LAPORAN TUGAS PYTON & COMMON ATTACK

Oleh:

MUHAMMAD SU’ADI (2231740040)

Dosen Pengajar:

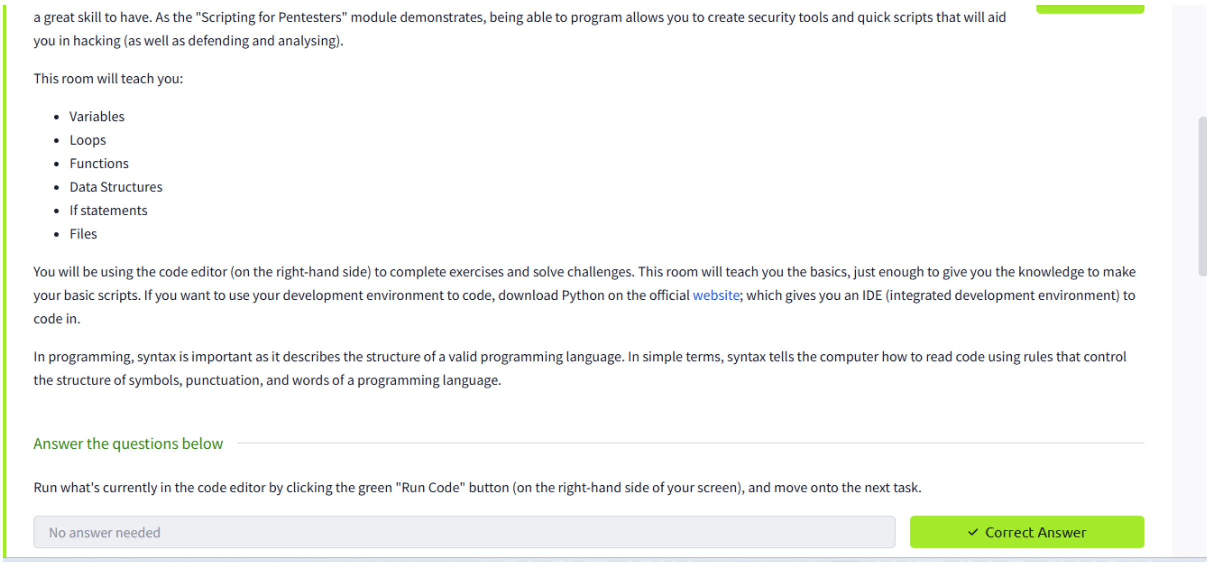
Vipkas Al Hadid Firdaus, S.T, M.T.

PROGRAM STUDI D3 TEKNOLGI INFORMASI

POLITEKNIK NEGERI MALANG PSDKU LUMAJANG TAHUN 2025

Pyton basics

1.



a great skill to have. As the "Scripting for Pentesters" module demonstrates, being able to program allows you to create security tools and quick scripts that will aid you in hacking (as well as defending and analysing).

This room will teach you:

- Variables
- Loops
- Functions
- Data Structures
- If statements
- Files

You will be using the code editor (on the right-hand side) to complete exercises and solve challenges. This room will teach you the basics, just enough to give you the knowledge to make your basic scripts. If you want to use your development environment to code, download Python on the official website; which gives you an IDE (integrated development environment) to code in.

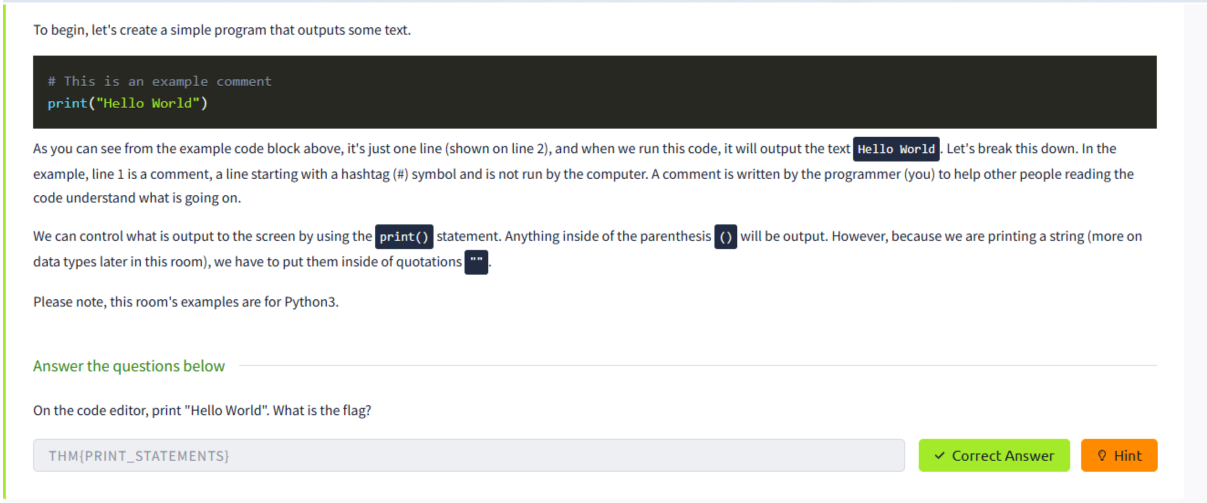
In programming, syntax is important as it describes the structure of a valid programming language. In simple terms, syntax tells the computer how to read code using rules that control the structure of symbols, punctuation, and words of a programming language.

Answer the questions below

Run what's currently in the code editor by clicking the green "Run Code" button (on the right-hand side of your screen), and move onto the next task.

No answer needed

2.



To begin, let's create a simple program that outputs some text.

```
# This is an example comment
print("Hello World")
```

As you can see from the example code block above, it's just one line (shown on line 2), and when we run this code, it will output the text `Hello World`. Let's break this down. In the example, line 1 is a comment, a line starting with a hashtag (#) symbol and is not run by the computer. A comment is written by the programmer (you) to help other people reading the code understand what is going on.

We can control what is output to the screen by using the `print()` statement. Anything inside of the parenthesis `()` will be output. However, because we are printing a string (more on data types later in this room), we have to put them inside of quotations `""`.

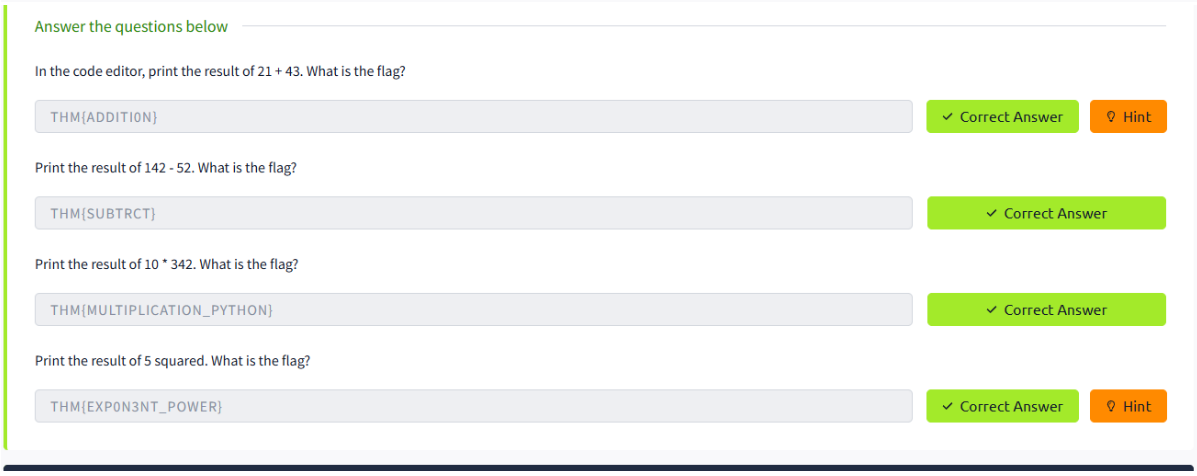
Please note, this room's examples are for Python3.

Answer the questions below

On the code editor, print "Hello World". What is the flag?

THM{PRINT_STATEMENTS}

3.



Answer the questions below

In the code editor, print the result of 21 + 43. What is the flag?

THM{ADDITION}

Print the result of 142 - 52. What is the flag?

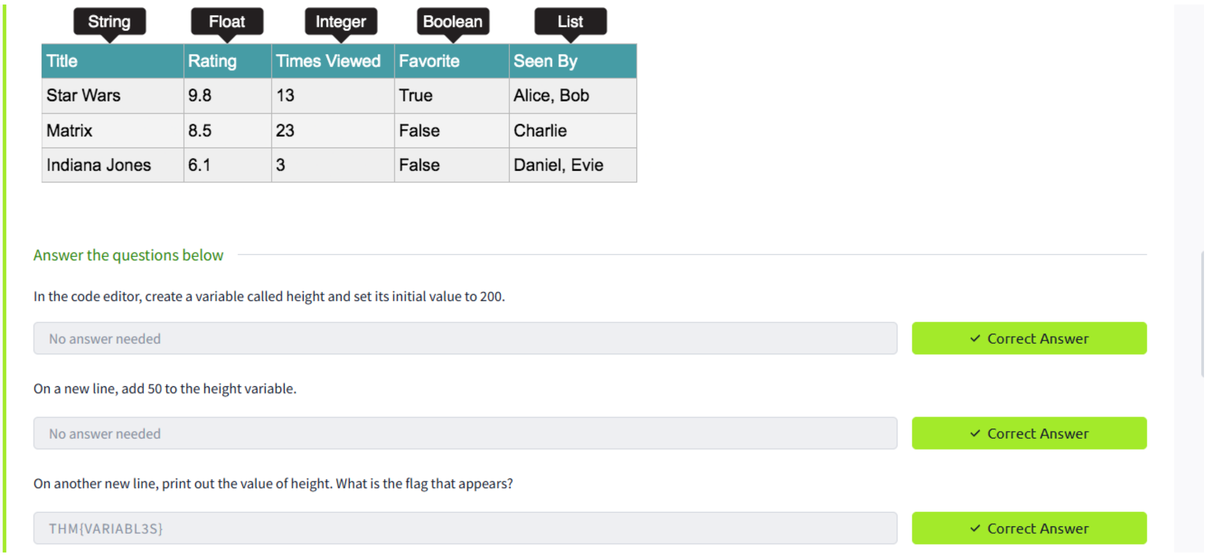
THM{SUBTRCT}

Print the result of 10 * 342. What is the flag?

THM{MULTIPLICATION_PYTHON}

Print the result of 5 squared. What is the flag?

THM{EXP0N3NT_POWER}



String	Float	Integer	Boolean	List
Title	Rating	Times Viewed	Favorite	Seen By
Star Wars	9.8	13	True	Alice, Bob
Matrix	8.5	23	False	Charlie
Indiana Jones	6.1	3	False	Daniel, Evie

Answer the questions below

In the code editor, create a variable called height and set its initial value to 200.

No answer needed ✓ Correct Answer

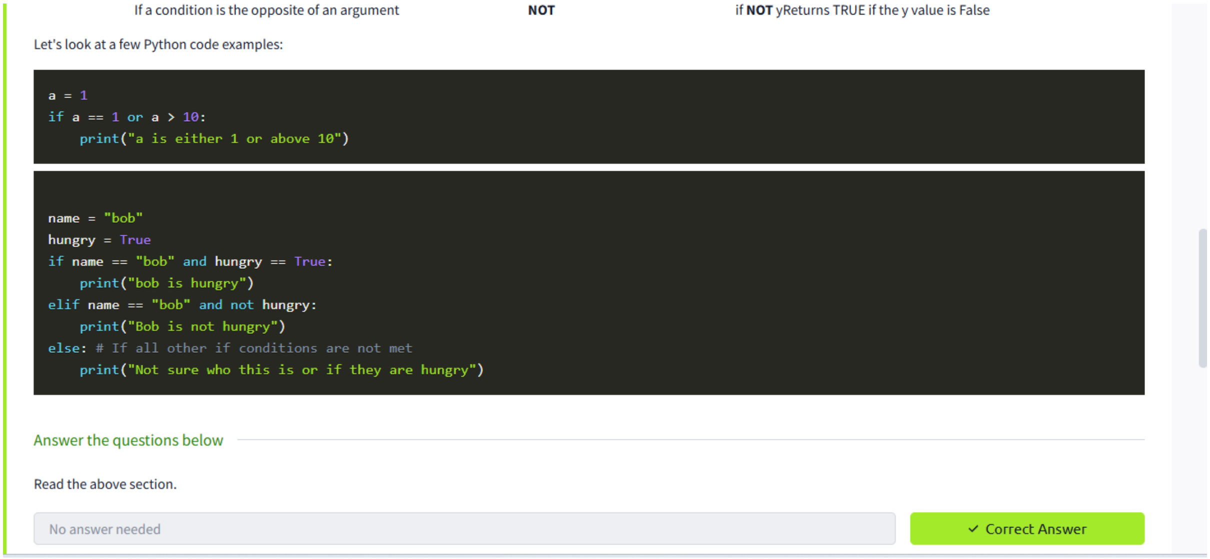
On a new line, add 50 to the height variable.

No answer needed ✓ Correct Answer

On another new line, print out the value of height. What is the flag that appears?

THM{VARIABL3S} ✓ Correct Answer

4.



If a condition is the opposite of an argument	**NOT**	if **NOT** yReturns TRUE if the y value is False

Let's look at a few Python code examples:

```
a = 1
if a == 1 or a > 10:
    print("a is either 1 or above 10")
```

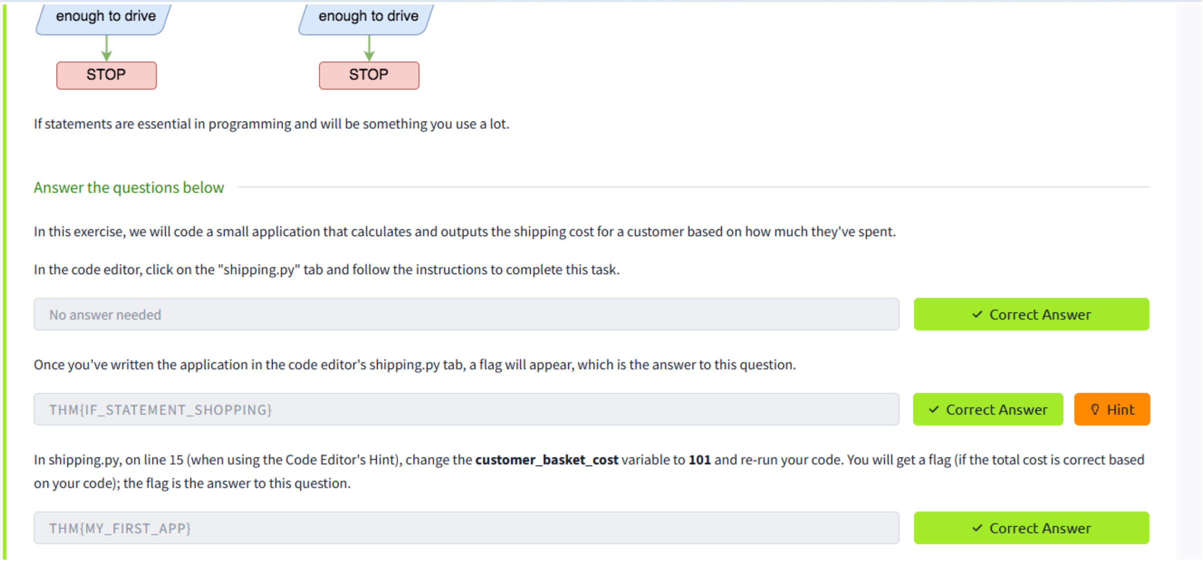
```
name = "bob"
hungry = True
if name == "bob" and hungry == True:
    print("bob is hungry")
elif name == "bob" and not hungry:
    print("Bob is not hungry")
else: # If all other if conditions are not met
    print("Not sure who this is or if they are hungry")
```

Answer the questions below

Read the above section.

No answer needed ✓ Correct Answer

5.



If statements are essential in programming and will be something you use a lot.

Answer the questions below

In this exercise, we will code a small application that calculates and outputs the shipping cost for a customer based on how much they've spent.

In the code editor, click on the "shipping.py" tab and follow the instructions to complete this task.

No answer needed ✓ Correct Answer

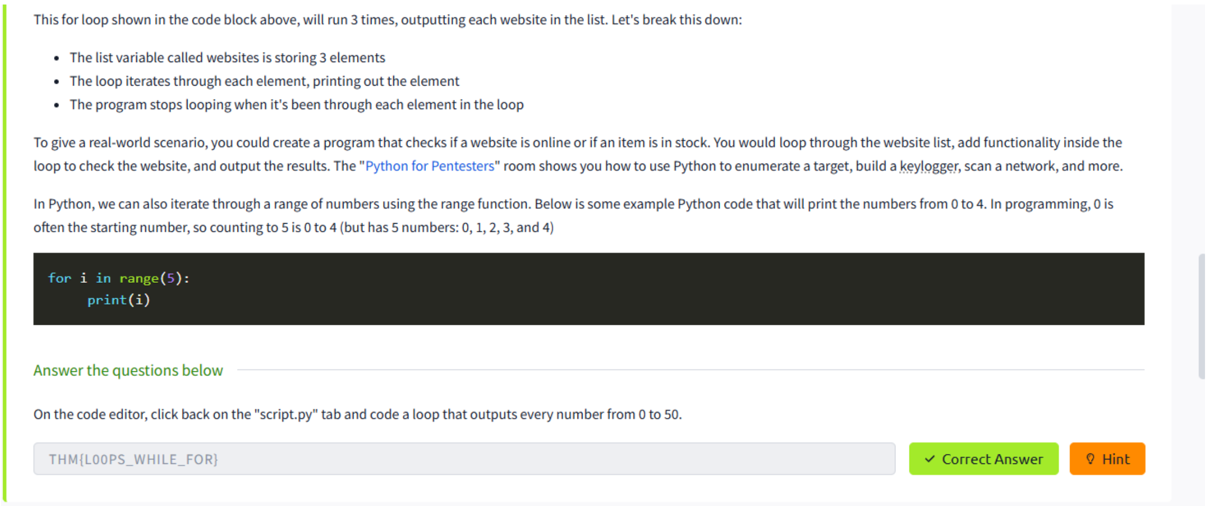
Once you've written the application in the code editor's shipping.py tab, a flag will appear, which is the answer to this question.

THM{IF_STATEMENT_SHOPPING} ✓ Correct Answer 💡 Hint

In shipping.py, on line 15 (when using the Code Editor's Hint), change the **customer_basket_cost** variable to **101** and re-run your code. You will get a flag (if the total cost is correct based on your code); the flag is the answer to this question.

THM{MY_FIRST_APP} ✓ Correct Answer

6.



This for loop shown in the code block above, will run 3 times, outputting each website in the list. Let's break this down:

- The list variable called websites is storing 3 elements
- The loop iterates through each element, printing out the element
- The program stops looping when it's been through each element in the loop

To give a real-world scenario, you could create a program that checks if a website is online or if an item is in stock. You would loop through the website list, add functionality inside the loop to check the website, and output the results. The "Python for Pentesters" room shows you how to use Python to enumerate a target, build a keylogger, scan a network, and more.

In Python, we can also iterate through a range of numbers using the range function. Below is some example Python code that will print the numbers from 0 to 4. In programming, 0 is often the starting number, so counting to 5 is 0 to 4 (but has 5 numbers: 0, 1, 2, 3, and 4)

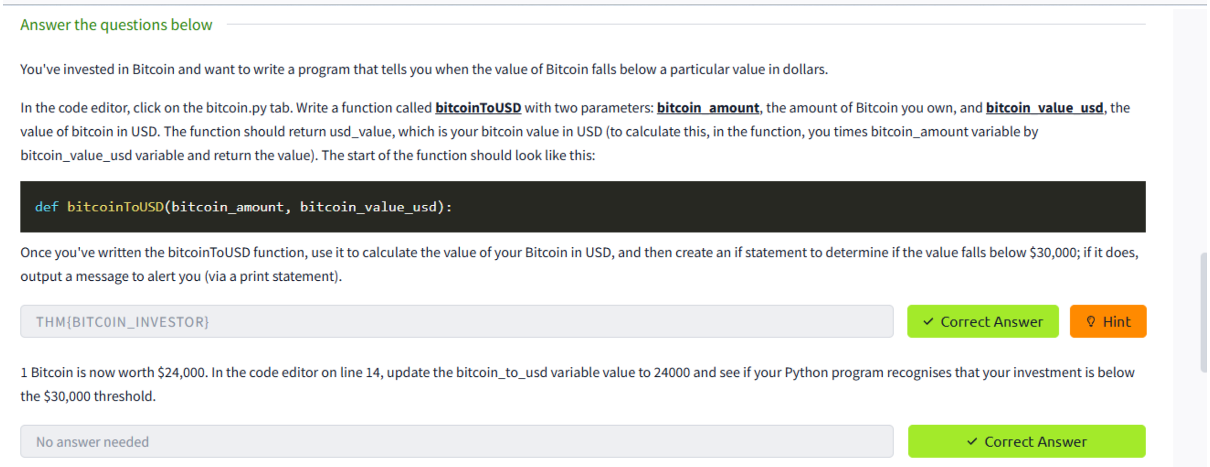
```
for i in range(5):
     print(i)
```

Answer the questions below

On the code editor, click back on the "script.py" tab and code a loop that outputs every number from 0 to 50.

THM{L00PS_WHILE_FOR}

7.



Answer the questions below

You've invested in Bitcoin and want to write a program that tells you when the value of Bitcoin falls below a particular value in dollars.

In the code editor, click on the bitcoin.py tab. Write a function called **bitcoinToUSD** with two parameters: **bitcoin_amount**, the amount of Bitcoin you own, and **bitcoin_value_usd**, the value of bitcoin in USD. The function should return usd_value, which is your bitcoin value in USD (to calculate this, in the function, you times bitcoin_amount variable by bitcoin_value_usd variable and return the value). The start of the function should look like this:

```
def bitcoinToUSD(bitcoin_amount, bitcoin_value_usd):
```

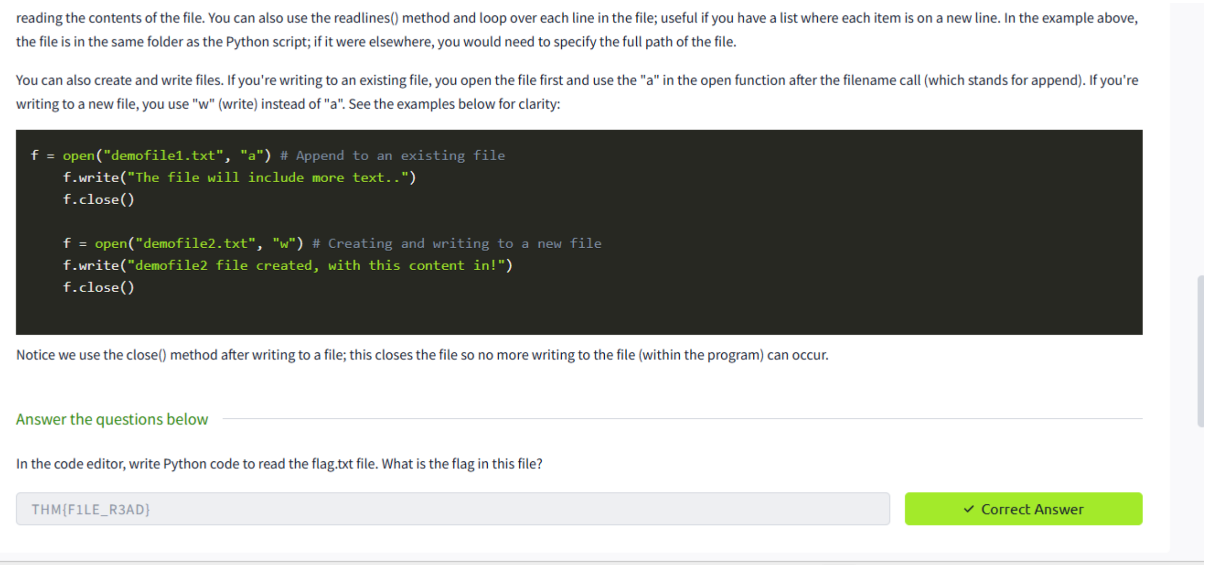
Once you've written the bitcoinToUSD function, use it to calculate the value of your Bitcoin in USD, and then create an if statement to determine if the value falls below $30,000; if it does, output a message to alert you (via a print statement).

THM{BITCOIN_INVESTOR}

1 Bitcoin is now worth $24,000. In the code editor on line 14, update the bitcoin_to_usd variable value to 24000 and see if your Python program recognises that your investment is below the $30,000 threshold.

No answer needed

8.



reading the contents of the file. You can also use the readlines() method and loop over each line in the file; useful if you have a list where each item is on a new line. In the example above, the file is in the same folder as the Python script; if it were elsewhere, you would need to specify the full path of the file.

You can also create and write files. If you're writing to an existing file, you open the file first and use the "a" in the open function after the filename call (which stands for append). If you're writing to a new file, you use "w" (write) instead of "a". See the examples below for clarity:

```
f = open("demofile1.txt", "a") # Append to an existing file
    f.write("The file will include more text..")
    f.close()

    f = open("demofile2.txt", "w") # Creating and writing to a new file
    f.write("demofile2 file created, with this content in!")
    f.close()
```

Notice we use the close() method after writing to a file; this closes the file so no more writing to the file (within the program) can occur.

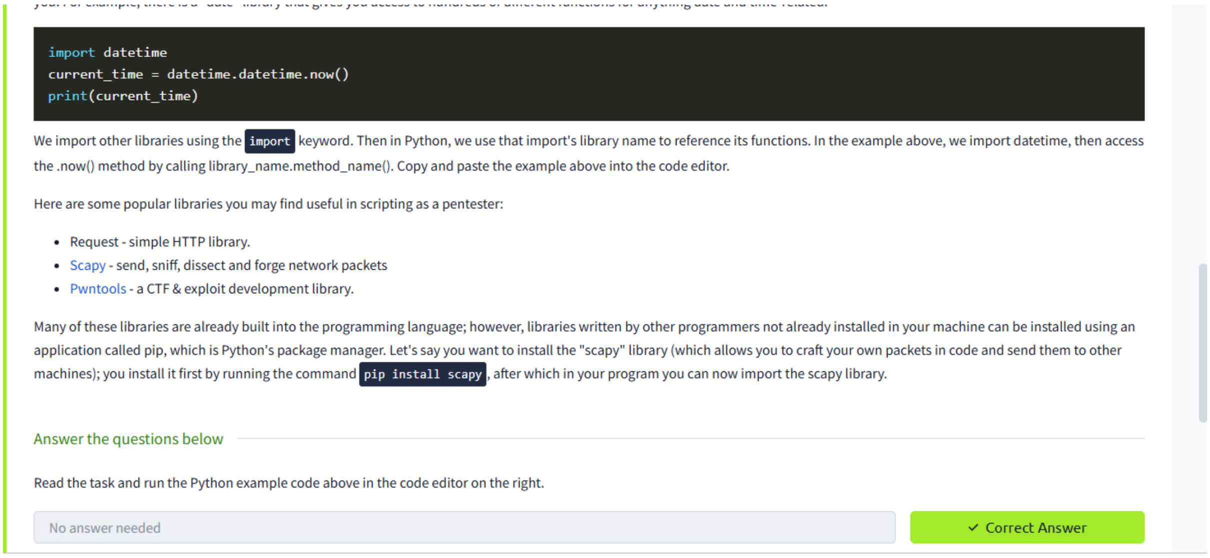
Answer the questions below

In the code editor, write Python code to read the flag.txt file. What is the flag in this file?

THM{F1LE_R3AD}

9.

10.



you. For example, there is a "date" library that gives you access to hundreds of different functions for anything date and time-related.

```
import datetime
current_time = datetime.datetime.now()
print(current_time)
```

We import other libraries using the `import` keyword. Then in Python, we use that import's library name to reference its functions. In the example above, we import datetime, then access the .now() method by calling library_name.method_name(). Copy and paste the example above into the code editor.

Here are some popular libraries you may find useful in scripting as a pentester:

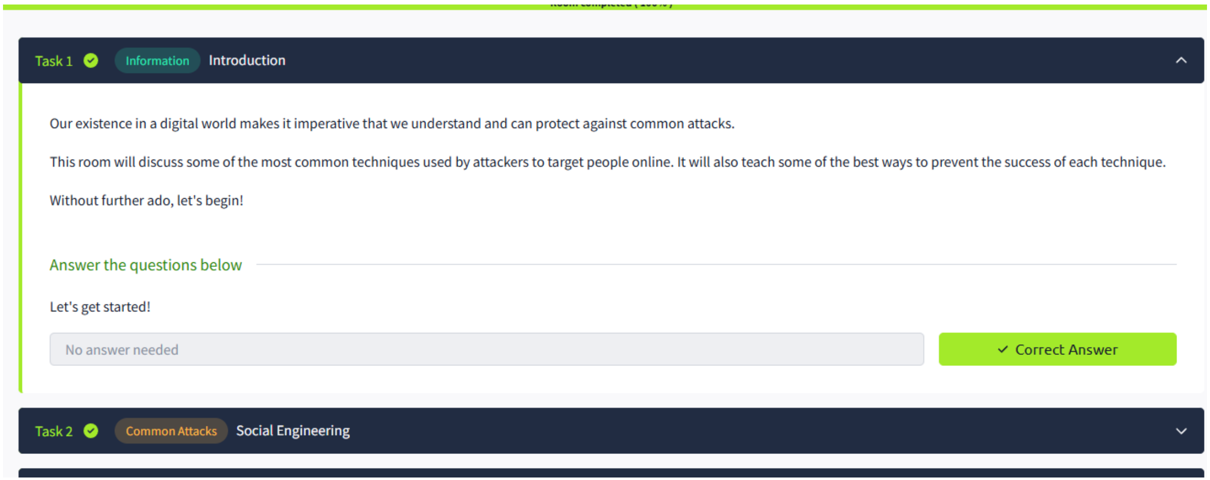
- Request - simple HTTP library.
- Scapy - send, sniff, dissect and forge network packets
- Pwntools - a CTF & exploit development library.

Many of these libraries are already built into the programming language; however, libraries written by other programmers not already installed in your machine can be installed using an application called pip, which is Python's package manager. Let's say you want to install the "scapy" library (which allows you to craft your own packets in code and send them to other machines); you install it first by running the command `pip install scapy`, after which in your program you can now import the scapy library.

Answer the questions below

Read the task and run the Python example code above in the code editor on the right.

Common Attack



Task 1 ✓ Information Introduction

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!

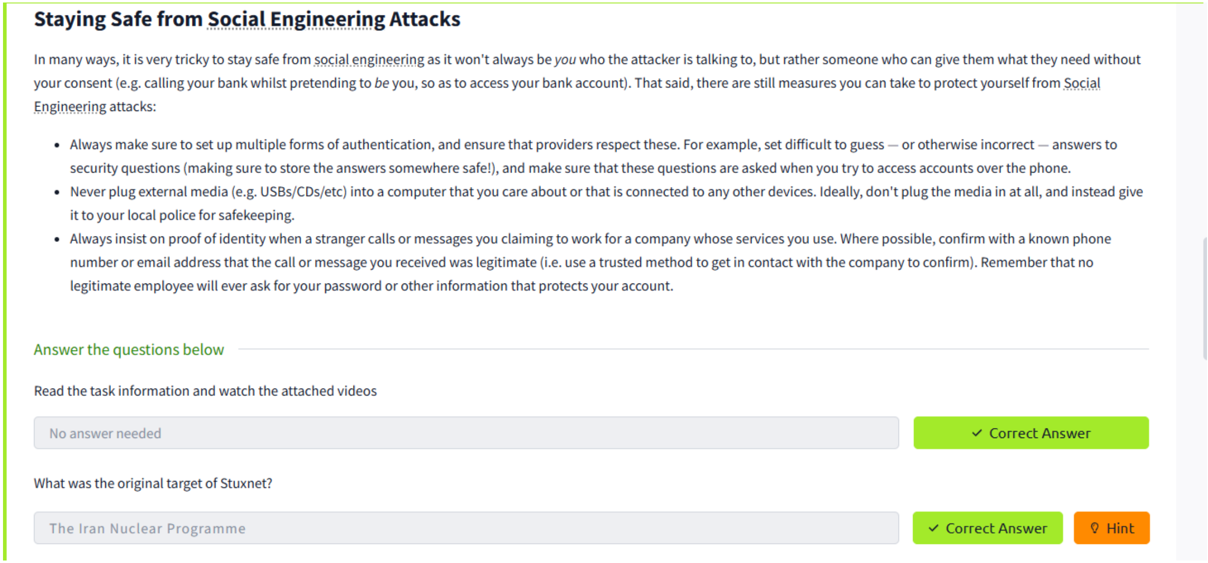
Answer the questions below

Let's get started!

No answer needed ✓ Correct Answer

Task 2 ✓ Common Attacks Social Engineering

1.



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

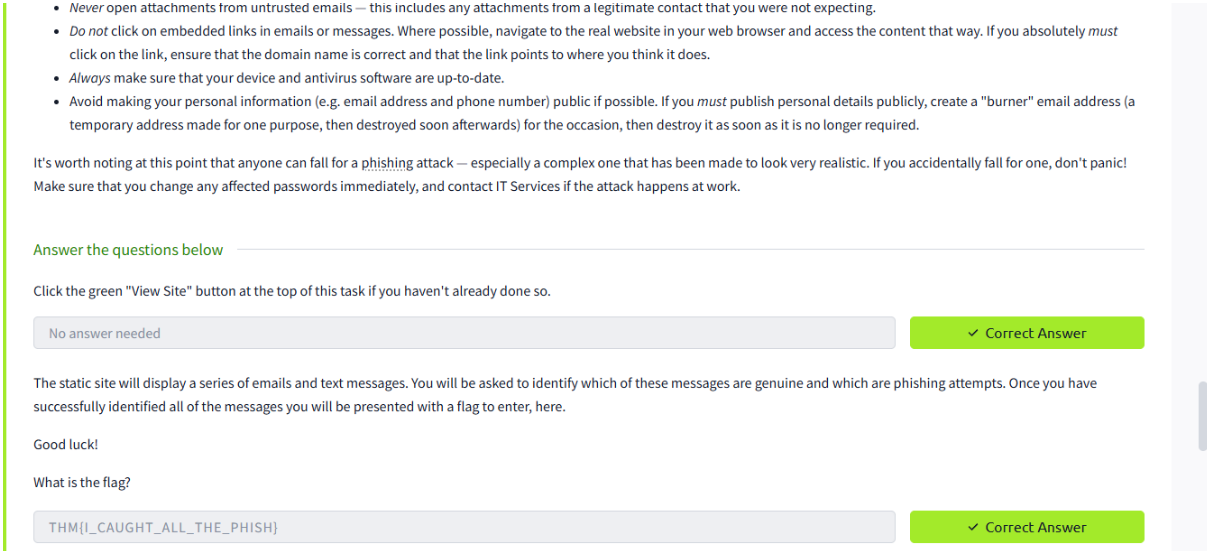
Read the task information and watch the attached videos

No answer needed ✓ Correct Answer

What was the original target of Stuxnet?

The Iran Nuclear Programme ✓ Correct Answer Hint

2.



- *Never* open attachments from untrusted emails — this includes any attachments from a legitimate contact that you were not expecting.
- *Do not* click on embedded links in emails or messages. Where possible, navigate to the real website in your web browser and access the content that way. If you absolutely *must* click on the link, ensure that the domain name is correct and that the link points to where you think it does.
- *Always* make sure that your device and antivirus software are up-to-date.
- 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.

No answer needed ✓ Correct Answer

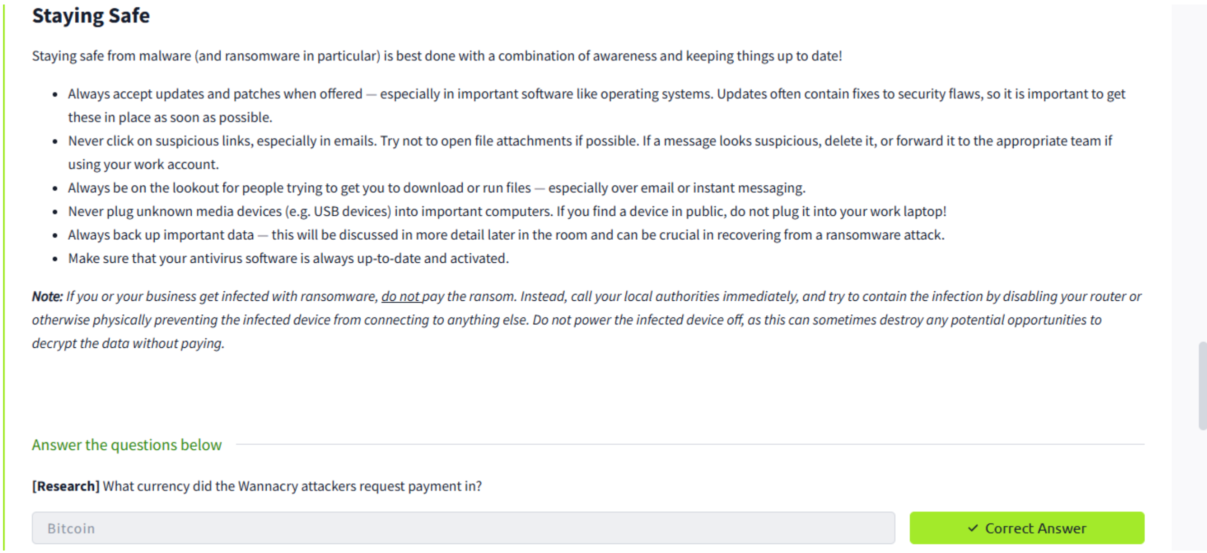
The static site will display a series of emails and text messages. You will be asked to identify which of these messages are genuine and which are phishing attempts. Once you have successfully identified all of the messages you will be presented with a flag to enter, here.

Good luck!

What is the flag?

THM{I_CAUGHT_ALL_THE_PHISH} ✓ Correct Answer

3.



Staying Safe

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

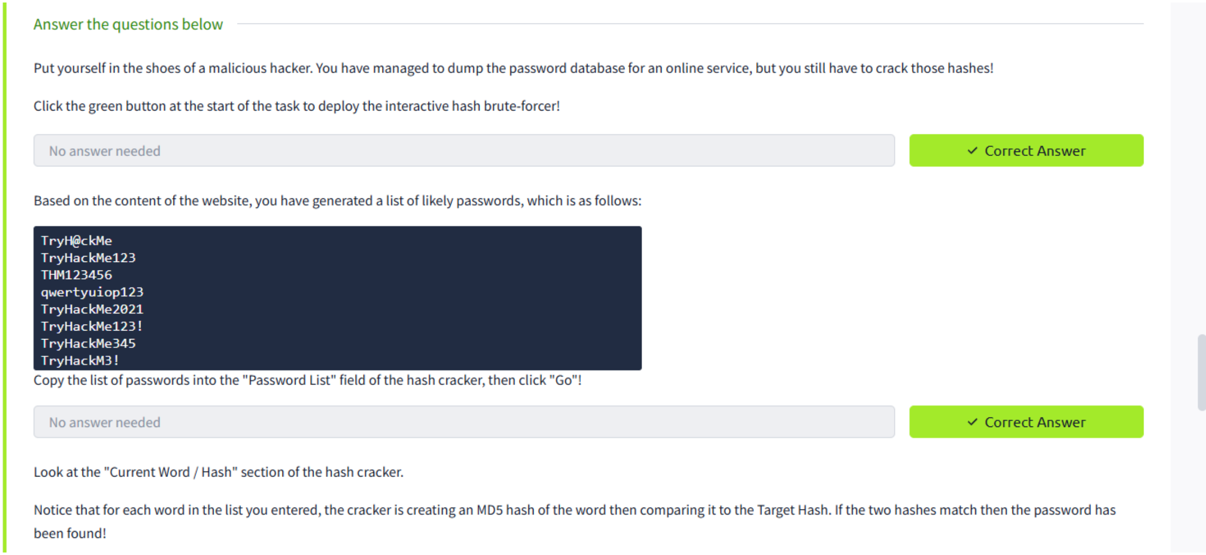
- Always accept updates and patches when offered — especially in important software like operating systems. Updates often contain fixes to security flaws, so it is important to get these in place as soon as possible.
- Never click on suspicious links, especially in emails. Try not to open file attachments 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?

4. Bitcoin ✓ Correct Answer



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
THM123456
qwertyuiop123
TryHackMe2021
TryHackMe123!
TryHackMe345
TryHackM3!
```

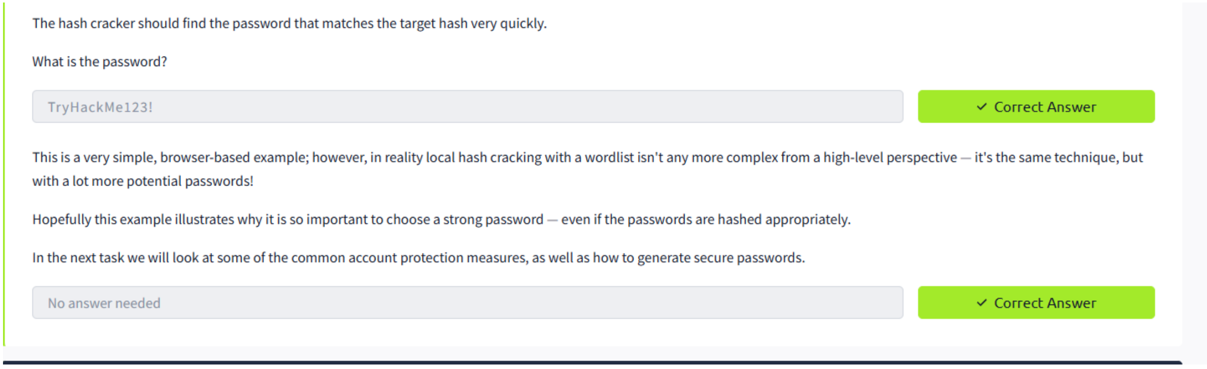
Copy the list of passwords into the "Password List" field of the hash cracker, then click "Go"!

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!

5.



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

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 TOTPs or Authenticator App based TOTPs (SMS or App)?

App

✓ Correct Answer

6.

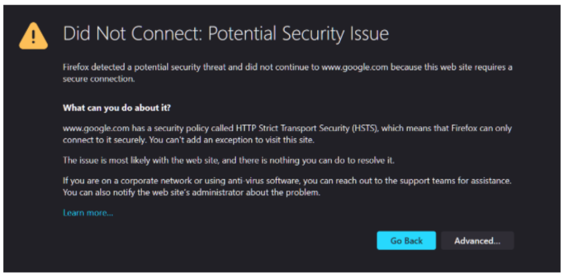
With this in place, your traffic can only be decrypted in very select circumstances: namely, if it is a work or school managed device and you are connected to a work/school network.

Note: *The presence of the padlock indicates that the connection is secure; it does not guarantee that the website itself is* safe *. In other words, a malicious website can still easily have a TLS cert (meaning that your traffic with the server* is *encrypted), but that doesn't stop the site from having a malicious purpose.*

If you are accessing a website *without* the padlock symbol, **never** enter any credentials or sensitive information — especially if you are using an untrusted network.

In some instances, you may also see a padlock with a cross through it or an exclamation mark over it; this indicates that the connection is *theoretically* secure but that there is something wrong with the certificate in use by the server. The presence of this altered padlock icon can mean anything from the server administrator simply letting the certificate go out of date to an attacker actively meddling with the security of your connection. In other words: if the icon is anything other than a regular padlock, *do not trust that connection is secure.*

You may also encounter full-page errors related to certificate security when trying to access web pages; these can look something like this:



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...

7.

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.

Answer the questions below

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

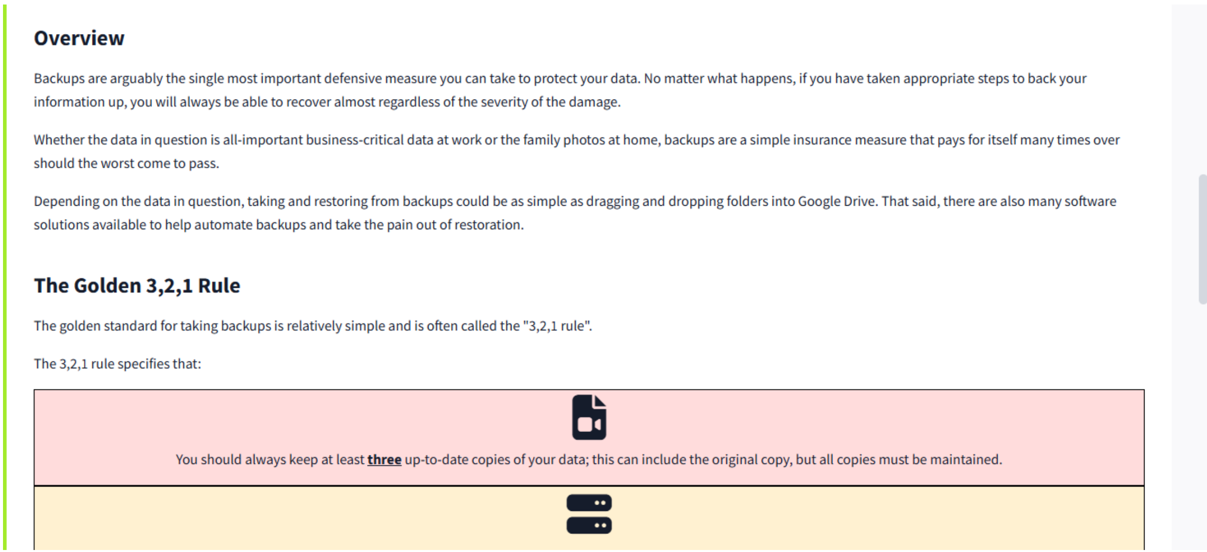
No answer needed

✓ Correct Answer

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

✓ Correct Answer



Overview

Backups are arguably the single most important defensive measure you can take to protect your data. No matter what happens, if you have taken appropriate steps to back your information up, you will always be able to recover almost regardless of the severity of the damage.

Whether the data in question is all-important business-critical data at work or the family photos at home, backups are a simple insurance measure that pays for itself many times over should the worst come to pass.

Depending on the data in question, taking and restoring from backups could be as simple as dragging and dropping folders into Google Drive. That said, there are also many software solutions available to help automate backups and take the pain out of restoration.

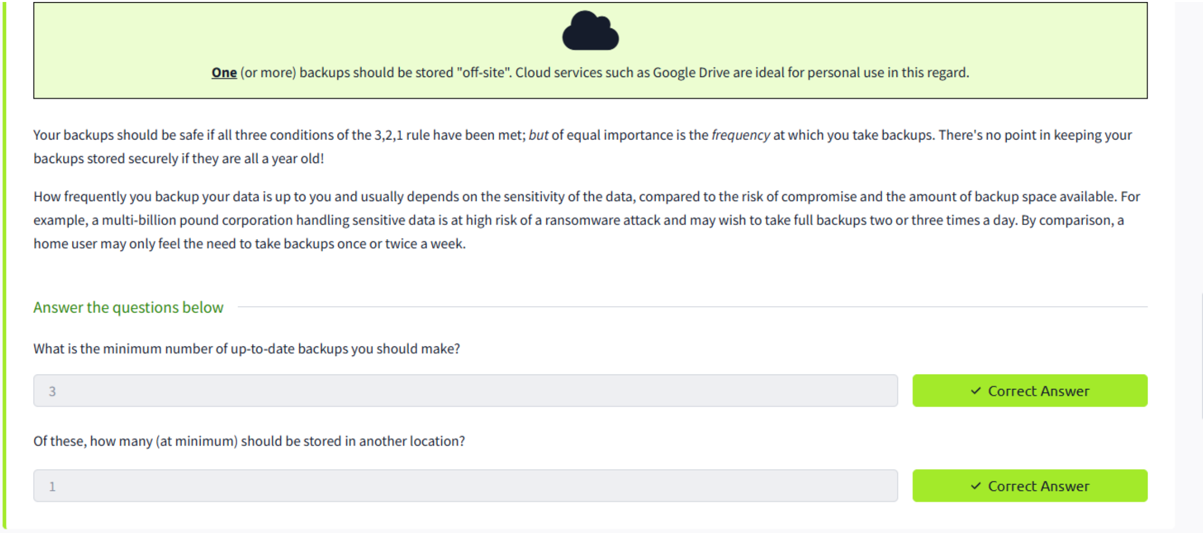
The Golden 3,2,1 Rule

The golden standard for taking backups is relatively simple and is often called the "3,2,1 rule".

The 3,2,1 rule specifies that:

You should always keep at least **three** up-to-date copies of your data; this can include the original copy, but all copies must be maintained.

8.



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.

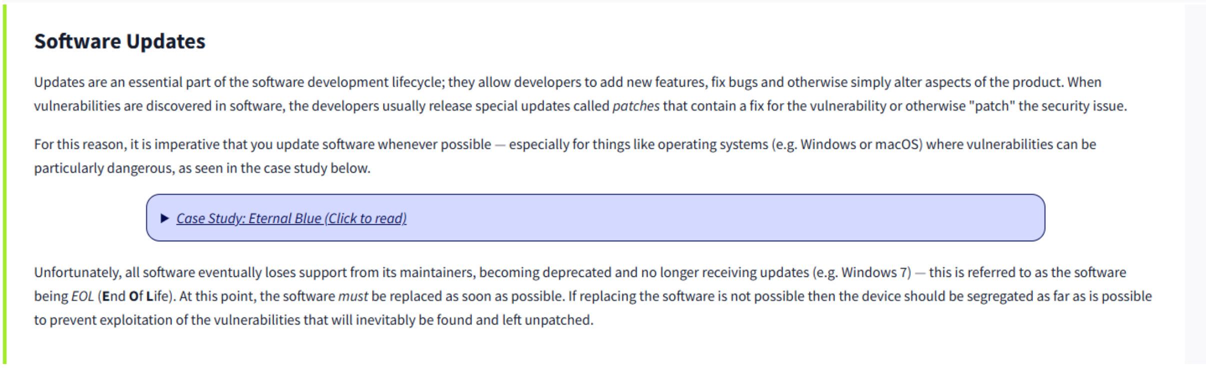
Answer the questions below

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

3

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

1



Software Updates

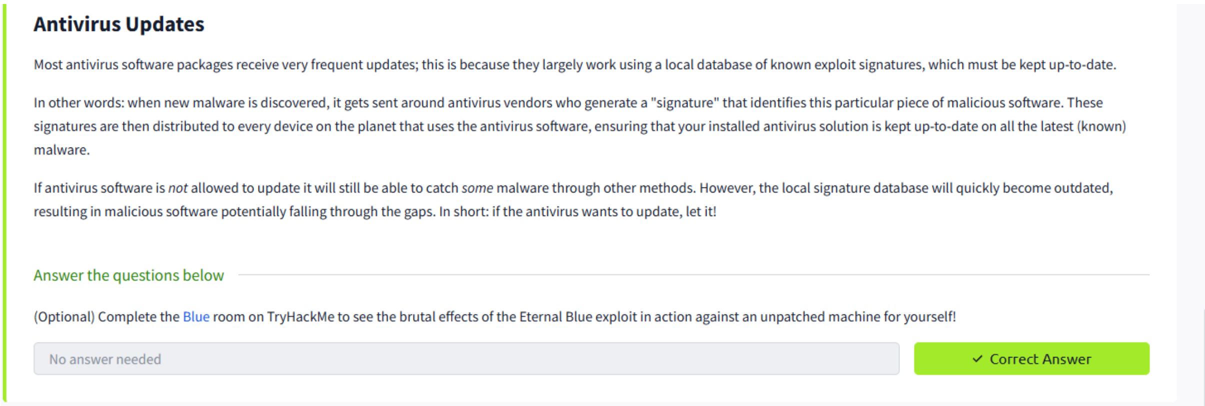
Updates are an essential part of the software development lifecycle; they allow developers to add new features, fix bugs and otherwise simply alter aspects of the product. When vulnerabilities are discovered in software, the developers usually release special updates called *patches* that contain a fix for the vulnerability or otherwise "patch" the security issue.

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* (**E**nd **O**f **L**ife). 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.

9.



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.

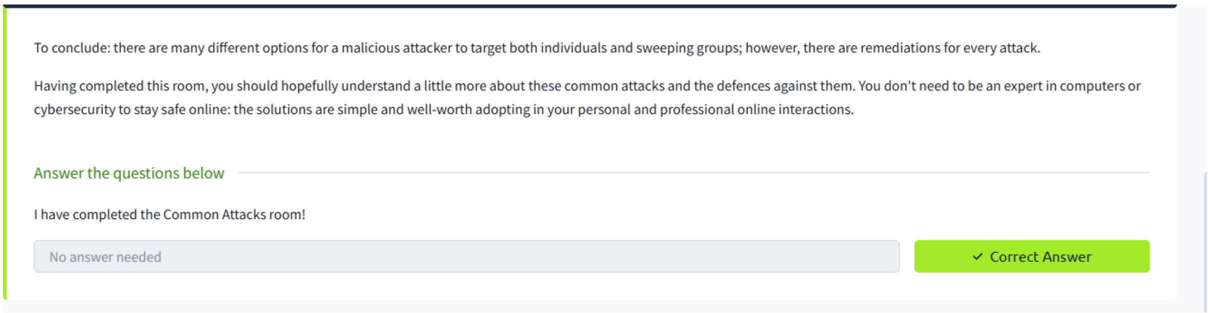
In other words: when new malware is discovered, it gets sent around antivirus vendors who generate a "signature" that identifies this particular piece of malicious software. These signatures are then distributed to every device on the planet that uses the antivirus software, ensuring that your installed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

10. 

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