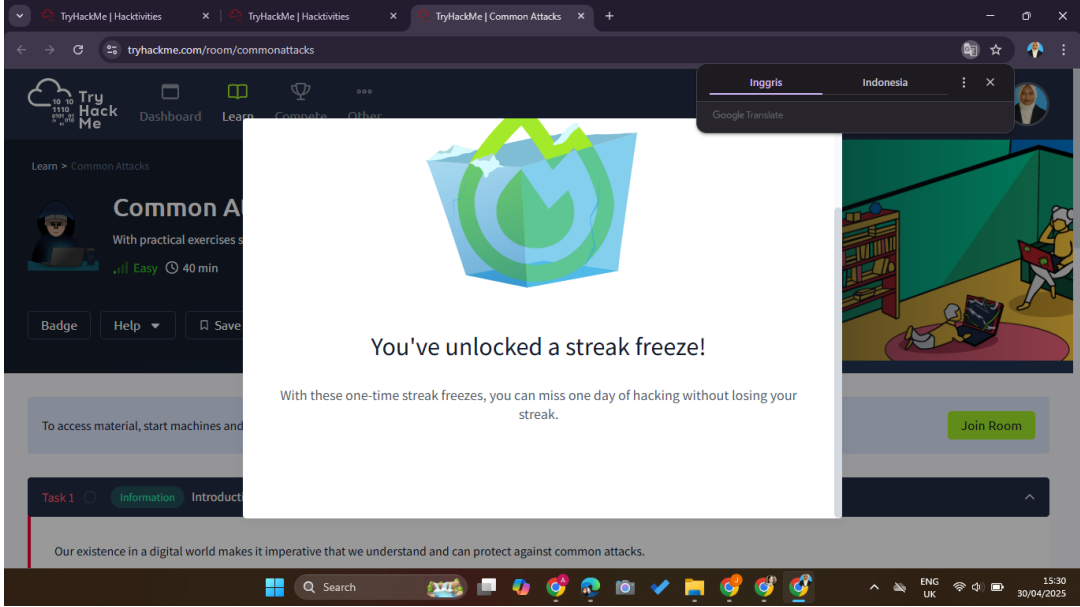
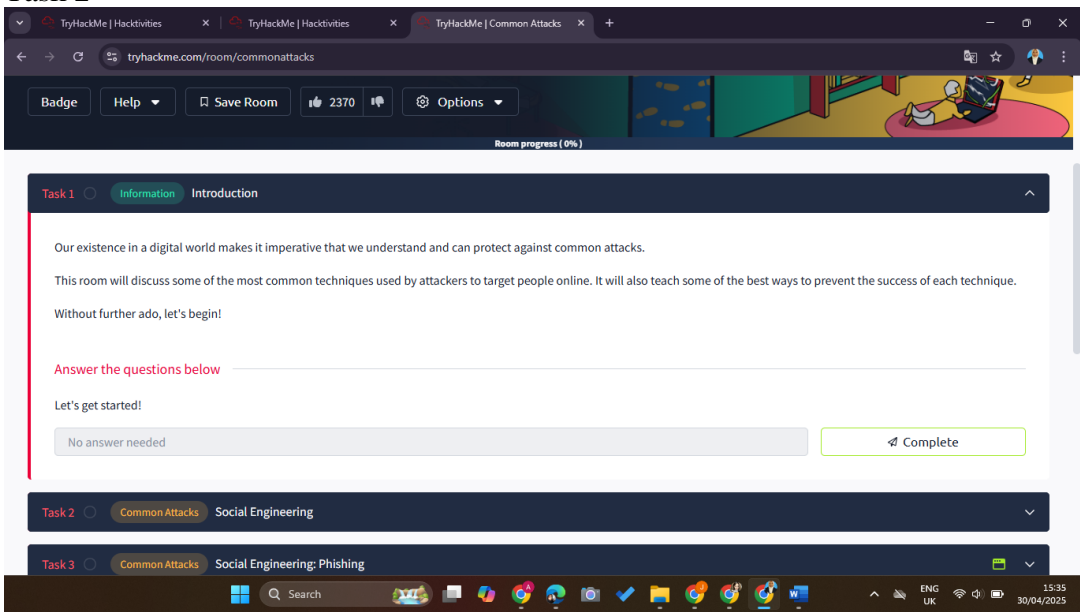
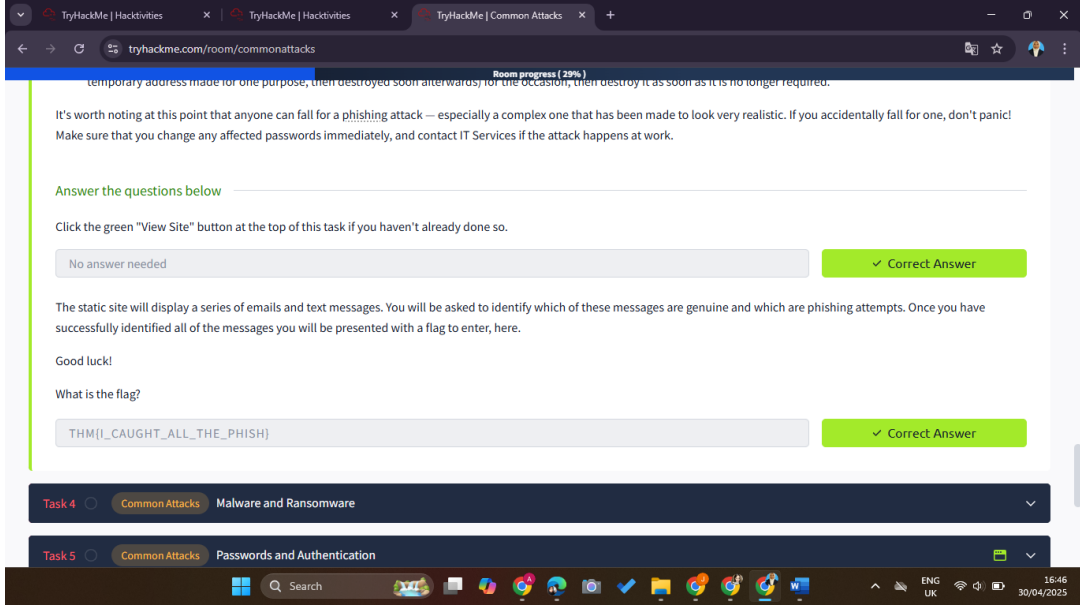
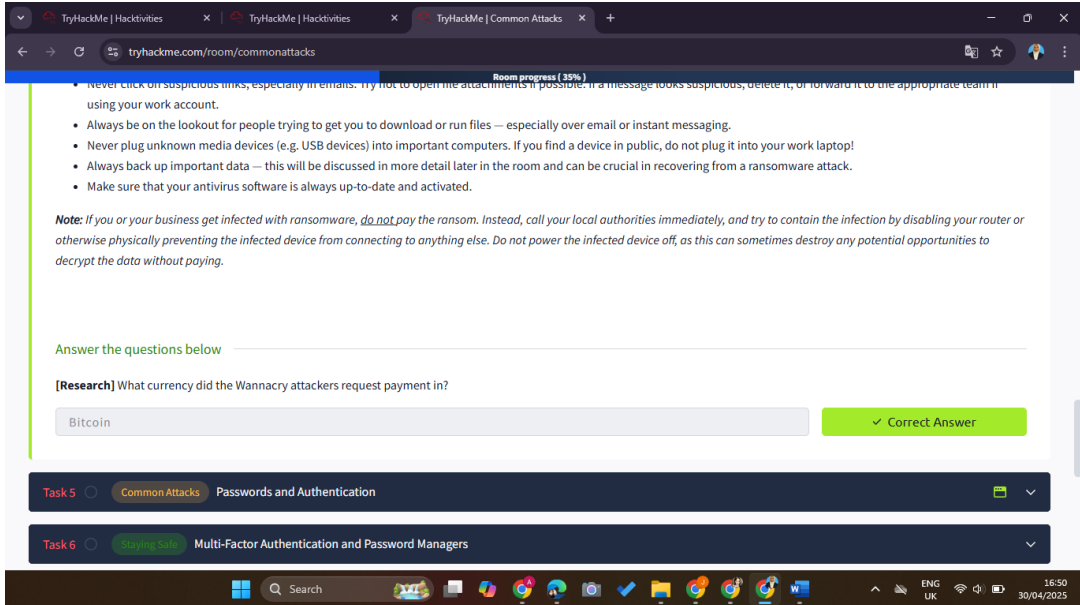


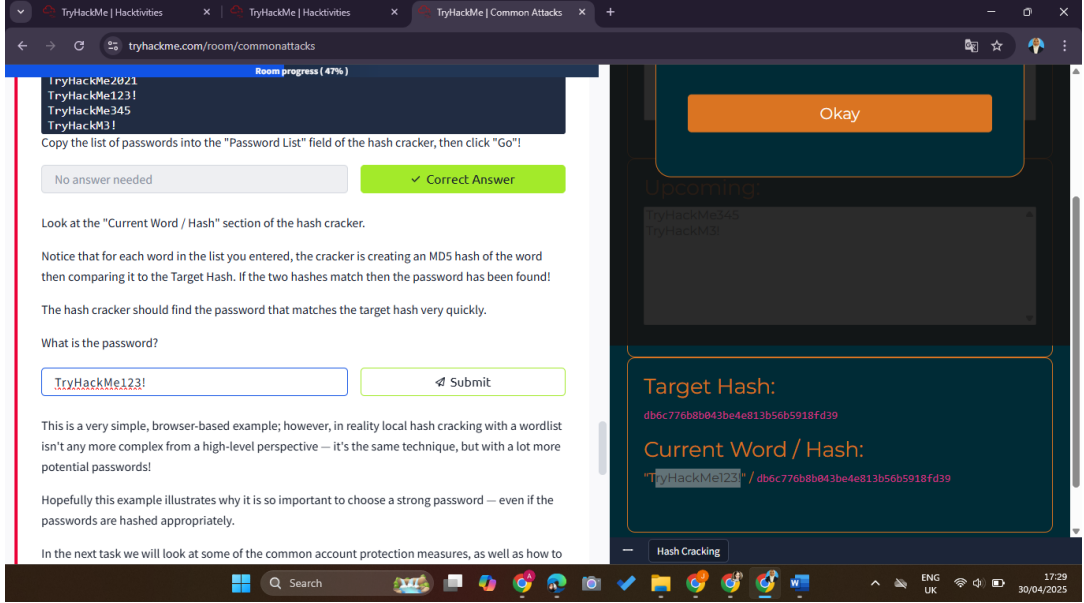
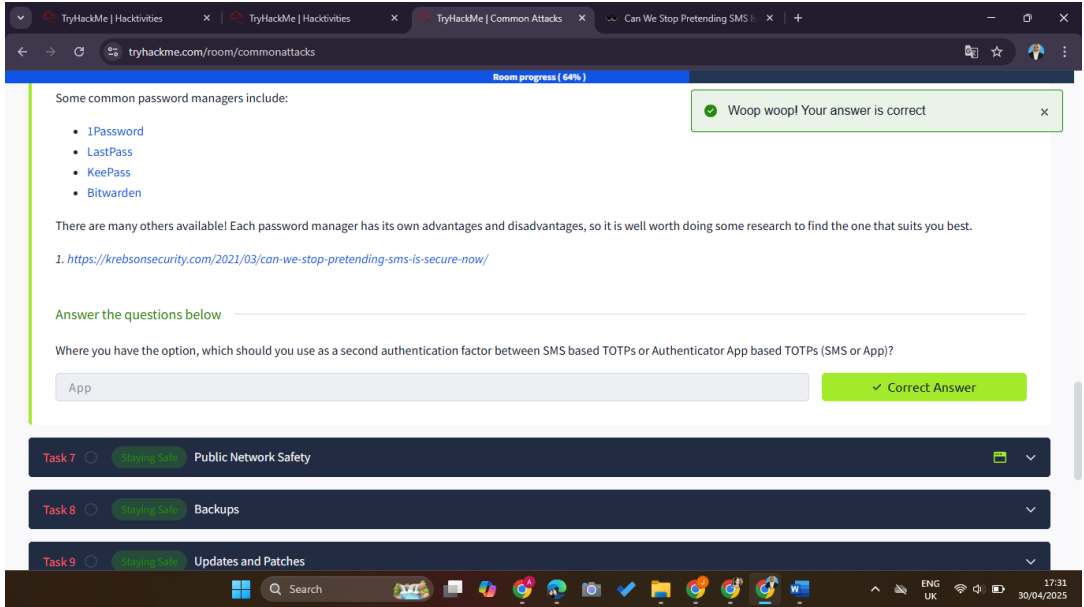
Nama : Aprintan Dwi Cahyani

NIM : 2231740021

Roadmap : CommonAttack

NO	Screenshoot Progres
1.	<div>Task 1</div>  A screenshot of a web browser showing the TryHackMe 'Common Attacks' room. A large white modal box in the center displays a green and blue circular logo with a checkmark and the text 'You've unlocked a streak freeze!'. Below the logo, it says 'With these one-time streak freezes, you can miss one day of hacking without losing your streak.' The background shows the room's interface with a 'Join Room' button and a task list on the left.
2.	<div>Task 2</div>  A screenshot of the TryHackMe 'Common Attacks' room showing the 'Introduction' task. The task text reads: 'Our existence in a digital world makes it imperative that we understand and can protect against common attacks. This room will discuss some of the most common techniques used by attackers to target people online. It will also teach some of the best ways to prevent the success of each technique. Without further ado, let's begin!'. Below the text, there is a section titled 'Answer the questions below' with a 'Let's get started!' button and a 'Complete' button. The task list on the left shows 'Task 1' as 'Introduction' and 'Task 2' as 'Social Engineering'.
3.	<div>Task 3</div>

	 <p>temporary address made for one purpose, then destroyed soon afterwards; for the occasion, then destroy it as soon as it is no longer required.</p> <p>It's worth noting at this point that anyone can fall for a <b>phishing</b> 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.</p> <p>Answer the questions below</p> <p>Click the green "View Site" button at the top of this task if you haven't already done so.</p> <p>No answer needed <span>✓ Correct Answer</span></p> <p>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.</p> <p>Good luck!</p> <p>What is the flag?</p> <p>THM(I_CAUGHT_ALL_THE_PHISH) <span>✓ Correct Answer</span></p> <p><b>Task 4</b> Common Attacks Malware and Ransomware</p> <p><b>Task 5</b> Common Attacks Passwords and Authentication</p>
4.	<h3>Task 4</h3>  <p>Room progress ( 35% )</p> <ul style="list-style-type: none"> <li>Never click on suspicious links, especially in emails. Try not to open the attachments, if possible. If a message looks suspicious, delete it, or forward it to the appropriate team if using your work account.</li> <li>Always be on the lookout for people trying to get you to download or run files — especially over email or instant messaging.</li> <li>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!</li> <li>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.</li> <li>Make sure that your antivirus software is always up-to-date and activated.</li> </ul> <p><b>Note:</b> If you or your business get infected with ransomware, <u>do not</u> 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.</p> <p>Answer the questions below</p> <p><b>[Research]</b> What currency did the Wannacry attackers request payment in?</p> <p>Bitcoin <span>✓ Correct Answer</span></p> <p><b>Task 5</b> Common Attacks Passwords and Authentication</p> <p><b>Task 6</b> Stealing Data Multi-Factor Authentication and Password Managers</p>
5.	<h3>Task 5</h3>

	
6.	<h3>Task 6</h3> 
7.	<h3>Task 7</h3>

TryHackMe | HacktivitiesTryHackMe | HacktivitiesTryHackMe | Common AttacksCan We Stop Pretending SMS

tryhackme.com/room/commonattacks

Room progress ( 88% )

Woop woopl! Your answer is correct

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* 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

Task 10 Information Conclusion

SearchENG UK17:3230/04/2025


8.

## Task 8

TryHackMe | HacktivitiesTryHackMe | HacktivitiesTryHackMe | Common AttacksCan We Stop Pretending SMS

tryhackme.com/room/commonattacks

Woop woopl! Your answer is correct



Congratulations on completing Common Attacks!!! 🎉

Leave Feedback

Next

SearchENG UK17:3230/04/2025