

**LAPORAN TUGAS**  
**PEMBELAJARAN TRYHACKME**  
**“Common Attacks”**



Olgeh :

Fannisa Az Zahra (2231740037)

Dosen Pengajar :

Vipkas Al Hadid Firdaus, S.T, M.T.

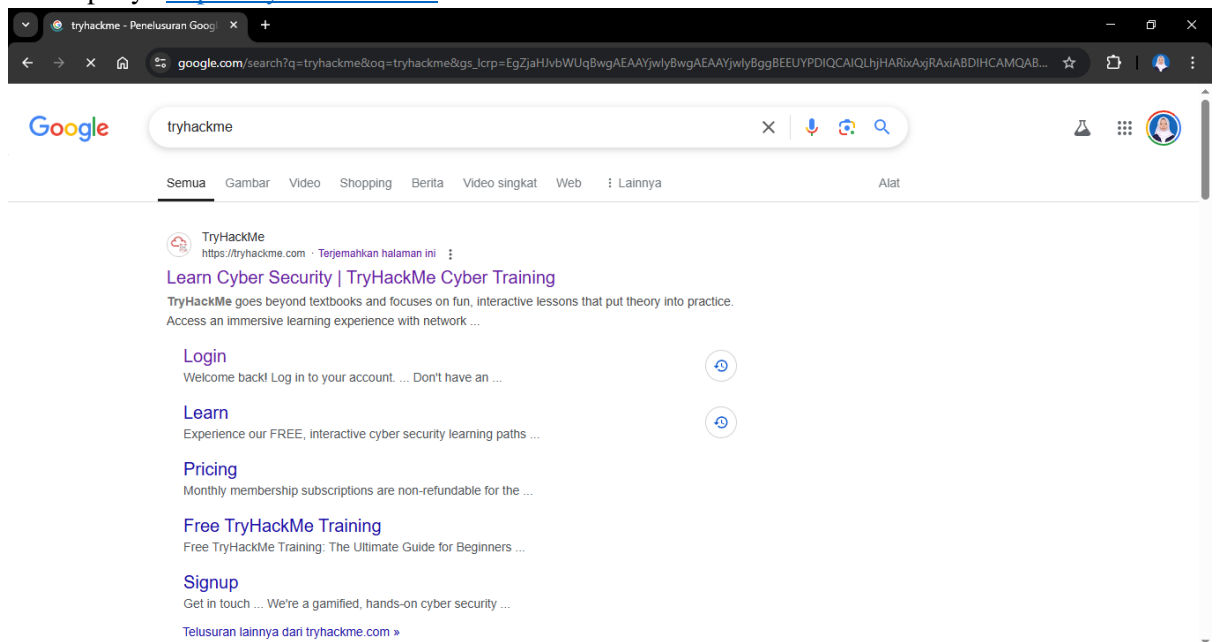
**POLITEKNIK NEGERI MALANG PSDKU LUMAJANG**

Jl. Lintas Timur, Area Sawah/Kebun, Jogoturunan, Kec. Lumajang, Kab. Lumajang

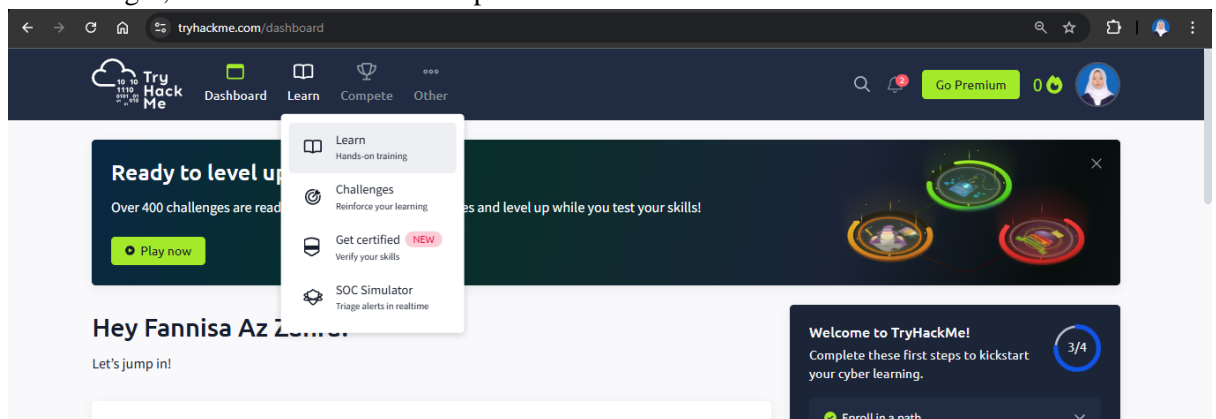
Jawa Timur 67314

**2025**

1. Buka laman chrome, lalu ketikkan tryhackme kemudian Login dengan akun yang sudah kalian punya <https://tryhackme.com/>



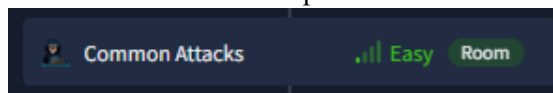
2. Setelah login, masuk ke dashboard dan pilih learn.



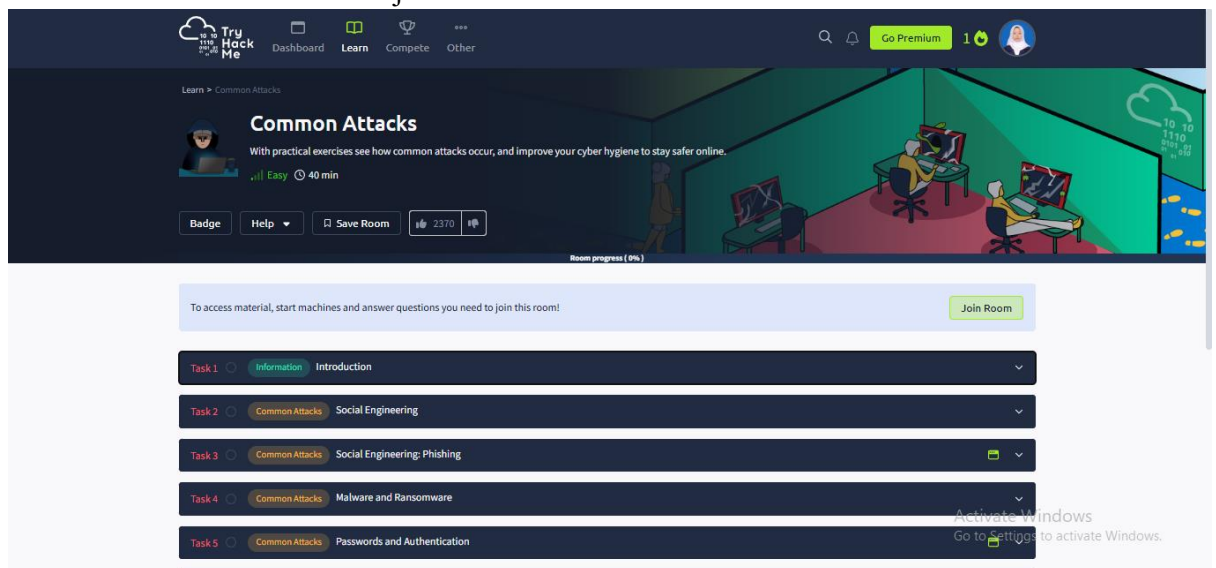
3. Setelah itu scroll kebawah dan pilih Free Roadmap



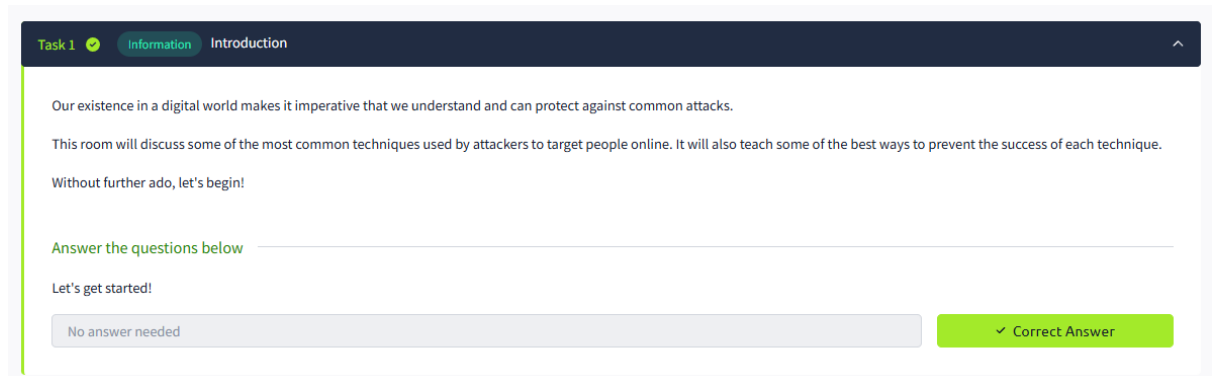
4. Lalu scroll kebawah dan pilih “room Common Attacks”



5. Setelah masuk room klik untuk “join room”



6. Task 1.



## 7. Task 2.

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

✓ Correct Answer

What was the original target of Stuxnet?

✓ Correct Answer

Hint

Activate Windows

## 8. Task 3.

Room progress ( 29% )

- Avoid making your personal information (e.g. email address and phone number) public if possible. If you *must* publish personal details publicly, create a "burner" email address (a temporary address made for one purpose, then destroyed soon afterwards) for the occasion, then destroy it as soon as it is no longer required.

It's worth noting at this point that anyone can fall for a phishing attack — especially a complex one that has been made to look very realistic. If you 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.

✓ 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?

✓ Correct Answer

Phishing Test

Woop woop! Your answer is correct

Woop woop! Your answer is correct

Well done you completed the challenge

THM[I\_CAUGHT\_ALL\_THE\_PHISH]

Test -accounts@acmeltsupport.thm>  
to me >

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

PDF

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

Next

Activate Windows

## 9. Task 4.

Room progress ( 35% )

### Staying Safe

Staying safe from malware (and ransomware in particular) is best done with a combination of awareness and keeping things up to date!

- Always accept updates and patches when offered — especially in important software like operating systems. Updates often contain fixes to security flaws, so it is important to get these in place as soon as possible.
- Never click on suspicious links, especially in emails. Try not to open file attachments if possible. If a message looks suspicious, delete it, or forward it to the appropriate team if using your work account.
- Always be on the lookout for people trying to get you to download or run files — especially over email or instant messaging.
- Never plug unknown media devices (e.g. USB devices) into important computers. If you find a device in public, do not plug it into your work laptop!
- Always back up important data — this will be discussed in more detail later in the room and can be crucial in recovering from a ransomware attack.
- Make sure that your antivirus software is always up-to-date and activated.

**Note:** If you or your business get infected with ransomware, do not pay the ransom. Instead, call your local authorities immediately, and try to contain the infection by disabling your router or otherwise physically preventing the infected device from connecting to anything else. Do not power the infected device off, as this can sometimes destroy any potential opportunities to decrypt the data without paying.

Answer the questions below

[Research] What currency did the Wannacry attackers request payment in?

✓ Correct Answer

Activate Windows

10. Task 5.

Room progress (41%)

Local attacks require a stolen copy of the credentials in question. The attacker will take a file full of stolen usernames/emails and hash guess the input that created the hash either using randomly generated sequences of characters (slower but more thorough) or by using a wordlist (faster but much more likely to miss things). Hybrid types are also very widely used; these are when an attacker takes an existing wordlist and mutates it to add new characters, symbols or random elements. Local password attacks will be demonstrated in the interactive element for this task.

Remote attacks tend to be one of two categories; they either involve attempting to brute-force known usernames by sending requests to the server and seeing what it responds with, or they use known username and password pairs from previous breaches to see if they are valid on the target site — this is the aforementioned credential stuffing.

Answer the questions below

Put yourself in the shoes of a malicious hacker. You have managed to dump the password database for an online service, but you still have to crack those hashes!

Click the green button at the start of the task to deploy the interactive hash brute-forcer!

No answer needed

✓ Correct Answer

Based on the content of the website, you have generated a list of likely passwords, which is as follows:

```
TryH@ckMe
TryHackMe123
tH@123456
qwertyuiop123
TryHackMe2021
TryHackMe123!
TryHackMe345
TryHackM3!
```

Copy the list of passwords into the "Password List" field of the hash cracker, then click "Go"!

No answer needed

✓ Correct Answer

Room progress (52%)

Click the green button at the start of the task to deploy the interactive hash brute-forcer!

No answer needed

✓ Correct Answer

Based on the content of the website, you have generated a list of likely passwords, which is as follows:

```
TryH@ckMe
TryHackMe123
tH@123456
qwertyuiop123
TryHackMe2021
TryHackMe123!
TryHackMe345
TryHackM3!
```

Copy the list of passwords into the "Password List" field of the hash cracker, then click "Go"!

No answer needed

✓ Correct Answer

Look at the "Current Word / Hash" section of the hash cracker.

Notice that for each word in the list you entered, the cracker is creating an MD5 hash of the word then comparing it to the Target Hash. If the two hashes match then the password has been found!

The hash cracker should find the password that matches the target hash very quickly.

What is the password?

TryHackMe123!

✓ Correct Answer

Room progress (52%)

Look at the "Current Word / Hash" section of the hash cracker.

Notice that for each word in the list you entered, the cracker is creating an MD5 hash of the word then comparing it to the Target Hash. If the two hashes match then the password has been found!

The hash cracker should find the password that matches the target hash very quickly.

What is the password?

TryHackMe123!

✓ Correct Answer

This is a very simple, browser-based example; however, in reality local hash cracking with a wordlist isn't any more complex from a high-level perspective — it's the same technique, but with a lot more potential passwords!

Hopefully this example illustrates why it is so important to choose a strong password — even if the passwords are hashed appropriately.

In the next task we will look at some of the common account protection measures, as well as how to generate secure passwords.

No answer needed

✓ Correct Answer

Room progress (41%)

Local attacks require a stolen copy of the credentials in question. The attacker will take a file full of stolen usernames/emails and hash guess the input that created the hash either using randomly generated sequences of characters (slower but more thorough) or by using a wordlist (faster but much more likely to miss things). Hybrid types are also very widely used; these are when an attacker takes an existing wordlist and mutates it to add new characters, symbols or random elements. Local password attacks will be demonstrated in the interactive element for this task.

Remote attacks tend to be one of two categories; they either involve attempting to brute-force known usernames by sending requests to the server and seeing what it responds with, or they use known username and password pairs from previous breaches to see if they are valid on the target site — this is the aforementioned credential stuffing.

Answer the questions below

Put yourself in the shoes of a malicious hacker. You have managed to dump the password database for an online service, but you still have to crack those hashes!

Click the green button at the start of the task to deploy the interactive hash brute-forcer!

No answer needed

✓ Correct Answer

Based on the content of the website, you have generated a list of likely passwords, which is as follows:

```
TryH@ckMe
TryHackMe123
tH@123456
qwertyuiop123
TryHackMe2021
TryHackMe123!
TryHackMe345
TryHackM3!
```

Copy the list of passwords into the "Password List" field of the hash cracker, then click "Go"!

No answer needed

✓ Correct Answer

Room progress (52%)

Click the green button at the start of the task to deploy the interactive hash brute-forcer!

No answer needed

✓ Correct Answer

Based on the content of the website, you have generated a list of likely passwords, which is as follows:

```
TryH@ckMe
TryHackMe123
tH@123456
qwertyuiop123
TryHackMe2021
TryHackMe123!
TryHackMe345
TryHackM3!
```

Copy the list of passwords into the "Password List" field of the hash cracker, then click "Go"!

No answer needed

✓ Correct Answer

Look at the "Current Word / Hash" section of the hash cracker.

Notice that for each word in the list you entered, the cracker is creating an MD5 hash of the word then comparing it to the Target Hash. If the two hashes match then the password has been found!

The hash cracker should find the password that matches the target hash very quickly.

What is the password?

TryHackMe123!

✓ Correct Answer

Room progress (52%)

Look at the "Current Word / Hash" section of the hash cracker.

Notice that for each word in the list you entered, the cracker is creating an MD5 hash of the word then comparing it to the Target Hash. If the two hashes match then the password has been found!

The hash cracker should find the password that matches the target hash very quickly.

What is the password?

TryHackMe123!

✓ Correct Answer

This is a very simple, browser-based example; however, in reality local hash cracking with a wordlist isn't any more complex from a high-level perspective — it's the same technique, but with a lot more potential passwords!

Hopefully this example illustrates why it is so important to choose a strong password — even if the passwords are hashed appropriately.

In the next task we will look at some of the common account protection measures, as well as how to generate secure passwords.

No answer needed

✓ Correct Answer

## 11. Task 6.

Room progress ( 64% )

— or (more commonly in recent years) biometric data such as a fingerprint. Some password managers are free, whilst others require a subscription. Paid offerings often make them well worth the expense!

Woop woop! Your answer is correct

The more fully-featured password managers usually also include a range of additional capabilities, such as storing other types of data (e.g. images, files, etc.), auto-filling passwords automatically for other services, and secure password generation. Having these features available means that you can quickly and easily generate very strong passwords and store them automatically, then seamlessly have the password entered for you when you attempt to log into an app, all within the same application.

Password managers are the recommended way to handle authentication for your many accounts; however, it is worth remembering that the security of the whole structure can revolve around a single master password, so make sure that it's solid!

Some common password managers include:

- 1Password
- LastPass
- KeePass
- Bitwarden

There are many others available! Each password manager has its own advantages and disadvantages, so it is well worth doing some research to find the one that suits you best.

1. <https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/>

Answer the questions below

Where you have the option, which should you use as a second authentication factor between SMS based TOTP's or Authenticator App based TOTP's (SMS or App)?

App

Woop woop! Your answer is correct

## 12. Task 7.

Room progress ( 70% )

Did Not Connect: Potential Security Issue

Firefox detected a potential security threat and did not continue to www.google.com because this web site requires a secure connection.

What can you do about it?

www.google.com has a security policy called HTTP Strict Transport Security (HSTS), which means that Firefox can only connect to it securely. You can't add an exception to visit this site.

The issue is most likely with the web site, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the web site's administrator about the problem.

Learn more...

Go Back Advanced...

Certificate Error Message in Firefox

As a general rule, if you see an error like this, you should click the "Go Back" button (or equivalent in other browsers); it usually means that there is something wrong with the encrypted connection, potentially leaving your traffic open to being stolen.

Woop woop! Your answer is correct

Woop woop! Your answer is correct

Answer the questions below

Deploy the interactive content by clicking the green button at the top of the task.

No answer needed

Woop woop! Your answer is correct

The interactive content for this task demonstrates what can happen if information is sent over a potentially unsafe network with various types of encryption (or lack thereof). There is no flag for this task, but you are encouraged to try each of the different scenarios, mixing and matching the options provided in the control box at the bottom right of the screen.

No answer needed

Woop woop! Your answer is correct

## 13. Task 8.

Room progress ( 88% )

Backups should be stored on at least **two** different storage mediums; for example: a cloud backup and a USB device. This can include a hard drive on your PC.

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

Woop woop! Your answer is correct

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

1

Woop woop! Your answer is correct

#### 14. Task 9.

Room progress ( 68% )

For this reason, it is imperative that you update software whenever possible — especially for things like operating systems (e.g. Windows or macOS) where vulnerabilities can be particularly dangerous, as seen in the case study below.

▶ [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

#### 15. Task 10.

Room completed ( 100% )

Task 10 ✓ Information Conclusion

To conclude: there are many different options for a malicious attacker to target both individuals and sweeping groups; however, there are remediations for every attack.

Having completed this room, you should hopefully understand a little more about these common attacks and the defences against them. You don't need to be an expert in computers or cybersecurity to stay safe online: the solutions are simple and well-worth adopting in your personal and professional online interactions.

**Answer the questions below**


I have completed the Common Attacks room!

No answer needed

✓ Correct Answer

#### 16. Maka selesai sudah room “Common Attacks”

✓ Woop woopl Your answer is correct



## Congratulations on completing Common Attacks!!! 🎉

Points earned 🔥 56	Completed tasks ✅ 10	Room type 👤 Walkthrough	Difficulty 📶 Easy	Streak 🔥 1
-----------------------	-------------------------	----------------------------	----------------------	---------------

🗉 Leave Feedback

Next

Activate Windows