

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# MAL: Strings TryHackMe Writeup



Ayush Bagde · [Follow](#)

8 min read · Mar 10, 2021

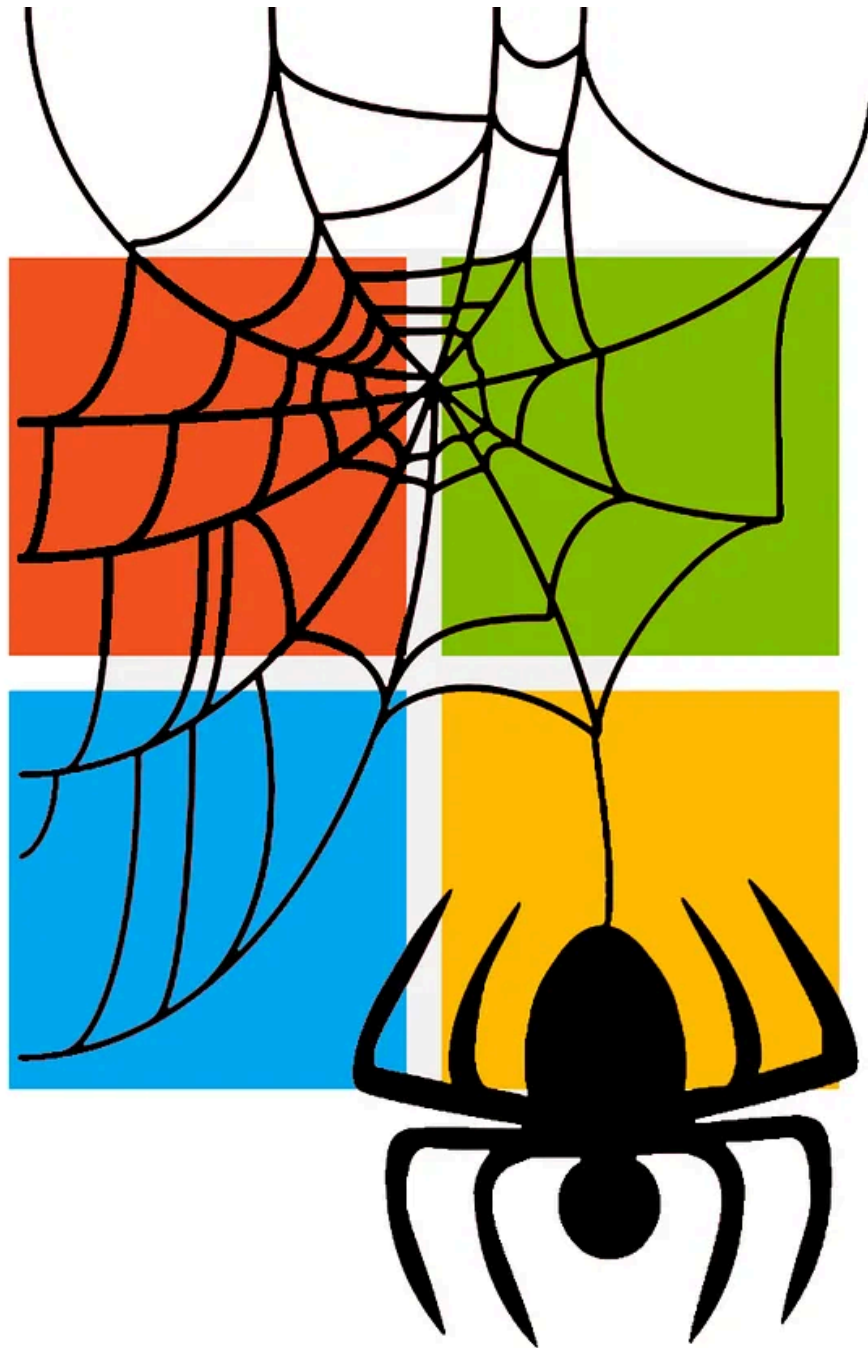


Listen



Share

... More



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

Hey Guys, Welcome back to another writeup. In This writeup we’ll learn about MAL: Strings machine which is VIP machine not available for free users. I’m Ayush bagde aka Override.

Here is the room Link: [MAL: Strings](#)

Let’s Start

### **TASK 1: What are “Strings”?**

You are here amongst the Malware series:

### **3. MP: Strings**

## 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”.

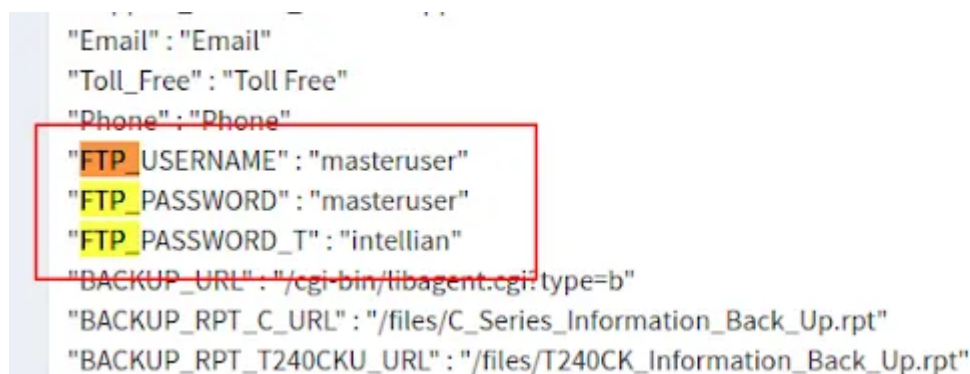
However “strings” can be stored within the application itself — where no input is necessary from the user. For example, using the example of usernames and passwords is a great representation of the many types of information that may be stored as a “string”.

## 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:



```
"Email" : "Email"
"Toll_Free" : "Toll Free"
"Phone" : "Phone"
"FTP_USERNAME" : "masteruser"
"FTP_PASSWORD" : "masteruser"
"FTP_PASSWORD_T" : "intellian"
"BACKUP_URL" : "/cgi-bin/libagent.cgi?type=b"
"BACKUP_RPT_C_URL" : "/files/C_Series_Information_Back_Up.rpt"
"BACKUP_RPT_T240CKU_URL" : "/files/T240CK_Information_Back_Up.rpt"
```

The screenshot shows a list of string resources in an Android application. A red rectangular box highlights three lines of code: `"FTP_USERNAME" : "masteruser"`, `"FTP_PASSWORD" : "masteruser"`, and `"FTP_PASSWORD_T" : "intellian"`. The word "FTP" in the first two lines is highlighted in orange, and "PASSWORD" in the second line is highlighted in yellow.

(Credit: [Ezequiel](#), [Skullarmy](#))

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

**#1 What is the name of the account that had the passcode of “12345678” in the intellian example discussed above?**

Answer: intellian

**#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

**#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 “string” From an Application

Download the material attached to the task.

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 one provided by

Open in app ↗

Medium

Search



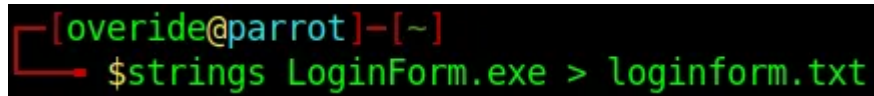
```
Welcome to the login portal.  
Enter your Username:
```

As displayed above, if you were to execute this on Windows you’d be greeted with a prompt asking for a Username and password. The problem is, we don’t know what the credentials are but we want to get in! Let’s have a look into how the application understands what usernames and passwords are right and wrong.

Load up a terminal and use the command `strings <filename>` replacing **<filename>** with the name and path of the downloaded file attached to this Task i.e. `strings /home/kali/Downloads/LoginForm.exe`

You will see a lot of text appear — and might be cut things out! Rather than just printing the output to the terminal, perhaps we should save it to a file? You can

“**pipe**” (or direct) the output to a file. If you are not familiar with Linux, I very highly recommend the following room: [Learning Linux](#)

A terminal window with a black background. The prompt is [override@parrot]-[~]. The command \$strings LoginForm.exe > loginform.txt is entered in green text. A red cursor is visible at the end of the command.

```
[override@parrot]-[~]  
$strings LoginForm.exe > loginform.txt
```

Now that we have stored the output into a file, we can do all sorts — filter it, sort it, search it! That’s what you’ll need to do. Open it in a text editor — either via terminal using `nano`, `vi` or Kali's installed GUI text editor `Mousepad`

```
[override@parrot]~$ cat loginform.txt
!This program cannot be run in DOS mode.
s_Rich
.text
`.rdata
@.data
.rsrc
@.reloc
h+.@
h\;@
h1-@
SVWP
Y_^[
hp-@
$SVW
@t=f
Y_^[
4SVW
HHuT
Y_^[
hX&@
h\1@
hP1@
hL1@
h@1@
Y_^[
Y_^[
h|1@
hD(@
>csm
h|)@
Y_^[
SVW3
ntel
5ineI
```

Looking through the file will show mostly garbage, but all you need is one golden nugget! You will be able to answer the following questions with this information. Think, what looks most likely a username and password?

**#1 What is the correct username required by the “LoginForm”?**

**Answer:** cmnatic

**#2 What is the required password to authenticate with?**

**Answer:** TryHackMeMerchWhen

### #3 What is the “hidden” THM flag?

Answer: THM{Not\_So\_Hidden\_Flag}

---

\* You will find answers under that file only. Just research on your own.

---

## TASK 3: Strings in the Context of Malware

Great, developers can be lazy — they leave passwords in applications as we have previously discussed. How does that relate to us as a malware analyst? Well...

We’ve discovered that even professional developers can “slip up” a few times, malware authors are still developers at the end of the day.

But more specifically, malware types such as botnets and ransomware rely upon information being stored within strings I.e. IP Addresses so that they are able to “call home” and connect to their “Command and Control” (C&C) server.

A famous example is the “Wannacry” ransomware. The “killswitch” was a domain that was discovered as a value contained within a string.

As we will later come on to discover, building a picture of the various stages a piece of malware proceeds through is essential to prevent further infection. Information such as who the software communicates to I.e. IP Addresses such as in the case of a botnet, or the payment address in the instances of ransomware is prevalent in building this picture.

### #1 What is the key term to describe a server that Botnets receive instructions from?

Answer: Command and Control

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

Answer: Wannacry

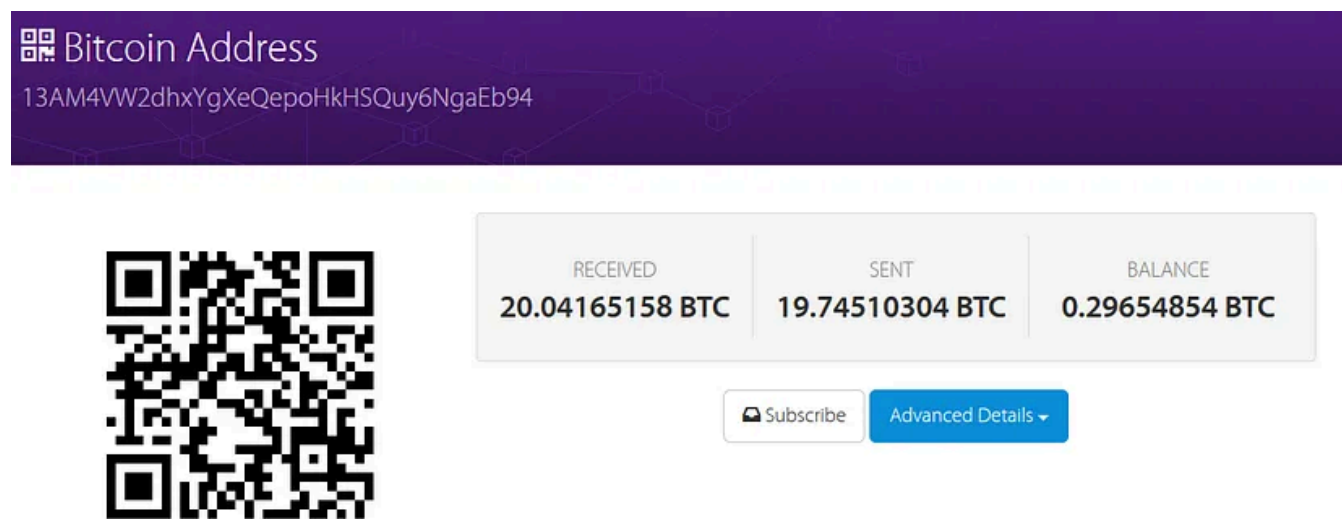
## TASK 4: Practical: Finding Bitcoin Addresses in Ransomware (Deploy!)

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



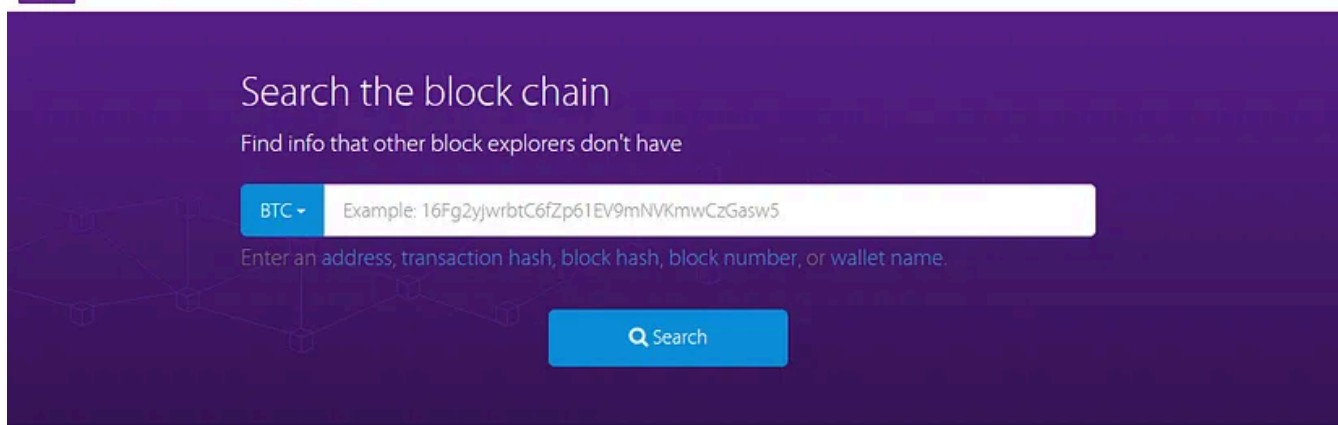
In this case, the previously mentioned Bitcoin address used for Wannacry has to-date received over 20BTC (Bitcoins) from victims, which translates into over just over £158k (as of 06/04/2020).

You can use a website such as [BlockCypher](#) to explore the Bitcoin network and transactions between wallets.





BLOCKCHAINS ▾



### Browse the Blockchain



Bitcoin



Grin



Litecoin



Dogecoin



Dash



BlockCypher Testnet

## Practical

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

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:

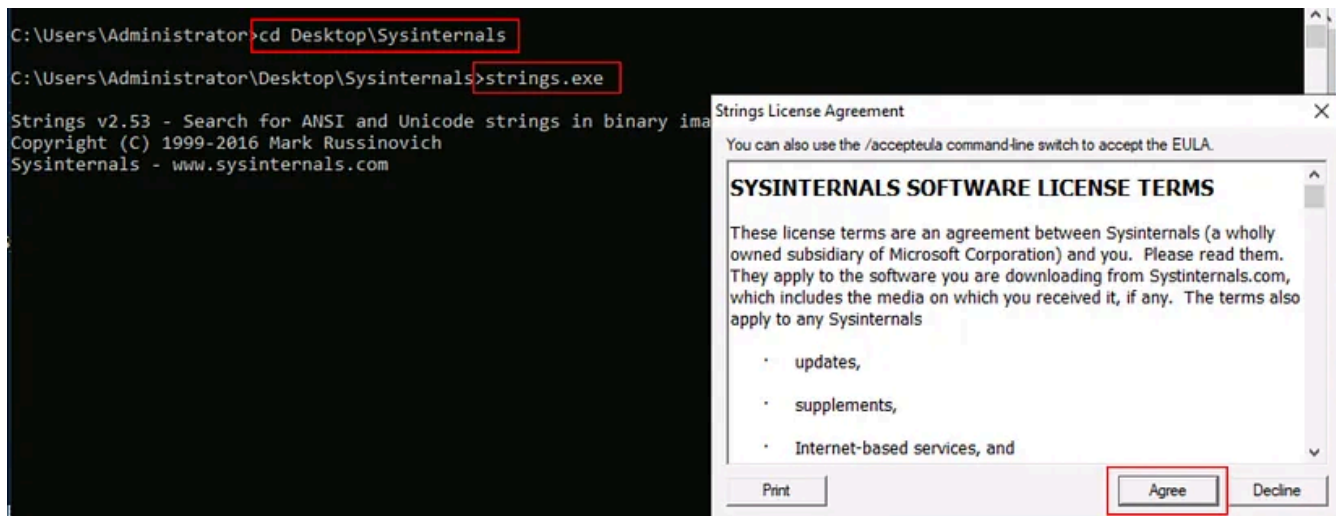
MACHINE\_IP

**Username:** analysis

**Password:** tryhackme

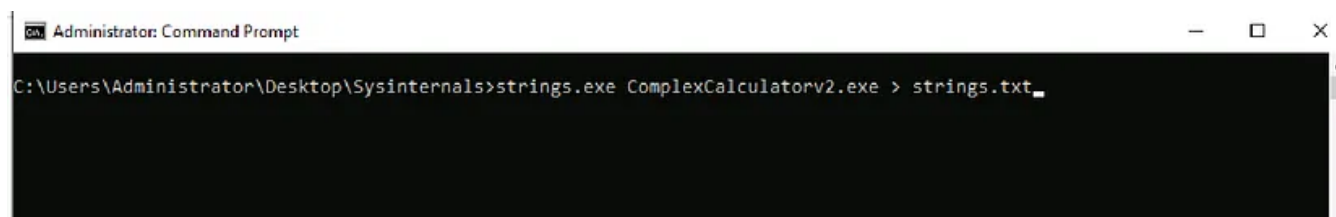
**Domain:** analysis-pc

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
```

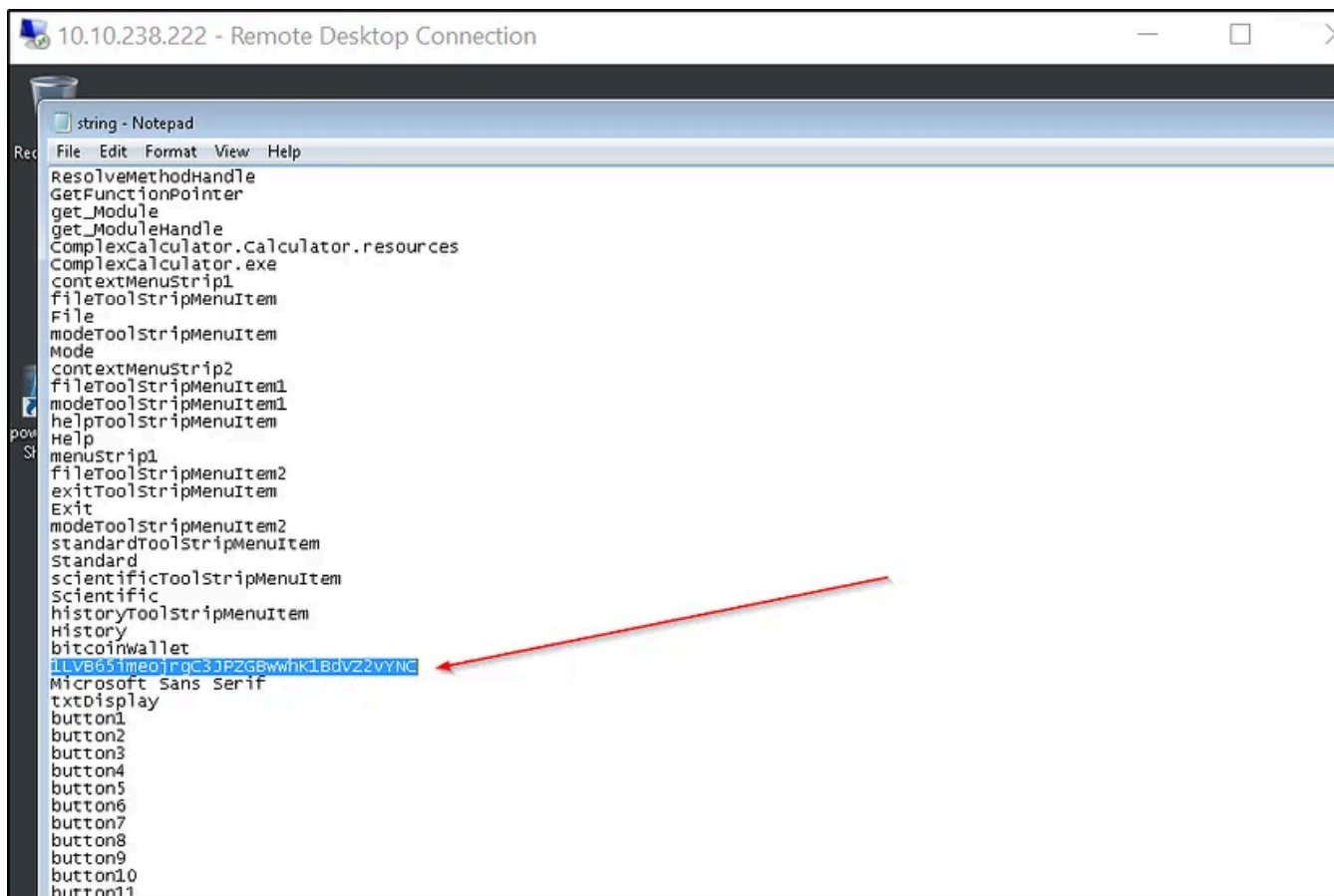


Now open up the text file created from the syntax we just entered with a text editor such as Notepad, where you will find the answer to solve Question #2.

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

Answer: 142

**#2 What is the Bitcoin Address stored within “ComplexCalculator.exe”?**



```
10.10.238.222 - Remote Desktop Connection

string - Notepad
File Edit Format View Help
ResolveMethodHandle
GetFunctionPointer
get_Module
get_ModuleHandle
ComplexCalculator.Calculator.resources
ComplexCalculator.exe
contextMenuStrip1
fileToolStripMenuItem
File
modeToolStripMenuItem
Mode
contextMenuStrip2
fileToolStripMenuItem1
modeToolStripMenuItem1
helpToolStripMenuItem
Help
menuStrip1
fileToolStripMenuItem2
exitToolStripMenuItem
Exit
modeToolStripMenuItem2
standardToolStripMenuItem
Standard
scientificToolStripMenuItem
Scientific
historyToolStripMenuItem
History
bitcoinwallet
1LVB65imeojrgC3JPZGBwWhK1BdVZ2vYNC
Microsoft Sans Serif
txtDisplay
button1
button2
button3
button4
button5
button6
button7
button8
button9
button10
button11
```

**Answer:** 1LVB65imeojrgC3JPZGBwWhK1BdVZ2vYNC

**\*Just see the outputed file.**

## Task 5: Summary

Let's Recap...

This room is somewhat arguably brief. However, we discussed the theory behind “strings” and why they are important for us as malware analysts. There isn’t all that much to the actual process of extracting “strings”, however, it is an important topic to discuss.

Moreover, hopefully after a bit of research, you now understand why “hard-coded” values such as credentials are a bad thing — and unfortunately still a re-occurring problem, least not an easy way to get into bug bounties!

We then extracted some of these “strings” from an example application that I made using Kali Linux’s strings command.

Whilst there isn’t a default command to extract “strings” within a program on Windows, there’s certainly a toolset that Microsoft provides that you can download!

Finally, we discussed how malware variants such as ransomware rely upon “strings” functionality i.e. “calling home” and/or bitcoin wallet addresses.

I hope you enjoyed the practical side and remember the tools available to you to extract these “strings” for use later on within the series!

~CMNatic

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

Answer: Sysinternals

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

Answer: >

**#3 What is the name of the currency that ransomware often uses for payment?**

Answer: Bitcoin

That’s all. Congratulations you learned something new today!

**Connect to me on:**

LinkedIn: <https://www.linkedin.com/in/ayush-bagde-49660219a/>

TryHackMe: <https://tryhackme.com/p/Override>

Discord: <https://discord.gg/5FzevEjqGj>

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!

Malware

Tryhackme

Writeup

Ctf

Cybersecurity



Follow

**Written by Ayush Bagde**

80 Followers · 3 Following

Associate | MTA Security Fundamentals | Junior Pentester | DLP | Brand Monitoring | Android Pentest |  
Seclore | Red Teaming

No responses yet




What are your thoughts?

Respond

More from Ayush Bagde

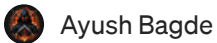


 Ayush Bagde

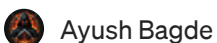
## MAL: REMnux-The Redux TryHackMe Writeup

A revitalised, hands-on showcase involving analysing malicious macro's, PDF's and Memory forensics of a victim of Jigsaw Ransomware; all...

W + ...



Learn how to use TShark to accelerate your pcap analysis!



A Charlie and The Chocolate Factory themed room, revisit Willy Wonka's chocolate factory!



Jan 18, 2021 🖱️ 105 💬 1



Ayush Bagde

## The Ultimate Ethical Hacking Roadmap: A Comprehensive Guide

Ethical hacking, also known as penetration testing or white-hat hacking, plays a crucial role in securing digital systems and networks. As...

Dec 3, 2023 🖱️ 54

[See all from Ayush Bagde](#)

### 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







In T3CH by Axoloth

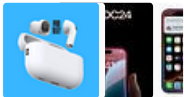
## TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

★ Nov 28, 2024 🖱 50

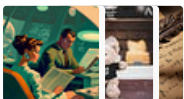


### Lists



#### Tech & Tools

22 stories · 380 saves



#### Medium's Huge List of Publications Accepting Submissions

377 stories · 4345 saves



#### Staff picks

796 stories · 1561 saves



#### Natural Language Processing

1884 stories · 1530 saves

Chicken0248

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

W+ ...

 Daniel Schwarzentraub

## Tryhackme Free Walk-through Room: REmux The Tmux





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



```
d
rd.img.old  lib64      media  opt    root  sbin  srv  tmp  var      vmlinuz.old
            lost+found mnt    proc  run   snap sys  usr    vmlinuz
var/log
log# ls
cloud-init-output.log  dpkg.log      kern.log      lxd      unattended-upgrades
cloud-init.log         fontconfig.log  landscape     syslog   wtmp
dist-upgrade          journal       lastlog      tallylog
log# cat auth.log | grep install
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log#
```



Dan Molina

## Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here:  
<https://tryhackme.com/room/disgruntled>

Oct 22, 2024



See more recommendations