

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



Valentine Special Challenge | Tryhackme Writeup/Walkthrough | by Md Amiruddin



Md Amiruddin · Follow

 Published in InfoSec Write-ups

4 min read · Feb 13, 2023

 Listen

 Share

 More

This is a writeup/walkthrough of Tryhackme room “Valentine Special Challenge” by Md Amiruddin



Room link : <https://tryhackme.com/jr/valentinespecialchallenge>

Task 1: Tools Required

Setting Up John The Ripper

If you're using Parrot OS, Kali Linux or TryHackMe's own AttackBox- you should already have Jumbo John installed. You can double check this by typing `john` into the terminal. You should be met with a usage guide for john, with the first line reading: "John the Ripper 1.9.0-jumbo-1" or similar with a different version number. If not, you can use `sudo apt install john` to install it.

Cracking a Password Protected Zip File using John The Ripper

We can use John to crack the password on password protected Zip files.

Example Usage

```
zip2john zipfile.zip > ziphash.txt
```

For cracking use this command

```
john --wordlist=/usr/share/wordlists/rockyou.txt ziphash.txt
```

Symmetric encryption

A symmetric encryption algorithm uses the same key for encryption and decryption. Consequently, the communicating parties need to agree on a secret key before being able to exchange any messages.

We can decrypt a file using OpenSSL using the following command:

Note: you have to provide the secret key in order to decrypt it.

```
openssl aes-256-cbc -d -in encrypted_message -out message.txt
```

Install ExifTool

To install the ExifTool component, execute the following command:

```
sudo apt-get update && sudo apt-get install -y libimage-exiftool-perl
```

Task 2 : Challenge

Recently lordofficial has fallen in love with a cybergirl and she has send one love letter to him. In order to accept the valentine date request he needs to crack that love letter so, you are all requested to help him in order to accept her valentine request.

Answer the questions below :

Open in app ↗

Medium



Search



```
[lordofficial@parrot]~
└─$ zip2john love_letter.zip > hash.txt
love_letter.zip/love_letter/ is not encrypted!
ver 78.8 love_letter.zip/love_letter/ is not encrypted, or stored with non-handled compression type
ver 81.9 love_letter.zip/love_letter/valentine.jpg is not encrypted, or stored with non-handled compression type
ver 81.9 love_letter.zip/love_letter/valentine_message is not encrypted, or stored with non-handled compression type
[lordofficial@parrot]~
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
iloveyou      (love_letter.zip/love_letter/valentine.jpg)
1g 0:00:00:00 DONE (2023-02-13 14:18) 2.631g/s 21557p/s 21557c/s 21557C/s 123456..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[lordofficial@parrot]~
└─$
```

Command used

```
[lordofficial@parrot]~
└─$ zip2john love_letter.zip > hash.txt

[lordofficial@parrot]~
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

This is how we got our Answer 1.

2. What city is this person in?

Now we will use exif tool.

command used :

```
[lordofficial@parrot]~
└─$ exiftool valentine.jpg
```

```
Creator: love_letter.zip/love_le: type="Seq" lordofficial@1377
Description: love_letter.zip/love_le: I love hacking.
Creator City: love_letter.zip/love_le: Chennai
Creator Country: love_letter.zip/love_le: India
Creator Postal Code: love_letter.zip/love_le: 600002
Creator Region: love_letter.zip/love_le: Tamil Nadu
Profile CMM Typed hash (ZIP, WinZip): Little CMS SHA1 256/256 AVX2 8x]
Profile Version: love_letter.zip/love_le: 4.3.0
```

This is how we got our Answer 2.

3. What is the Description of valentine.jpg file ?

```
Creator love_letter.zip/love_le: type="Seq" lordofficial@1377 red w
Description ve_letter.zip/love_le: I love hacking.jpg is not encrypted
Creator City letter.zip/love_le: Chennai
Creator Country @parrot[-|-] : India
Creator Postal Code st=/usr/share: 600002 ts/rockyou.txt hash.txt
Creator Region Input encoding: UT: Tamil Nadu
Profile CMM Typed hash (ZIP, Win: Little CMS SHA1 256/256 AVX2 8x])
Profile Version P threads : 4.3.0
```

This is how we got our Answer 3.

4. Decrypt the file valentine_message encrypted (using AES256-CBC) with the key using openssl.

What is the key to decrypt the file?

```
Creator love_letter.zip/love_le: type="Seq" lordofficial@1377 red w
Description ve_letter.zip/love_le: I love hacking.jpg is not encrypted
Creator City letter.zip/love_le: Chennai
Creator Country @parrot[-|-] : India
Creator Postal Code st=/usr/share: 600002 ts/rockyou.txt hash.txt
Creator Region Input encoding: UT: Tamil Nadu
Profile CMM Typed hash (ZIP, Win: Little CMS SHA1 256/256 AVX2 8x])
Profile Version P threads : 4.3.0
```

this looks suspicious so, we will use lordofficial@1377 to decrypt the valentine_message and it works.

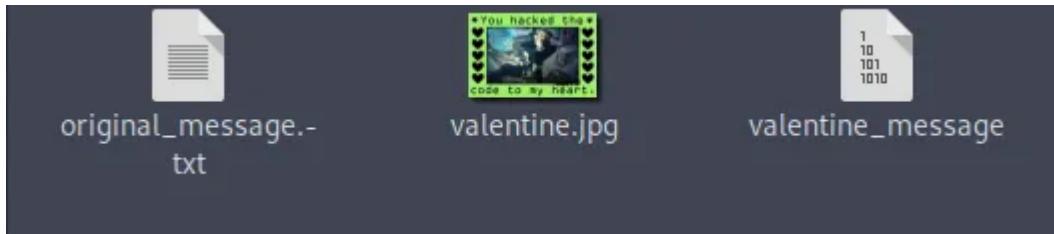
command used :

```
└─[lordofficial@parrot]─[~]
└─$ openssl aes-256-cbc -d -in valentine_message -out original_message.txt
enter aes-256-cbc decryption password:lordofficial@1377
```

This is how we got our Answer 4.

5. what is the hint you got after decrypting the valentine_message ?

Open the original_meassag.txt to read the hint.



This is how we got our Answer 5.

6. Decode the hint. what is the deoded hint ?

command used

```
echo '{decoded-hint}' | base64 --decode
```

This is how we got our Answer 6.

7. What is the Final flag ?

Go to the web browser and type the decoded hint and it will give your final flag.



This is how we got our Answer 7 final flag.

Tryhackme

Tryhackme Walkthrough

Tryhackme Writeup

Valentines Day

[Challenge](#)[Follow](#)

Published in InfoSec Write-ups

49K Followers · Last published 11 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

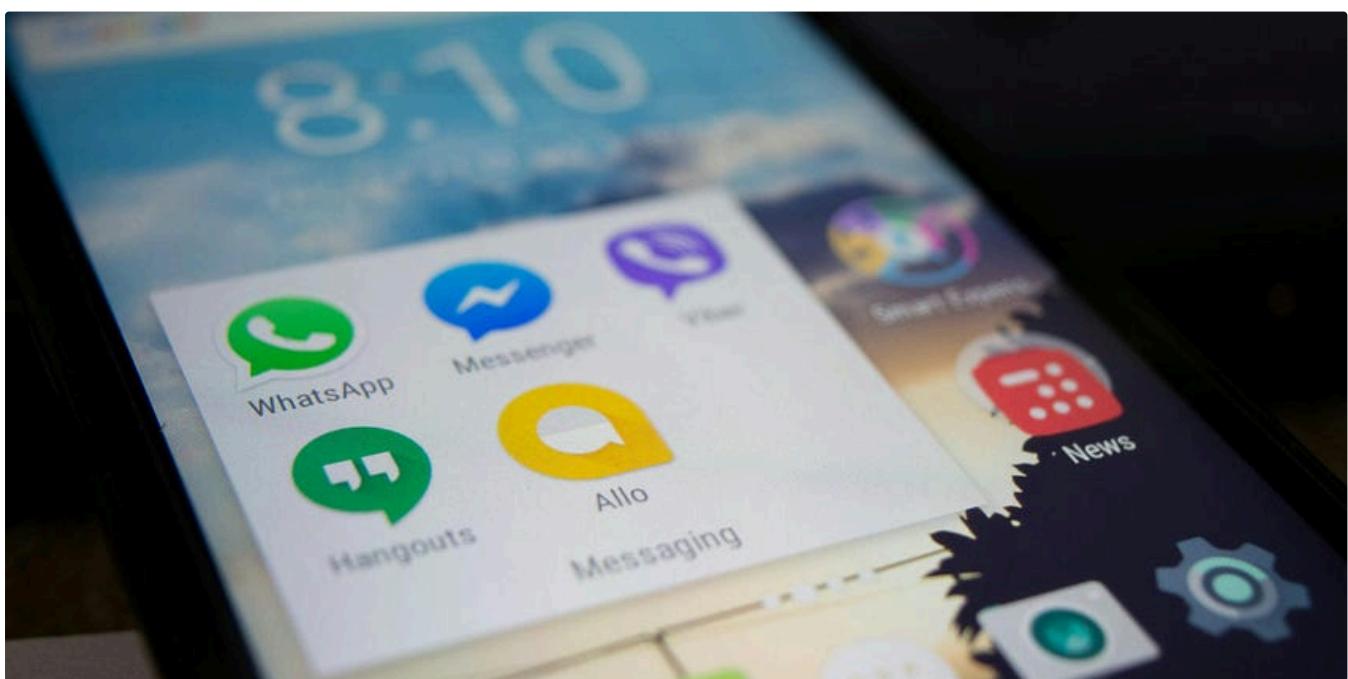
Vulnhub Writeup/Walkthrough SickOS 1.1 | By Md Amiruddin

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

Dec 21, 2022



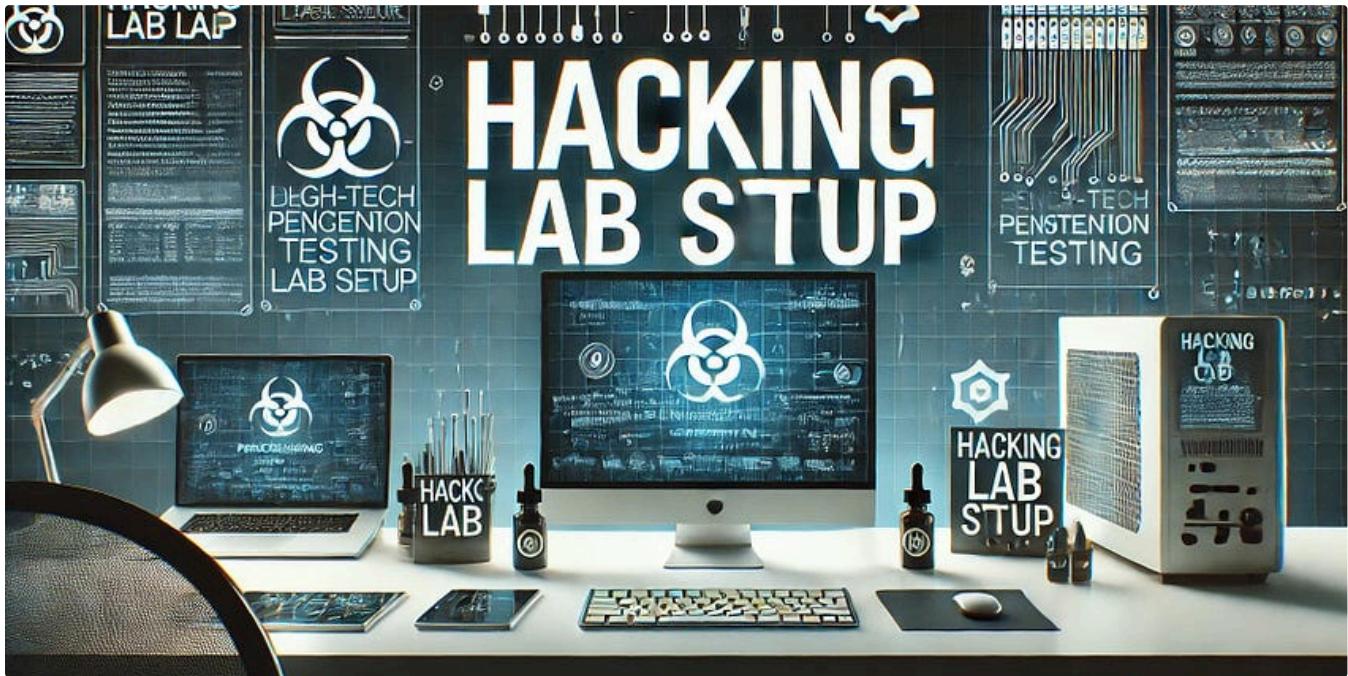
...



 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...

 6d ago  15 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

 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

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

Start AttackBox ▾ Badge Help ▾ Save Room Options

Room completed (100%)

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



Stories To Help You Overcome Writer's Block

8 stories · 663 saves

Attack Save

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

Results Positions Payloads Resource pool Settings

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	

Request Response

Pretty Raw Hex Render

```

22
<script>
<title>
    Reset Password
</title>
23
</head>
24
<body>
25     <div class="container">
26         <div class="content">
27             <h1>
28                 Reset Password
29             </h1>
30             <div class="column-50">
31                 <div id="messages">
32                     <p class="succ">
33                         Your new password is: TkSzveBP
34                     </p>
35                     <p class="succ">
36                         Email: admin@admin.com
37                     </p>
38                 </div>
39             </div>
40             <h2 id="osin">
41
42
43
44
45
46
47
48
49
49
50
51
52
53
54
55
56
57
58
59
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
79
80
81
82
83
84
85
86
87
88
89
89
90
91
92

```

0 highlights

 embossdotar

TryHackMe—Enumeration & Brute Force—Writeup

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

star Jul 31, 2024 hand 26


 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



...

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

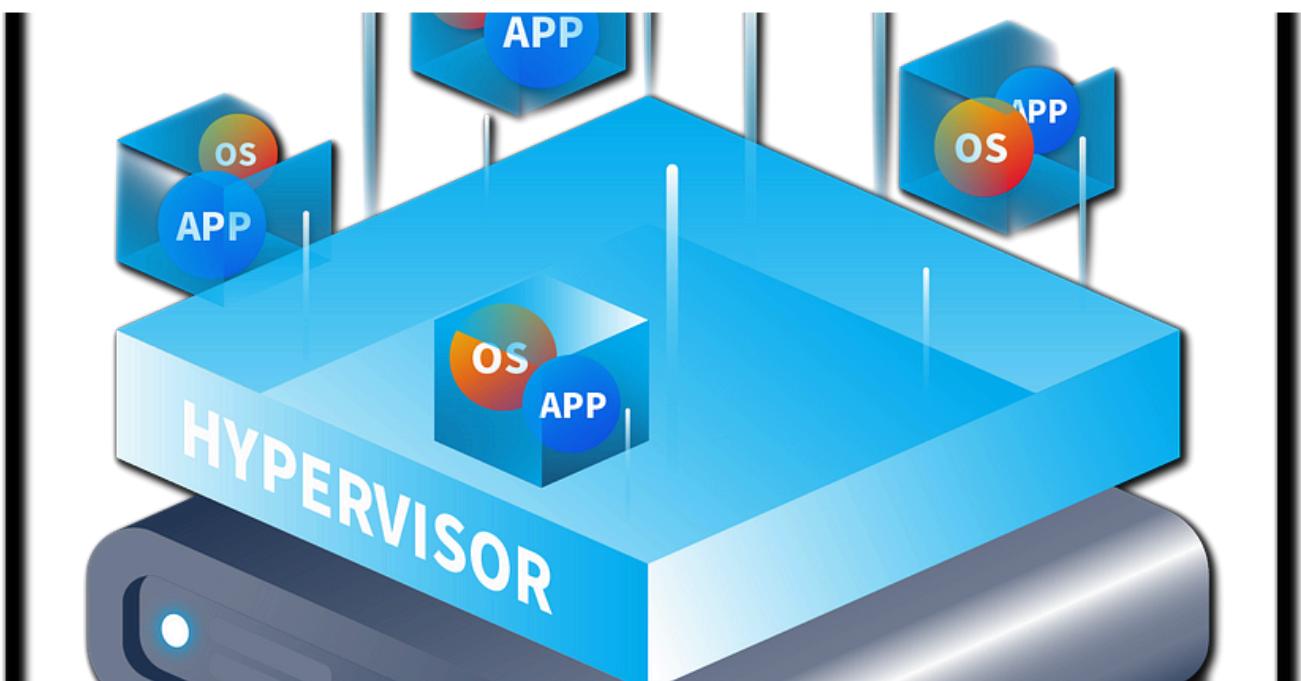
Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024



...



Sunny Singh Verma [SuNnY]

Hypervisor Internals TryHackMe Walkthrough

Brief Intro

Aug 29, 2024

50

1



...

See more recommendations