Report DMARC Vulnerabilities Efficiently To Earn Bounties Easily

Hello Guys 🙌🙌 , Prajit here from the BUG XS Team, so in this write-up I will be discussing the most easy P3-P4 vulnerability found on...

Jun 13, 2021 🖱️ 789 💬 10



<code>quit</code>	Exits telnet	<code>telnet> quit</code>
<code>status</code>	Shows the current status of the telnet client	<code>telnet> status</code>
<code>z</code>	Suspends telnet (on Unix/Linux systems)	<code>telnet> z</code>
<code>set</code>	Sets Telnet options (like terminal type)	<code>telnet> set term vt100</code>
<code>unset</code>	Unsets Telnet options	<code>telnet> unset term</code>
<code>display</code>	Displays current settings of Telnet options	<code>telnet> display</code>

 In Techiepedia by Vyshakhari

Telnet Pentesting: A Comprehensive Guide

Telnet, a network protocol used to provide a bidirectional interactive text-based communication system over the Internet, is a staple in...

Dec 16, 2024 🖱 1



See all from Vyshakhari

See all from Techiepedia

Recommended from Medium



Jawstar

Advent of Cyber 2024 { Day 2 } Tryhackme Write-up

(Log analysis)

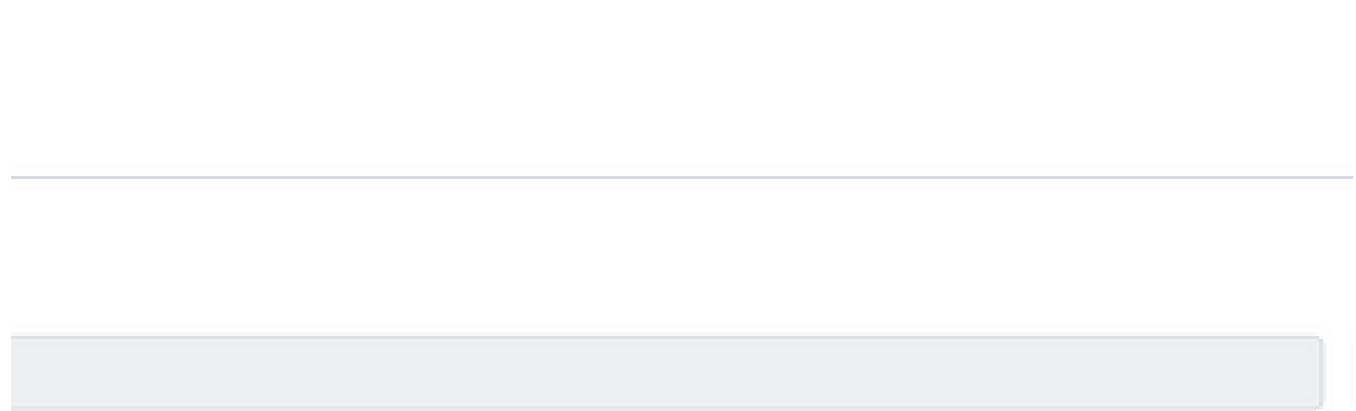



Dec 3, 2024 🖱 9



erative that we understand and can protect against common attacks.

mon techniques used by attackers to target people online. It will also teach some of the best wa



 Daniel Schwarzentraub

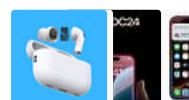
Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

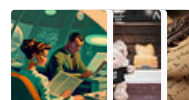


Lists



Tech & Tools

22 stories · 385 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4373 saves



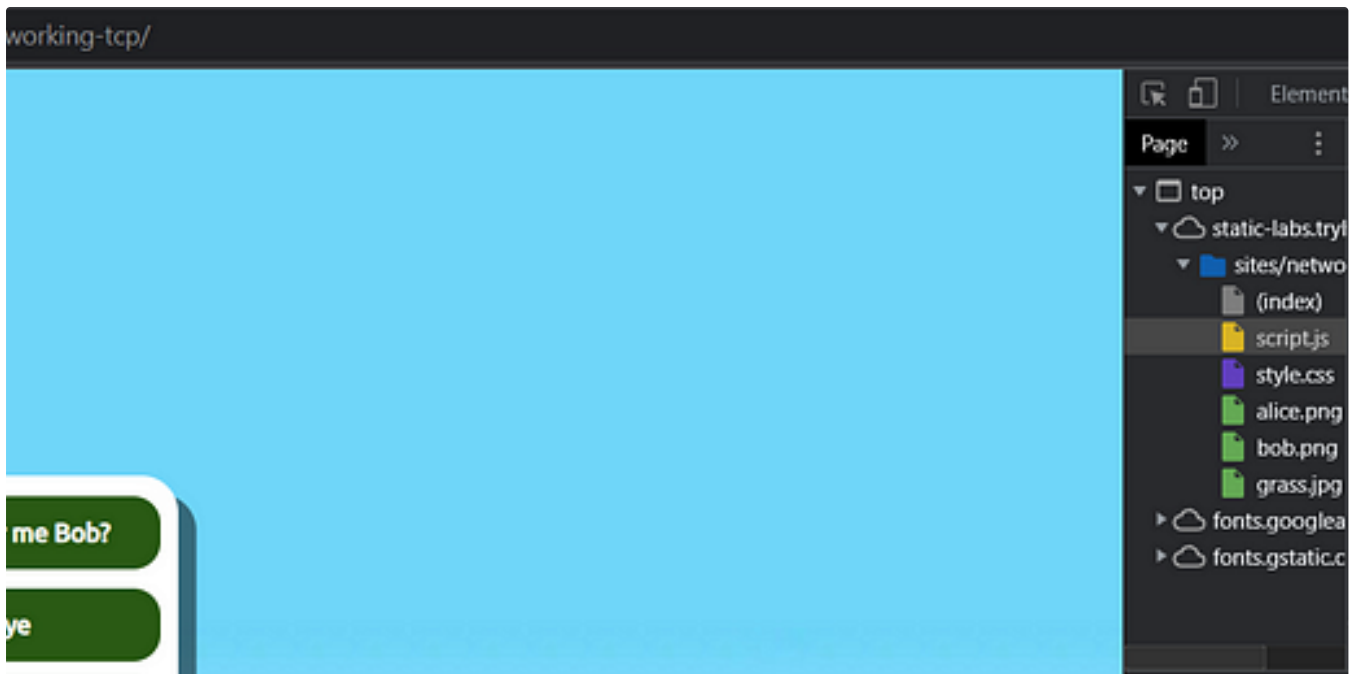
Staff picks

798 stories · 1566 saves



Natural Language Processing

1887 stories · 1536 saves



Trnty

TryHackMe | Active Reconnaissance WriteUp

Learn how to use simple tools such as traceroute, ping, telnet, and a web browser to gather information.

★ Nov 18, 2024



IritT

Windows Event Logs—Cyber Defense-Security Operations & Monitoring—TryHackMe Walkthrough

Introduction to Windows Event Logs and the tools to query them.

Oct 15, 2024



Jawstar

Advent of Cyber '24 Side Quest Answers { T 1 }

T1: Operation Tiny Frostbite



Jan 6



2



Abhijeet Singh

Advent of Cyber 2024 [Day 4] I'm all atomic inside! | TryHackMe Walkthrough

Please go through the story, Cyber Attacks, the Kill Chain and MITRE ATT&CK related content for better understanding of this room.

★ Dec 5, 2024 1



See more recommendations