

KEAMANAN SISTEM DAN JARINGAN KOMPUTER
TryHackMe: Common Attacks



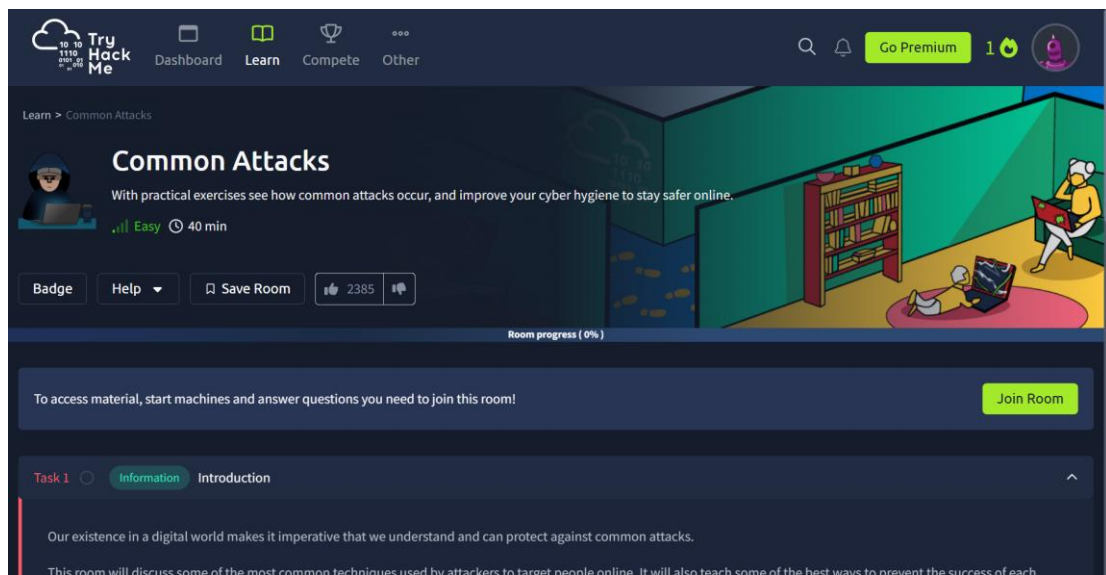
Nama :

Aldi Nur Fahmi

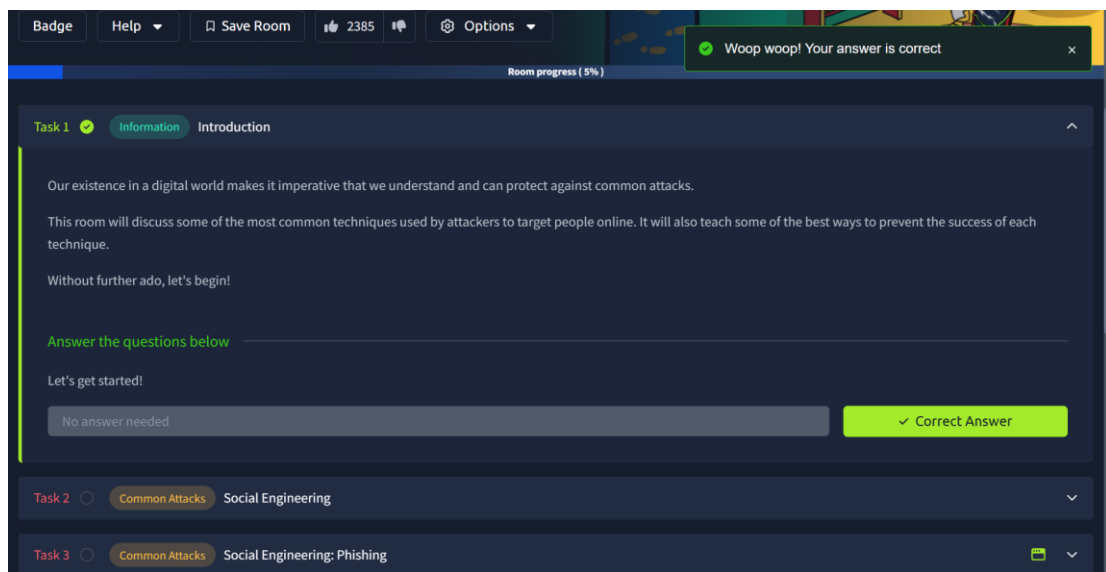
POLITEKNIK NEGERI MALANG KAMPUS
LUMAJANG

*Jl. Lintas Timur, Area Sawah/Kebun, Jogotrunan, Kec. Lumajang,
Kabupaten Lumajang, Jawa Timur 67314*

2025



1. Join room ada common attacks



2. Menyelesaikan task 1

Room progress (17%)

Staying Safe from Social Engineering Attacks

In many ways, it is very tricky to stay safe from social engineering as it won't always be you who the attacker is talking to, but rather someone who can give them what they need without your consent (e.g. calling your bank whilst pretending to be you, so as to access your bank account). That said, there are still measures you can take to protect yourself from Social Engineering attacks:

- Always make sure to set up multiple forms of authentication, and ensure that providers respect these. For example, set difficult to guess — or otherwise incorrect — answers to security questions (making sure to store the answers somewhere safe!), and make sure that these questions are asked when you try to access accounts over the phone.
- Never plug external media (e.g. USBs/CDs/etc) into a computer that you care about or that is connected to any other devices. Ideally, don't plug the media in at all, and instead give it to your local police for safekeeping.
- Always insist on proof of identity when a stranger calls or messages you claiming to work for a company whose services you use. Where possible, confirm with a known phone number or email address that the call or message you received was legitimate (i.e. use a trusted method to get in contact with the company to confirm). Remember that no legitimate employee will ever ask for your password or other information that protects your account.

Answer the questions below

Read the task information and watch the attached videos

No answer needed ✓ Correct Answer

What was the original target of Stuxnet?

The Iran Nuclear Programme ✓ Correct Answer 🔍 Hint

3. Menyelesaikan task 2 dengan menjawab pertanyaan "what was the original target of Stuxnet?"

Room progress (29%)

accidentally fall for one, don't panic. Make sure that you change any affected passwords immediately, and contact IT Services if the attack happens at work.

Answer the questions below

Click the green "View Site" button at the top of this task if you haven't already done so.

No answer needed ✓ Correct Answer

The static site will display a series of emails and text messages. You will be asked to identify which of these messages are genuine and which are phishing attempts. Once you have successfully identified all of the messages you will be presented with a flag to enter, here.

Good luck!

What is the flag?

THM{I_CAUGHT_ALL_THE_PHISH} ✓ Correct Answer

Phishing Test

Challenge Completed

Well done you completed the challenge

THM{I_CAUGHT_ALL_THE_PHISH}

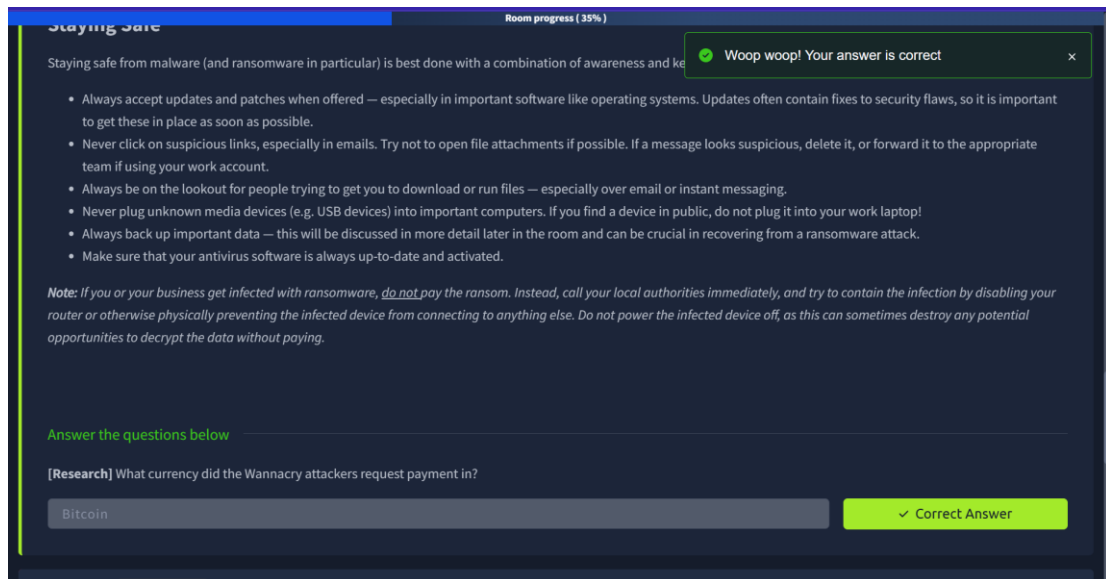
Test <accounts@acmeitsupport.thm> to me

Hello, I've attached the report you asked for, please don't show this to anyone!

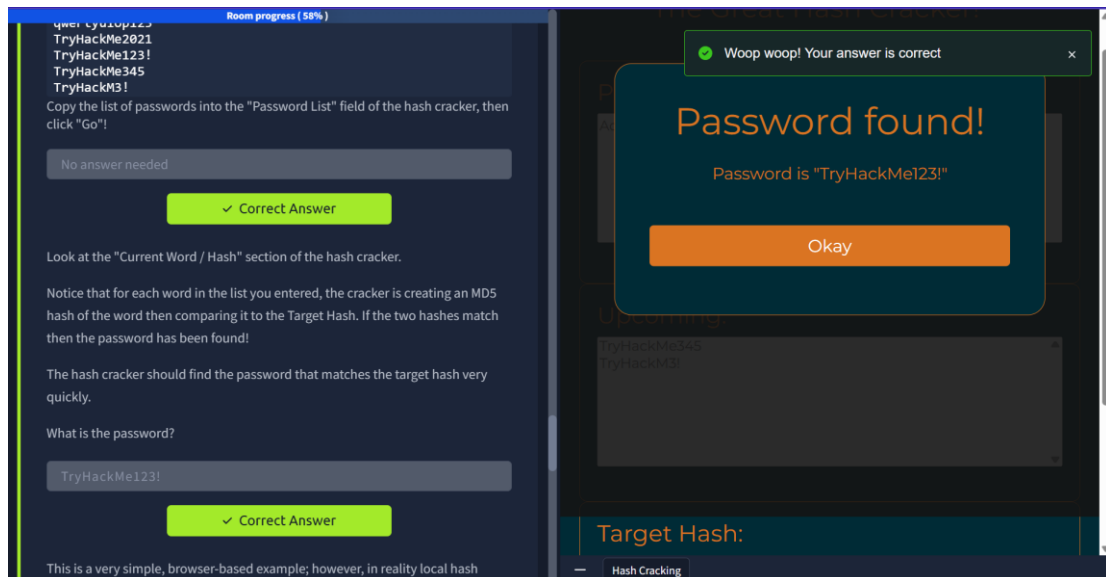
!Don't trust pdf file attachments that are not from a trusted source or unexpected as they could contain malware.

Next

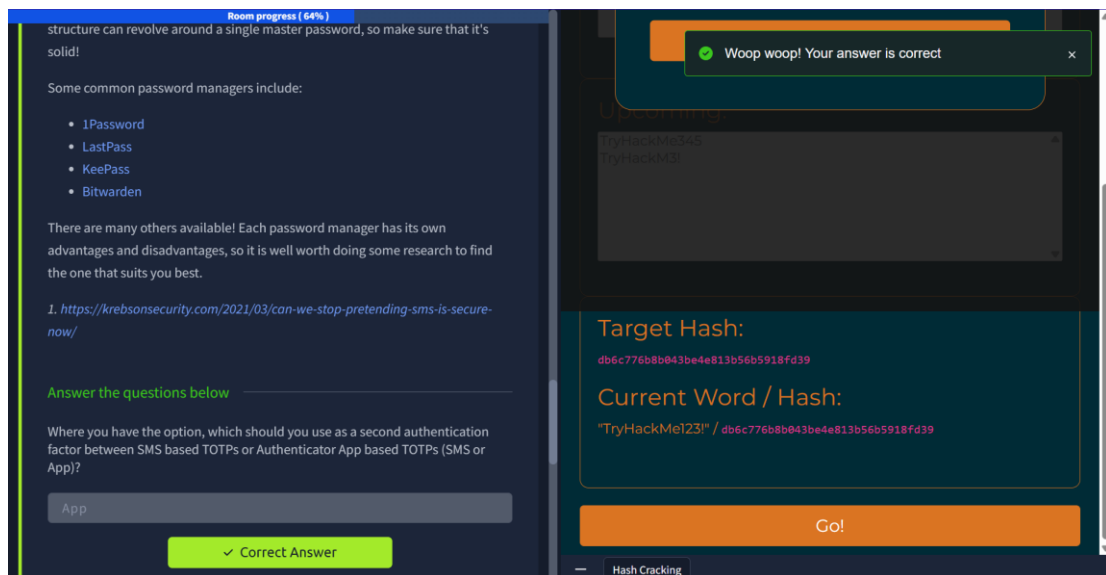
4. Menyelesaikan task 3 dengan menjawab pertanyaan dari menentukan apakah link yang diberikan phishing atau bukan



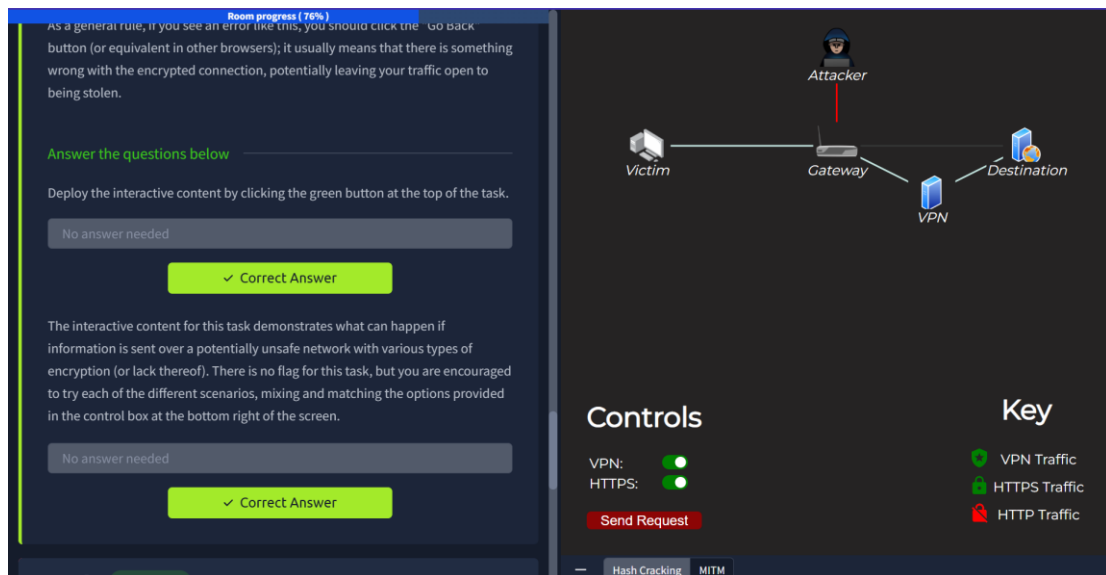
5. Menyelesaikan task 4 dengan menjawab pertanyaan ” [Research] What currency did the Wannacry attackers request payment in?”



6. Menyelesaikan task 5 dengan mencari password yang benar



7. Menyelesaikan task 6 dengan menjawab pertanyaan "Where you have the option, which should you use as a second authentication factor between SMS based TOTP or Authenticator App based TOTP (SMS or App)?"



8. Menyelesaikan task 7 dengan melihat demonstrasi potensi jaringan yang tidak aman

Room progress (88%)

Woop woop! Your answer is correct

One (or more) backups should be stored "off-site". Cloud services such as Google Drive are ideal for personal use in this regard.

Your backups should be safe if all three conditions of the 3,2,1 rule have been met; *but* of equal importance is the *frequency* at which you take backups. There's no point in keeping your backups stored securely if they are all a year old!

How frequently you backup your data is up to you and usually depends on the sensitivity of the data, compared to the risk of compromise and the amount of backup space available. For example, a multi-billion pound corporation handling sensitive data is at high risk of a ransomware attack and may wish to take full backups two or three times a day. By comparison, a home user may only feel the need to take backups once or twice a week.

Answer the questions below

What is the minimum number of up-to-date backups you should make?

3

✓ Correct Answer

Of these, how many (at minimum) should be stored in another location?

1

✓ Correct Answer

Task 9 Updates and Patches

9. Menyelesaikan task 8 dengan menjawab 2 pertanyaan

Room progress (94%)

Case Study: Eternal Blue. (Click to read)

Unfortunately, all software eventually loses support from its maintainers, becoming deprecated and no longer receiving updates (e.g. Windows 7) — this is referred to as the software being **EOL (End Of Life)**. At this point, the software *must* be replaced as soon as possible. If replacing the software is not possible then the device should be segregated as far as is possible to prevent exploitation of the vulnerabilities that will inevitably be found and left unpatched.

Antivirus Updates

Most antivirus software packages receive very frequent updates; this is because they largely work using a local database of known exploit signatures, which must be kept up-to-date.

In other words: when new malware is discovered, it gets sent around antivirus vendors who generate a "signature" that identifies this particular piece of malicious software. These signatures are then distributed to every device on the planet that uses the antivirus software, ensuring that your installed antivirus solution is kept up-to-date on all the latest (known) malware.

If antivirus software is *not* allowed to update it will still be able to catch *some* malware through other methods. However, the local signature database will quickly become outdated, resulting in malicious software potentially falling through the gaps. In short: if the antivirus wants to update, let it!

Answer the questions below

(Optional) Complete the [Blue](#) room on TryHackMe to see the brutal effects of the Eternal Blue exploit in action against an unpatched machine for yourself!

No answer needed

✓ Correct Answer

10. Menyelesaikan task 9



11. Semua task pada Common Attacks sudah terselesaikan