MAL: Strings TryHackme Writeup

Shamsher khan · Follow
6 min read · May 11, 2021

By Shamsher khan This is a Writeup of Tryhackme room “MAL: Strings”

https://tryhackme.com/room/malstrings

Room link: https://tryhackme.com/room/malstrings
Note: This room is for Premium Members Only. who purchased THM premium membership.

Investigating “strings” within an application and why these values are important!

Motivation:

What you will learn after completing this Room:

- String analysis

- OSINT
- Static Analysis(Part of Malware Analysis)

What are “strings”?

From a programming perspective, “strings” is the term given for data handled by an application. At a broader view, these pieces of data are used to store information such as text to numerical values.

For example, let’s say we have an application such as a calculator. A user will have to input two numerical values (e.g. 1 and 5) combined with an operator (e.g. + or plus) addition in this case. These values will be stored as “strings”.

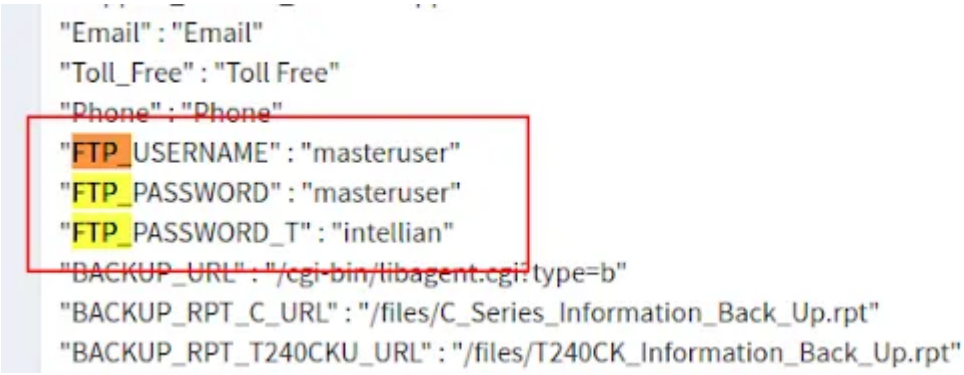
However “strings” can be stored within the application itself — where no input is necessary from the user. For example, using the example of usernames and passwords is a great representation of the many types of information that may be stored as a “string”.

Why are “strings” important?

We’re all security-minded people here and know that writing down passwords isn’t a very smart thing to do. However, developers are not quite so likeminded and often leave credentials in applications which are often essential i.e. An application that server needs to know the IP address of it. Arguably, an IP address is trivial in comparison to the sensitivity of a password — but both would be stored as strings.

There are a plethora of examples of companies storing sensitive information such as passwords within their applications. For example, Intellian, a satellite-communications focused company had the disclosure of their **“Aptus Web 1.24”** application retaining a default passcode of “12345678”.

Illustrated below is an example of an Android Application containing sensitive credentials within strings:



(Credit: Ezequiel., Skullarmy)

Time for a bit of research to solve the questions below!

Question 1. What is the **name of the account** that had the passcode of "12345678" in the intellian example discussed above?

> *Answer: intellian*

Question 2. What is the CVE entry disclosed by the company "Teradata" in their "Viewpoint" Application that has a password within a string?

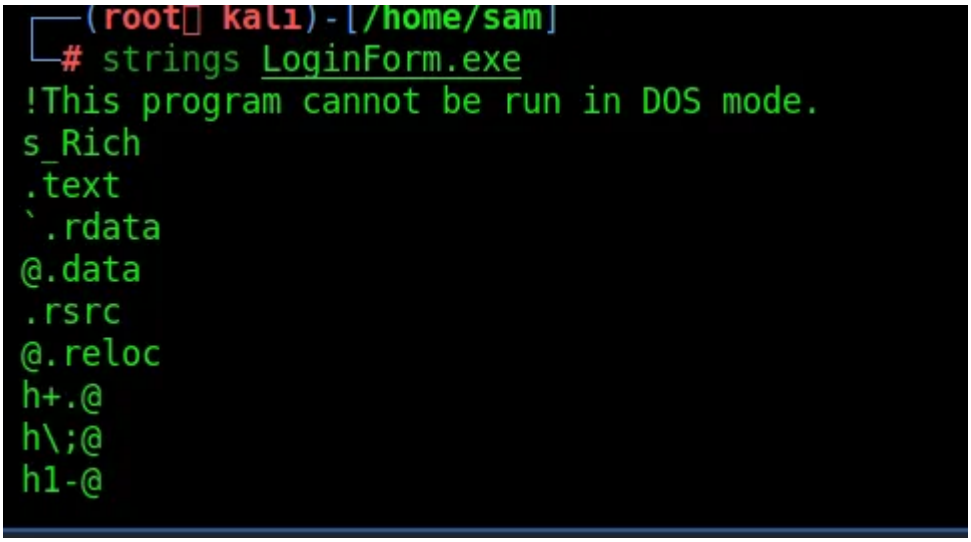
> *Answer: CVE-2019–6499*

Question 3. According to **OWASP's** list of **"Top Ten IoT"** vulnerabilities, name the ranking this vulnerability would fall within, represented as text.

> *Answer: one*

Task 2. Practical: Extracting "strings" From an Application

It is a little console program I have written in c++ for this example that replicates a login prompt. We will be using Kali Linux. You can use the



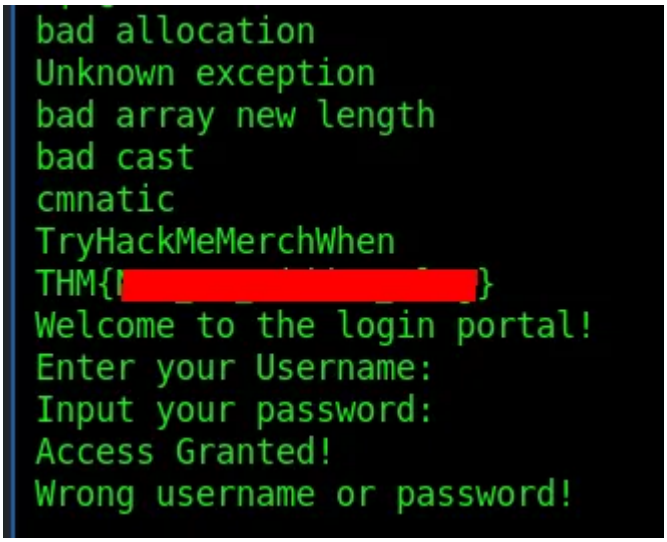
Question 1. What is the correct username required by the “LoginForm”?

> *Answer: cmnatic*

Question 2. What is the required password to authenticate with?

> *Answer: TryHackMeMerchWhen*

Question 3. What is the “hidden” THM{} flag?



Task 3. Strings in the Context of Malware

Question 1. What is the key term to describe a server that Botnets recieve instructions from?

> *Answer: Command and Control*

Question 2. Name the discussed example malware that uses “strings” to store the bitcoin wallet addresses for payment

> *Answer: Wannacry*

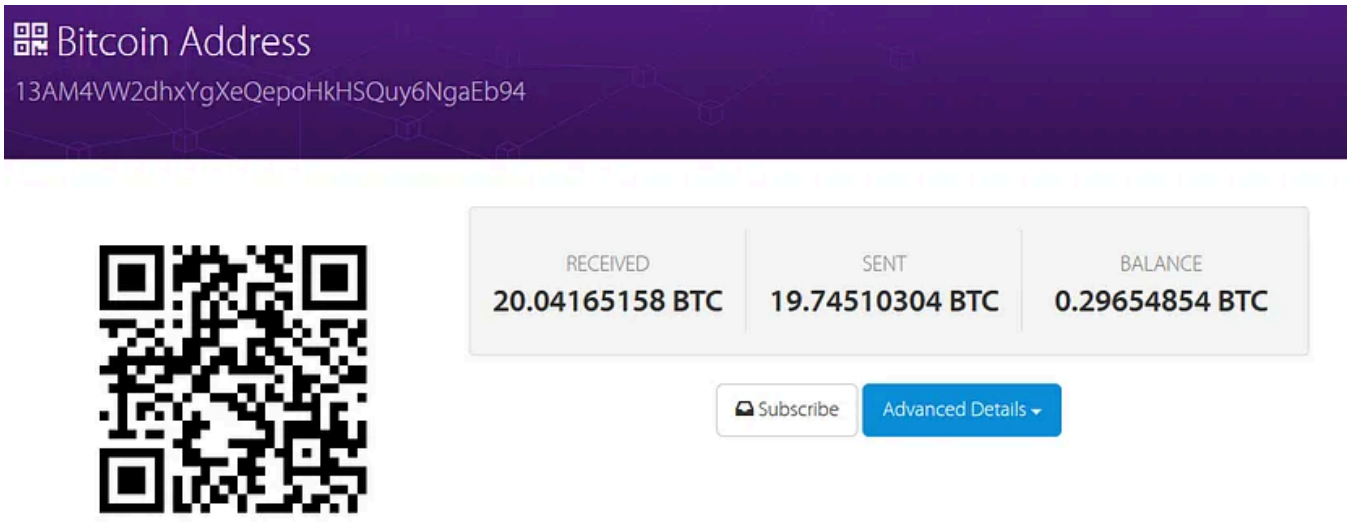
Task 4. Practical: Finding Bitcoin Addresses in Ransomware (Deploy!)

What is Bitcoin?

At a brief overview, Bitcoin is an "anonymous" online payment currency in the sense that there is no direct attribution between the sender and recipient. Authors of ransomware use this currency because of this trait — however, just because there is no attribution such as real names like traditional payment methods, it is traceable by Law Enforcement (albeit difficult).

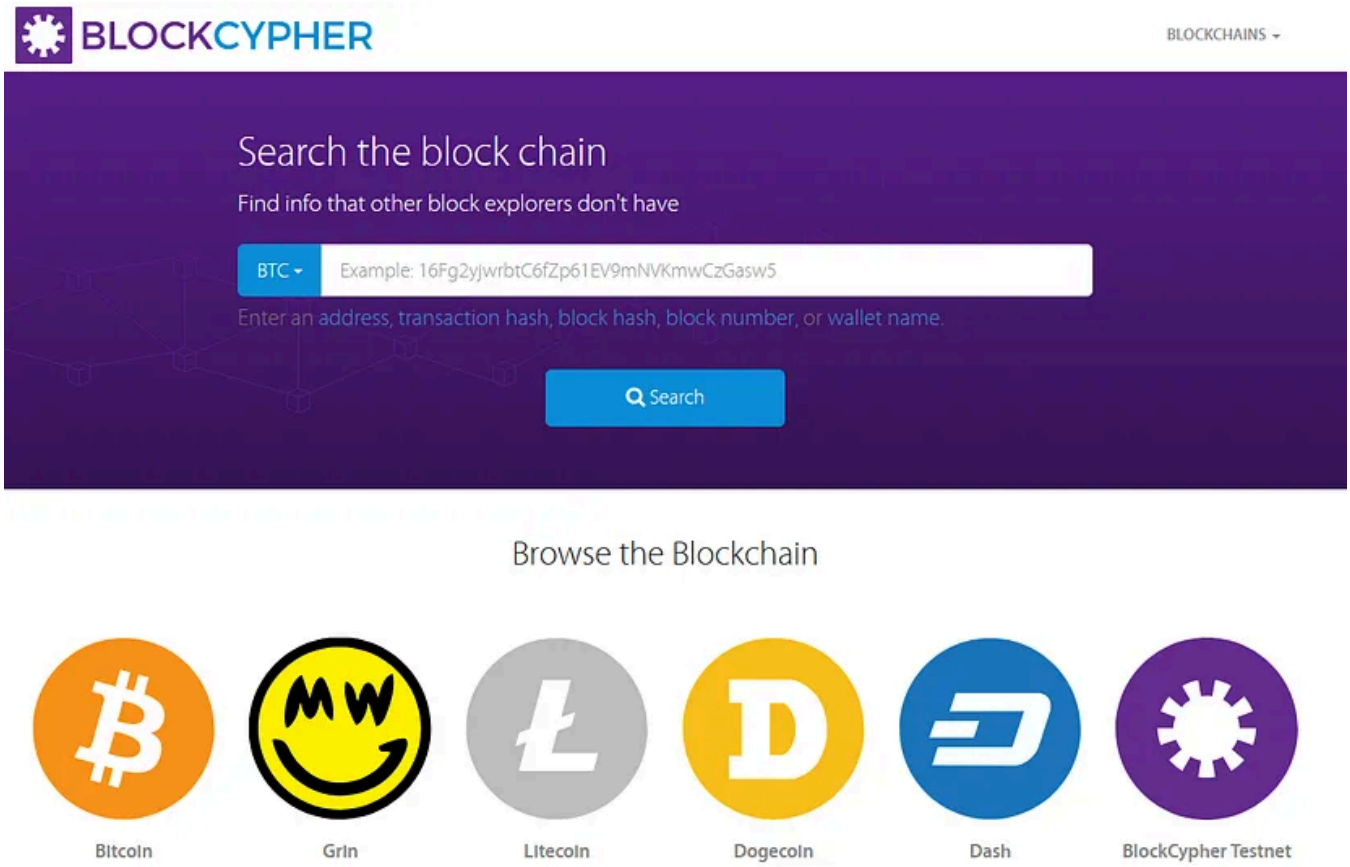
For example, Wannacry uses Bitcoin as the payment method for the decryption of files. Bitcoin uses virtual wallets, similar to a MAC address of a network interface card. MuirlandOracle explains the concept of MAC addresses in his Introductory: Networking room, these wallets have addresses who are unique.

I.e. The Bitcoin address used by the authors of Wannacry was 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94



In this case, the previously mentioned Bitcoin address used for Wannacry has to-date received over 20BTC (Bitcoins) from victims, which translates into over just over £158k (as of 06/04/2020).

You can use a website such as BlockCypher to explore the Bitcoin network and transactions between wallets.

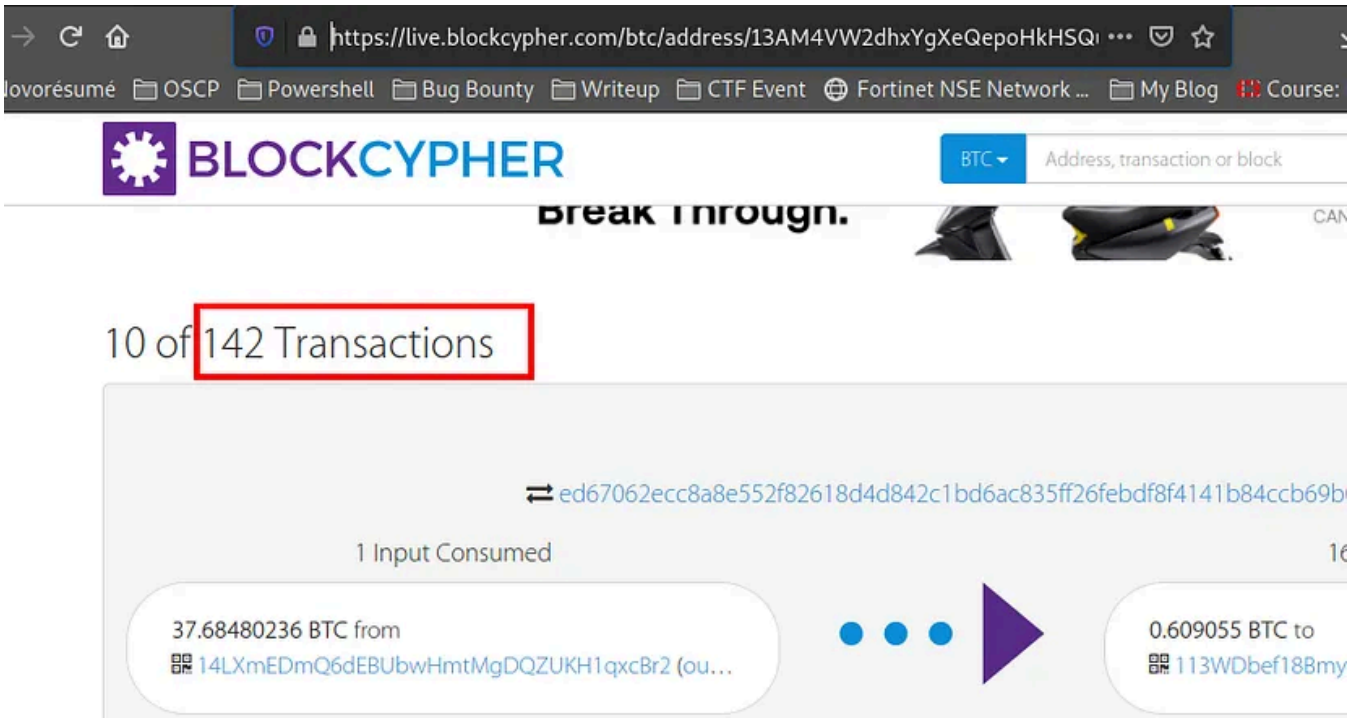


Practical

You need to perform a few prerequisites before you can complete this task, the steps are detailed below:

1. **Question 1.** List the number of total transactions that the Bitcoin wallet used by the “Wannacry” author(s)

Visit https://live.blockcypher.com/btc/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94/



Answer: 142

Question 2. What is the Bitcoin Address stored within “ComplexCalculator.exe”

1. Deploy the VM attached to this room and wait a couple of minutes for it to deploy. In the interim, ensure you are connected to TryHackMe via OpenVPN to RDP into the machine using the details below, or alternatively, control the instance in-browser at the top of the web page!
2. Open the “Sysinternals” folder located on the Desktop to proceed

To login to the instance via RDP:

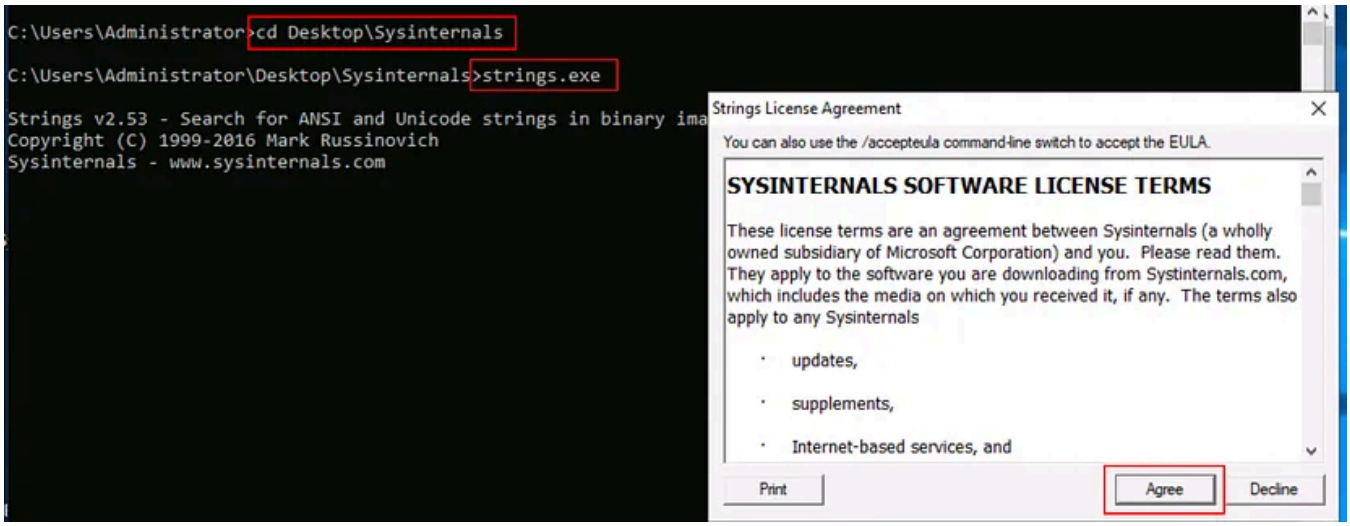
```
10.10.217.102
```

Username: analysis

Password: tryhackme

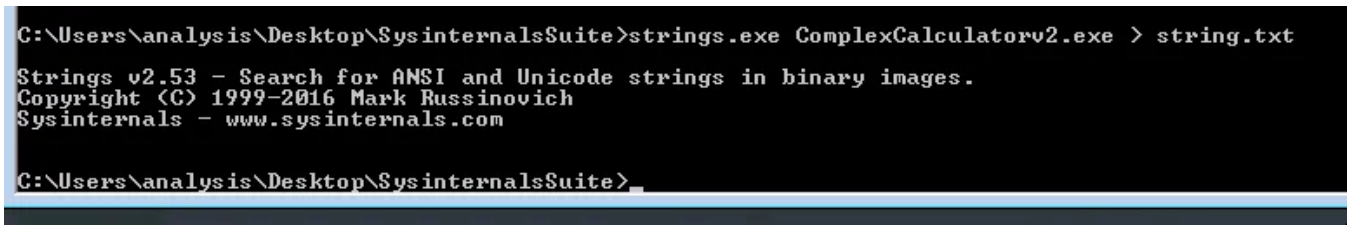
Domain: analysis-pc

Before using the “strings” tool provided with Sysinternals, we need to accept the license agreement first. You can do this by launching the executable through the command prompt and press “Agree” on the popup dialogue box.

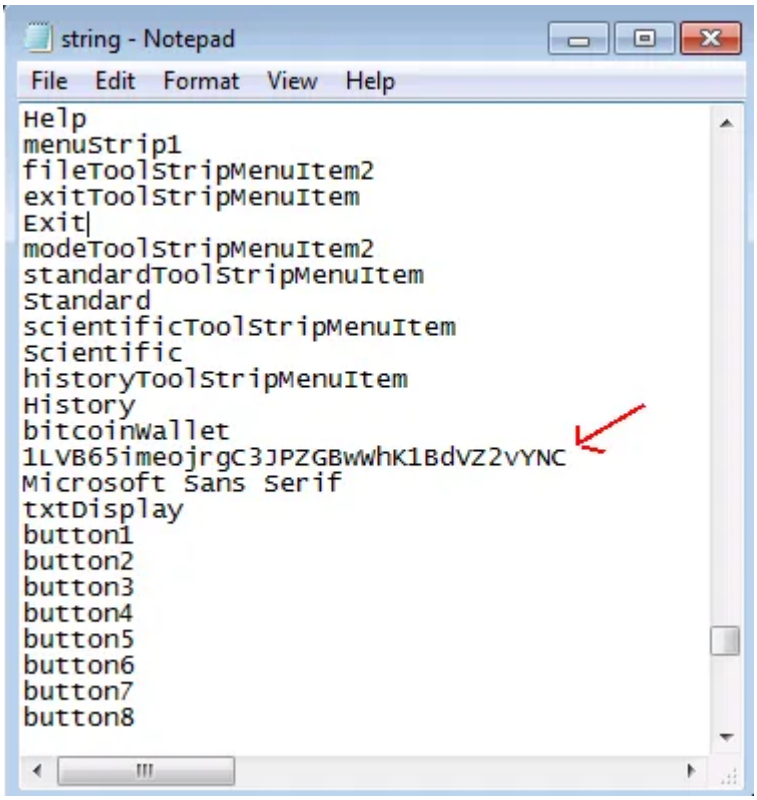


With this license accepted, we can now use this tool to extract the “strings” contained within the ComplexCalculatorv2.exe with the following syntax:

```
strings.exe ComplexCalculatorv2.exe > strings.txt
```



now open strings.txt in notepad



> *Answer: 1LVB65imeojrgC3JPZGBwWhK1BdVZ2vYNC*

Task 5. Summary

Question 1. What is the name of the toolset provided by Microsoft that allows you to extract the “strings” of an application?

> *Answer: Sysinternals*

Question 2. What operator would you use to “pipe” or store the output of the strings command?

> *Answer: >*

Question 3. What is the name of the currency that ransomware often uses for payment?

> *Answer: bitcoin*

You can find me on:
LinkedIn:- https://www.linkedin.com/in/shamsher-khan-651a35162/
Twitter:- https://twitter.com/shamsherkhannn
Tryhackme:- https://tryhackme.com/p/Shamsher

For more walkthroughs stay tuned…
Before you go…

Visit my other walkthrough's:-

and thank you for taking the time to read my walkthrough.
If you found it helpful, please hit the 👏 button 👏 (up to 40x) and share it to help others with similar interests! + Feedback is always welcome!

Reverse Engineering | Tryhackme | Tryhackme Walkthrough | Tryhackme Writeup | Oscp

Follow

Written by Shamsher khan

336 Followers · 5 Following

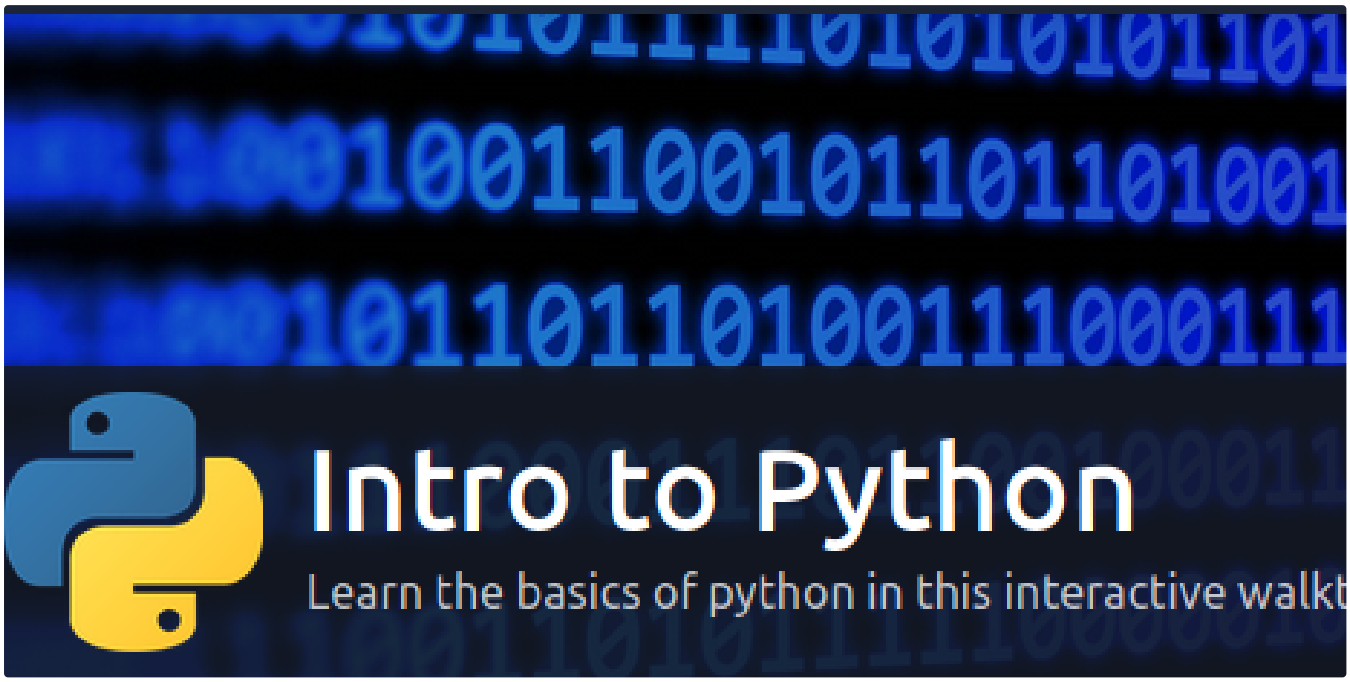
Web Application Pen-tester || CTF Player || Security Analyst || Freelance Cyber Security Trainer

No responses yet

What are your thoughts?

Respond

More from Shamsher khan



Shamsher khan

Intro to Python TryHackme

By Shamsher khna This is a Writeup of Tryhackme room “Intro to Python”

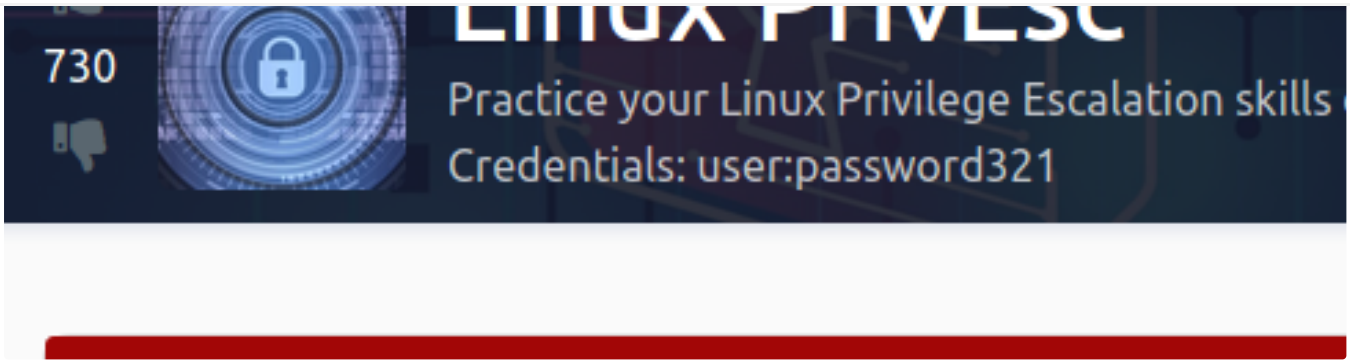
May 22, 2021 204 7

Shamsher khan

Linux Strength Training Tryhackme Writeup

By Shamsher khan This is a Writeup of Tryhackme room “Linux Strength Training”

May 8, 2021 15



In InfoSec Write-ups by Shamsher khan

Linux PrivEsc Tryhackme Writeup

By Shamsher khan This is a Writeup of Tryhackme room “JLinux PrivEsc”

Apr 20, 2021 105

Shamsher khan

Sysinternals Tryhackme Writeup

By Shamsher khna This is a Writeup of Tryhackme room “Sysinternals”

May 18, 2021 110

See all from Shamsher khan

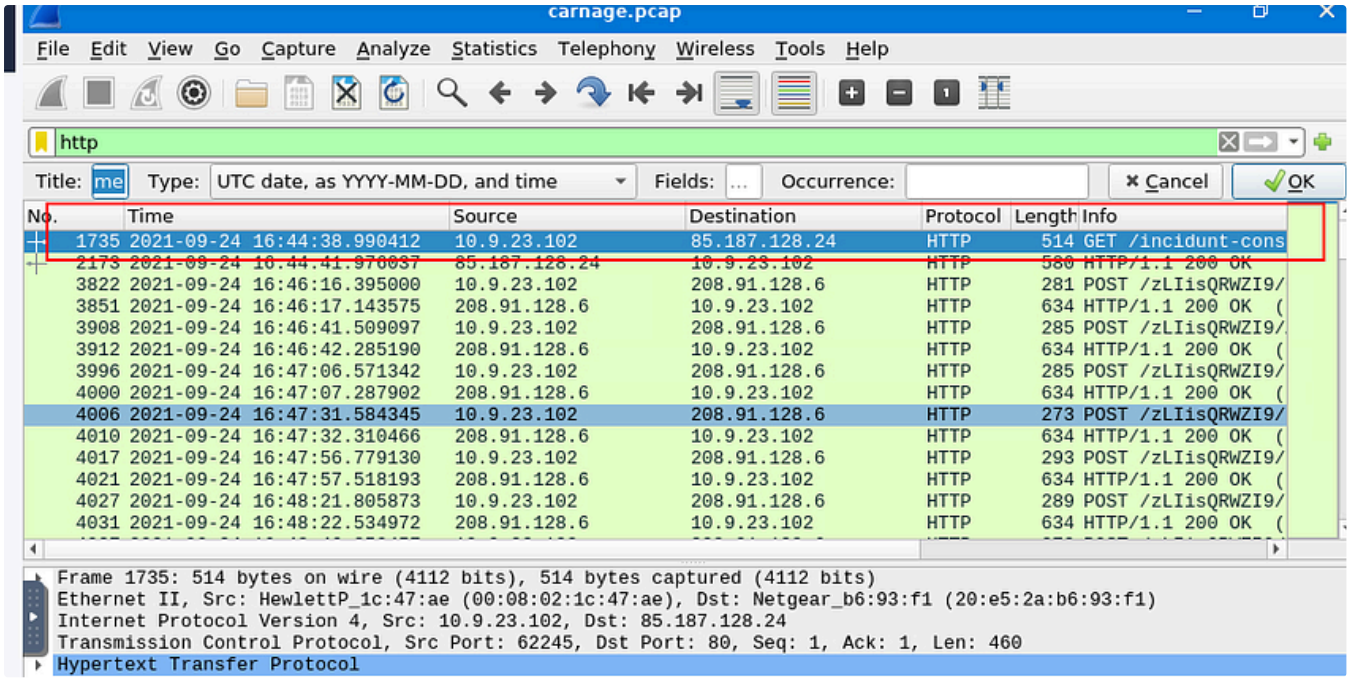
Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60



Chicken0248

[TryHackMe Write-up] Carnage

Apply your analytical skills to analyze the malicious network traffic using Wireshark.

Aug 17, 2024 50

Lists

Staff picks

796 stories · 1561 saves

Stories to Help You Level-Up at Work

19 stories · 912 saves

Self-Improvement 101

20 stories · 3192 saves

Productivity 101

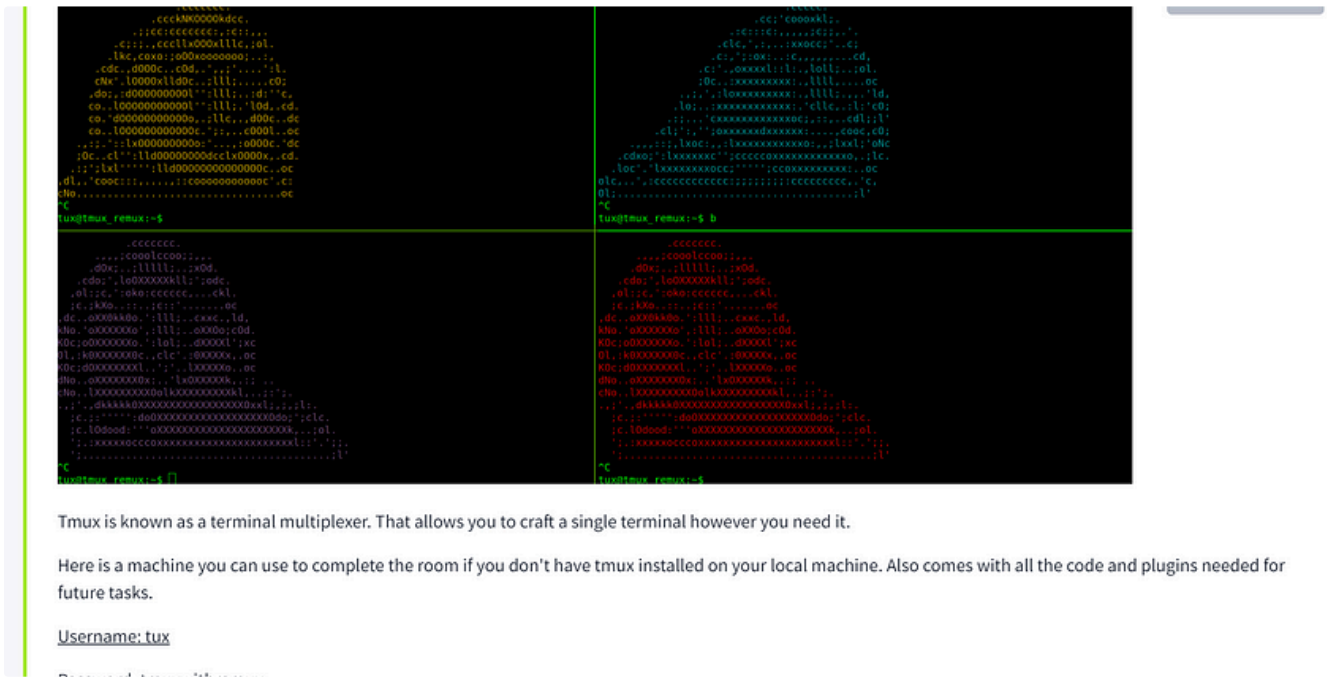
20 stories · 2706 saves

IritT

XSS—TryHackMe Walkthrough

Explore in-depth the different types of XSS and their root causes.

Sep 17, 2024



Tmux is known as a terminal multiplexer. That allows you to craft a single terminal however you need it.

Here is a machine you can use to complete the room if you don't have tmux installed on your local machine. Also comes with all the code and plugins needed for future tasks.

Username: tux

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: REmux The Tmux

Tryhackme Free Walk-through Room: REmux The Tmux

Nov 10, 2024 1

Rich

Advent of Cyber 2024

TL;DR Walkthrough of the first & current days of the 2024 Advent of Cyber, covering Google Fu, PowerShell, AD, a little Entra ID, and some...

Dec 17, 2024

K9ine95

Block ~ Tryhackme ~ walkthrough

One of your junior system administrators forgot to deactivate two accounts from a pair of recently fired employees. We believe these...

Aug 12, 2024 2

See more recommendations