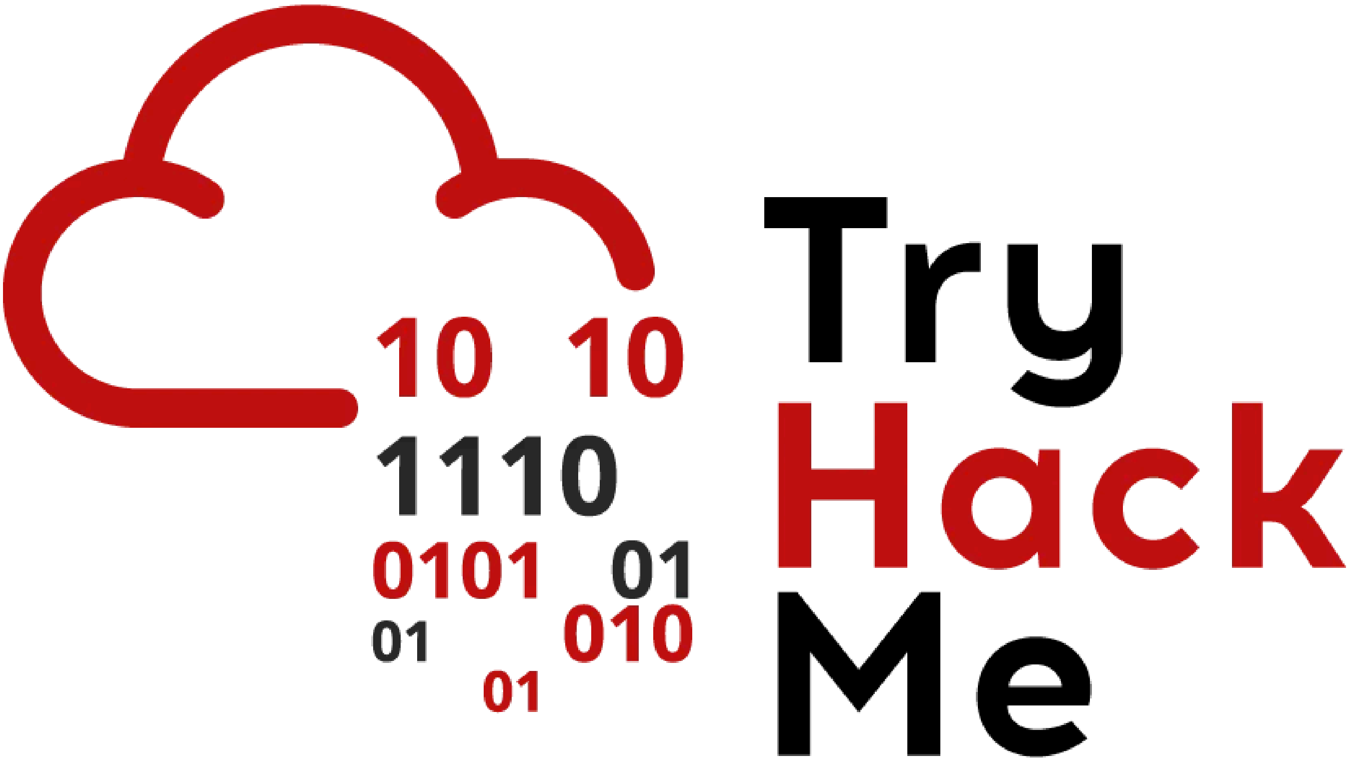
MAL: Strings TryHackMe Walkthrough

Rich · Follow

4 min read · Nov 20, 2023

Listen Share More



TL;DR Walkthrough of the TryHackMe MAL: Strings room, part of the Cyber Defense Pathway.

THM Walkthroughs:

A full list of our TryHackMe walkthroughs and cheatsheets is here.

Background

I have said it before, but maybe not on here, I found along the way of posting these that I actually enjoy technical writing. I like getting into the home lab, TryHackMe, a CTF, Slayer Labs, really anything hands on, finding the solution, and writing up how to do it.

I hate theory. I truly hate writing about theory. That was always a struggle for me back when we were working on a Bachelors degree and continues to this day. Maybe eventually I'll get over it, but I doubt it.

We ran through this room and banged out this writeup while taking another break from writing about theory for college.

But enough about that, let's get to the answers and how to find them :)

On an admin note, the sources to find the answers to the questions involving research are in the references at the end.

— — Task 1 — -

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

intellian

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

CVE-2019–6499

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

One

— — Task 2 — -

What is the correct username required by the "LoginForm"?

We know that the username is 7 characters thanks to THM's *s in the answer box, so:

```
strings LoginForm.exe | grep -E ‘^.{7}$’
```

cmnatic

What is the required password to authenticate with?

The password is 18 characters, so:

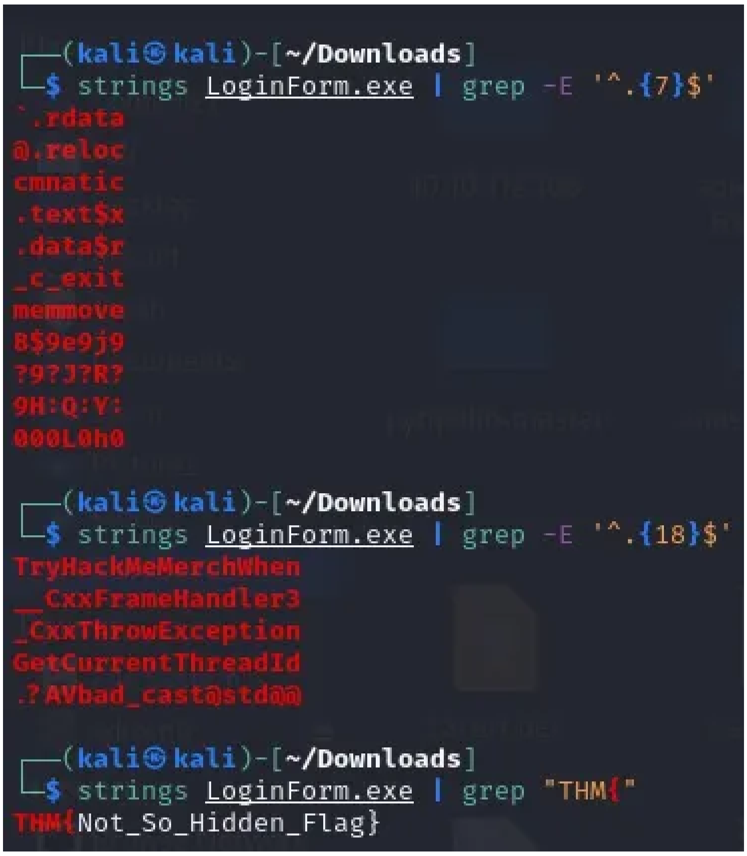
```
strings LoginForm.exe | grep -E ‘^.{18}$’
```

TryHackMeMerchWhen

What is the “hidden” THM{} flag?

```
strings LoginForm.exe | grep -E ‘THM{‘
```

THM{Not_So_Hidden_Flag}



```
┌──(kali㉿kali)-[~/Downloads]
└─$ strings LoginForm.exe | grep -E '^.{7}$'
`.rdata
@.reloc
cmnatic
.text$x
.data$r
_c_exit
memmove
8$9e9j9
?9?J?R?
9H:Q:Y:
000L0h0

┌──(kali㉿kali)-[~/Downloads]
└─$ strings LoginForm.exe | grep -E '^.{18}$'
TryHackMeMerchWhen
__CxxFrameHandler3
_CxxThrowException
GetCurrentThreadId
.?AVbad_cast@std@@

┌──(kali㉿kali)-[~/Downloads]
└─$ strings LoginForm.exe | grep "THM{"
THM{Not_So_Hidden_Flag}
```

— — Task 3 — -

We knew these already, but the answers are in THM's explanation.

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

Command and Control

Name the discussed example malware that uses "strings" to store the bitcoin wallet addresses for payment

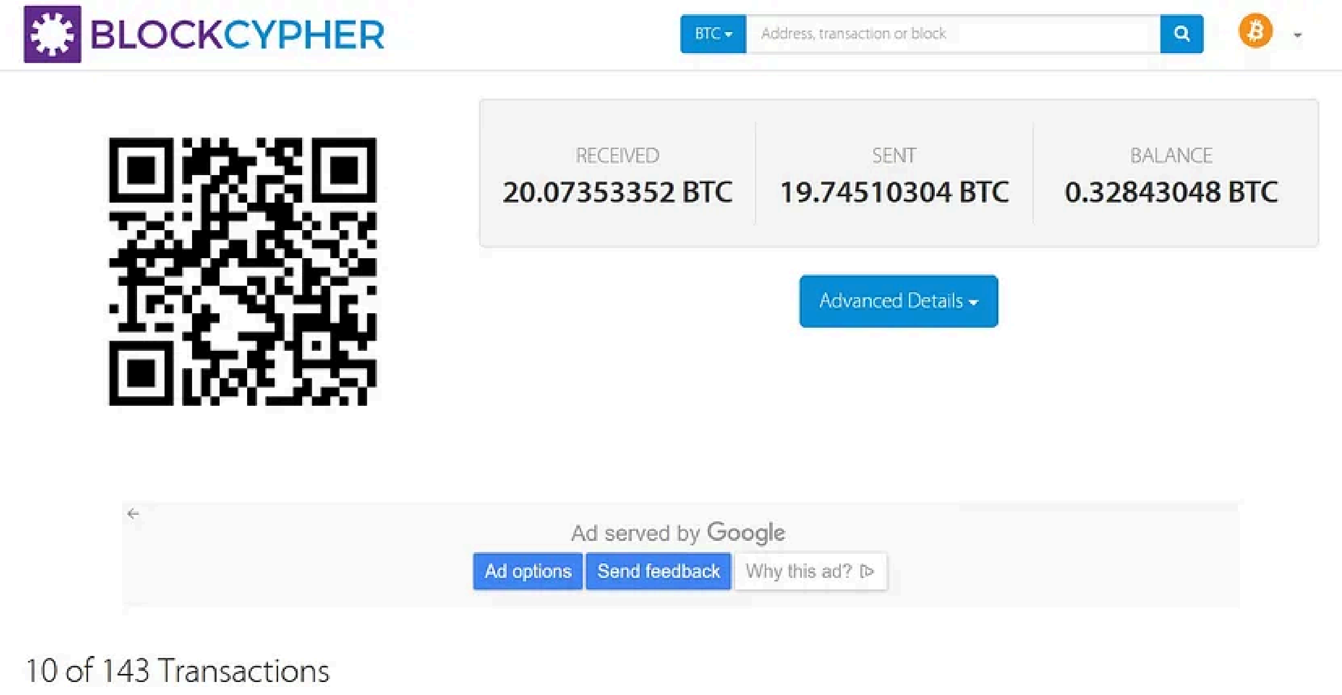
Wannacry

— — Task 4 — -

List the number of total transactions that the Bitcoin wallet used by the "Wannacry" author(s)

Just follow THM's link to the given Bitcoin address "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94".

143



RECEIVED	SENT	BALANCE
20.07353352 BTC	19.74510304 BTC	0.32843048 BTC

10 of 143 Transactions

What is the Bitcoin Address stored within "ComplexCalculator.exe"

This just takes a little cleverness to find very quickly.

```
xfreerdp /v:10.10.193.120 /u:Administrator /p:tryhackme123! /dynamic-resolutior
```

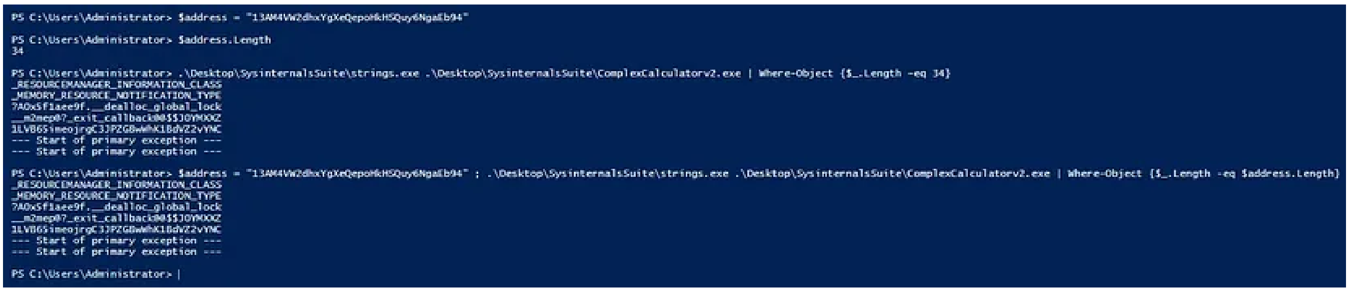
```
PowerShell.exe

.\Desktop\SysinternalsSuite\strings.exe
```

```
$address = "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"

$address.Length

.\Desktop\SysinternalsSuite\strings.exe .\Desktop\SysinternalsSuite\ComplexCalc
```

Or simply:

```
$address = “13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94” ; .\Desktop\SysinternalsSuite\s
```

1LVB65imeojrgC3JPZGBwWhK1BdVZ2vYNC



```
PS C:\Users\Administrator> $address = "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"

PS C:\Users\Administrator> $address.Length
34

PS C:\Users\Administrator> .\Desktop\SysinternalsSuite\strings.exe .\Desktop\SysinternalsSuite\ComplexCalculatorv2.exe | Where-Object {$_.Length -eq 34}
_RESOURCEMANAGER_INFORMATION_CLASS
_MEMORY_RESOURCE_NOTIFICATION_TYPE
?A0xSf1aee9f.__dealloc_global_lock
__m2mep@?_exit_callback@@$$J0YMXXZ
1LVB65imeojrgC3JPZGBwWhK1BdVZ2vYNC
--- Start of primary exception ---
--- Start of primary exception ---

PS C:\Users\Administrator> $address = "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94" ; .\Desktop\SysinternalsSuite\strings.exe .\Desktop\SysinternalsSuite\ComplexCalculatorv2.exe | Where-Object {$_.Length -eq $address.Length}
_RESOURCEMANAGER_INFORMATION_CLASS
_MEMORY_RESOURCE_NOTIFICATION_TYPE
?A0xSf1aee9f.__dealloc_global_lock
__m2mep@?_exit_callback@@$$J0YMXXZ
1LVB65imeojrgC3JPZGBwWhK1BdVZ2vYNC
--- Start of primary exception ---
--- Start of primary exception ---

PS C:\Users\Administrator> |
```

— — Task 5 — -

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

Sysinterals

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

Ok, I hate the verbiage of this question. In PowerShell you pipe with ‘ | ‘ and you “store the output” with ‘ > ‘ or ‘ >> ‘ if you want to append rather than overwrite. Of course ‘ >> ‘ is really just an alias for ‘ | Out-File .\Something.txt -Append ‘ and ‘ > ‘ is an alias for the same, but without the ‘ -Append ‘.

Hence I put | since I’d pipe to Out-File or Export-Csv, only for THM To immediately tell me I was wrong. The answer they are looking for is:

>

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

Bitcoin

Summary

This was another good little, fun, educational room. I should probably get back to my root canal now, errr, I mean college paper.

References

CVE-2020–8000 Details: https://nvd.nist.gov/vuln/detail/CVE-2020-8000

CVE-2019–6499 Details: https://nvd.nist.gov/vuln/detail/CVE-2019-6499

OWASP Top 10 IoT: https://owasp.org/www-chapter-toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introduction-and-Root-Causes.pdf

Details RE a specific Bitcoin wallet: https://live.blockcypher.com/btc/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94/

grep a specific # of characters: https://www.baeldung.com/linux/match-string-by-length

PowerShell find strings with specific length: https://shellgeek.com/string-length-of-variable-in-powershell/

Tryhackme Tryhackme Walkthrough Tryhackme Writeup Cybersecurity

Cyber Security Awareness

Follow

Written by Rich

285 Followers · 10 Following

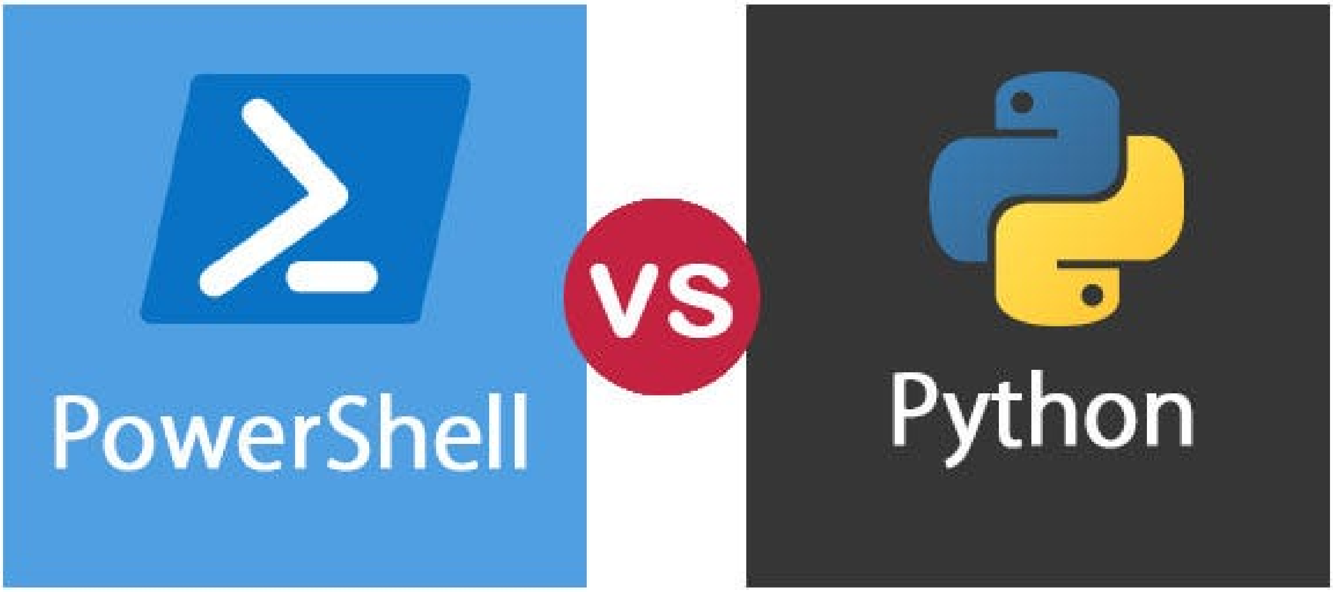
I work various IT jobs & like Windows domain security as a hobby. Most of what's here is my notes from auditing or the lab.

No responses yet

What are your thoughts?

Respond

More from Rich

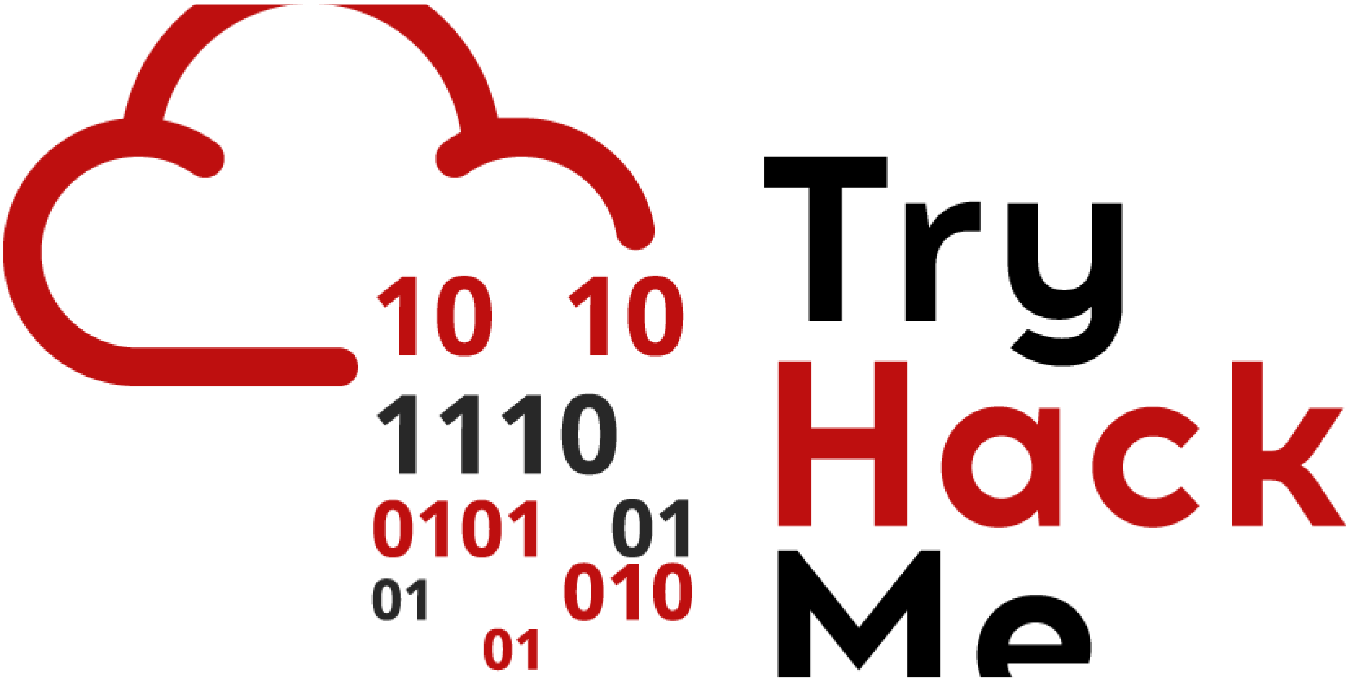


Rich

Python Basics TryHackMe Walkthrough

TL;DR Walkthrough of the Python Basics room, part of the Pentest+ Pathway.

Jan 22, 2024 24



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

Rich

Tempest TryHackMe Walkthrough

TL;DR walkthrough of the TryHackMe Tempest room.

Jun 14, 2024 52 1

Rich

Mimikatz Cheatsheet

TL;DR Mimikatz cheatsheet of things I have found useful in CRTP and the lab.

Aug 26, 2022 21

See all from Rich

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

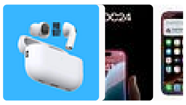
Rich

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...

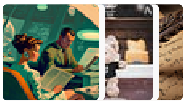
Dec 17, 2024

Lists



Tech & Tools

22 stories · 380 saves

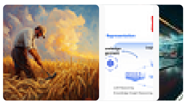


Medium's Huge List of Publications Accepting Submissions

377 stories · 4345 saves

Staff picks

796 stories · 1561 saves



Natural Language Processing

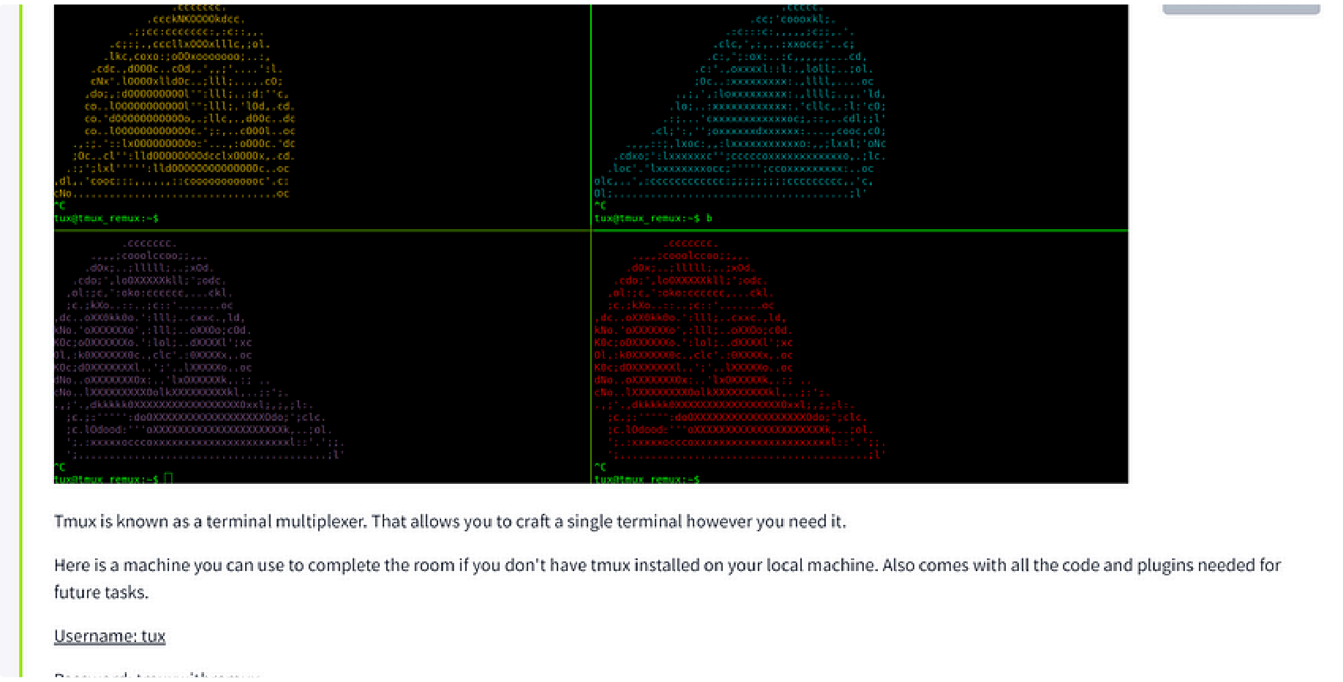
1884 stories · 1530 saves

IritT

TryHackMe MITRE Walkthrough

This room will discuss the various resources MITRE has made available for the cybersecurity community.

Aug 23, 2024



```
^C
tux@tmux_remux:~$
```

```
^C
tux@tmux_remux:~$ b
```

```
^C
tux@tmux_remux:~$
```

```
^C
tux@tmux_remux:~$
```

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.

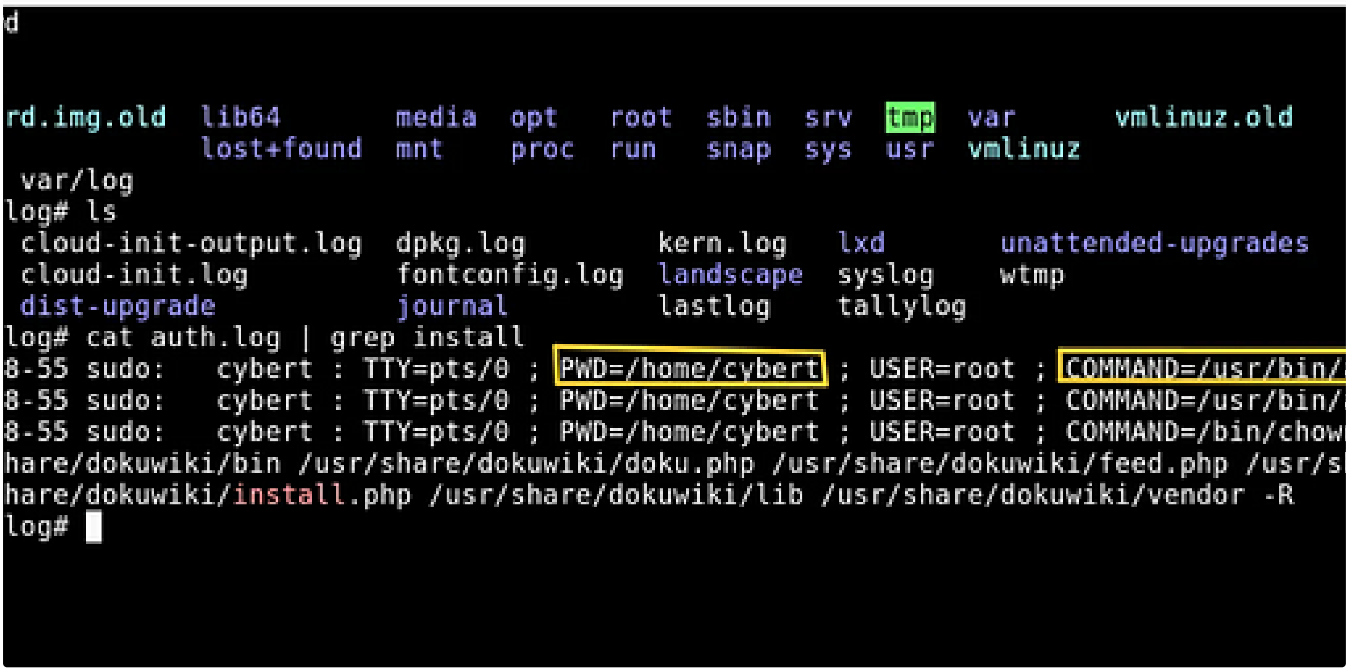
Username: tux

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: REmux The Tmux

Tryhackme Free Walk-through Room: REmux The Tmux

Nov 10, 2024 1



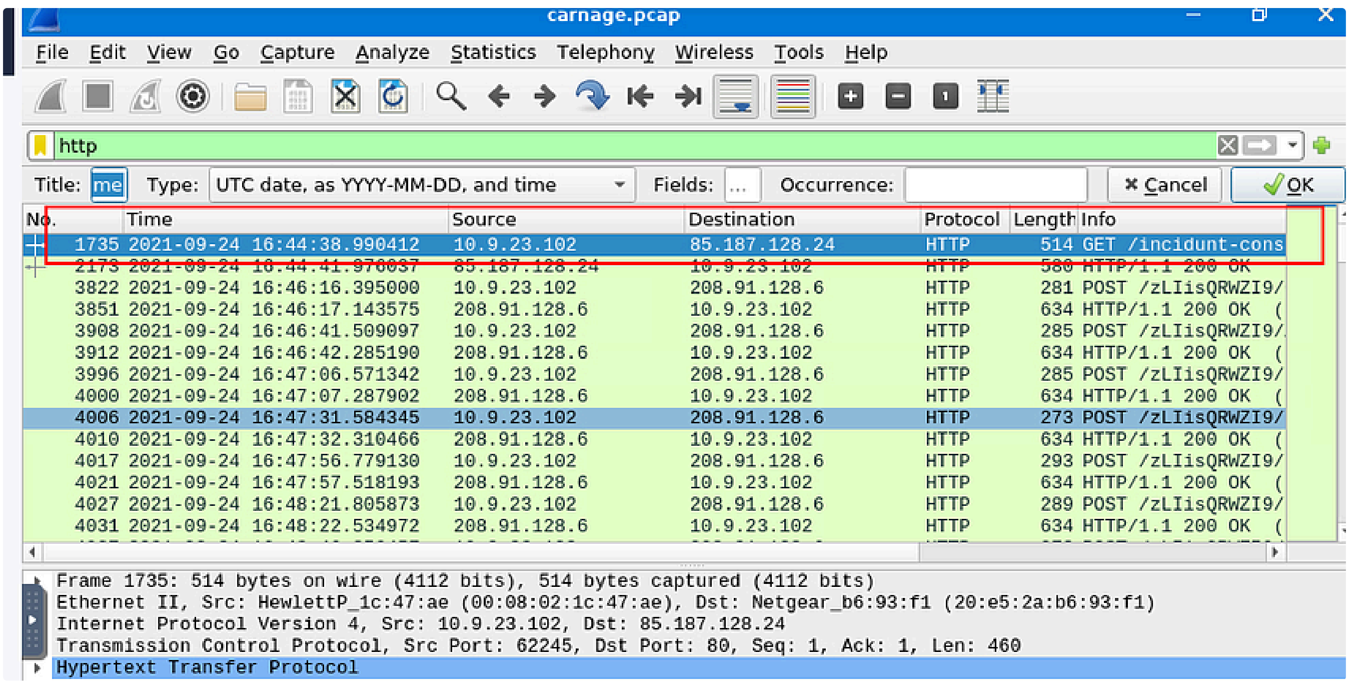
```
d

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


carnage.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
✖ Cancel
✓ OK

http

Title: me Type: UTC date, as YYYY-MM-DD, and time Fields: ... Occurrence:

```
No.  Time                        Source         Destination    Protocol Length Info
1735 2021-09-24 16:44:38.990412 10.9.23.102    85.187.128.24  HTTP     514 GET /incidunt-cons
2173 2021-09-24 16:44:41.976037 85.187.128.24  10.9.23.102    HTTP     580 HTTP/1.1 200 OK
3822 2021-09-24 16:46:16.395000 10.9.23.102    208.91.128.6   HTTP     281 POST /zLIisQRWZI9/
3851 2021-09-24 16:46:17.143575 208.91.128.6   10.9.23.102    HTTP     634 HTTP/1.1 200 OK  (
3908 2021-09-24 16:46:41.509097 10.9.23.102    208.91.128.6   HTTP     285 POST /zLIisQRWZI9/
3912 2021-09-24 16:46:42.285190 208.91.128.6   10.9.23.102    HTTP     634 HTTP/1.1 200 OK  (
3996 2021-09-24 16:47:06.571342 10.9.23.102    208.91.128.6   HTTP     285 POST /zLIisQRWZI9/
4000 2021-09-24 16:47:07.287902 208.91.128.6   10.9.23.102    HTTP     634 HTTP/1.1 200 OK  (
4006 2021-09-24 16:47:31.584345 10.9.23.102    208.91.128.6   HTTP     273 POST /zLIisQRWZI9/
4010 2021-09-24 16:47:32.310466 208.91.128.6   10.9.23.102    HTTP     634 HTTP/1.1 200 OK  (
4017 2021-09-24 16:47:56.779130 10.9.23.102    208.91.128.6   HTTP     293 POST /zLIisQRWZI9/
4021 2021-09-24 16:47:57.518193 208.91.128.6   10.9.23.102    HTTP     634 HTTP/1.1 200 OK  (
4027 2021-09-24 16:48:21.805873 10.9.23.102    208.91.128.6   HTTP     289 POST /zLIisQRWZI9/
4031 2021-09-24 16:48:22.534972 208.91.128.6   10.9.23.102    HTTP     634 HTTP/1.1 200 OK  (
```

```
Frame 1735: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 85.187.128.24
Transmission Control Protocol, Src Port: 62245, Dst Port: 80, Seq: 1, Ack: 1, Len: 460
Hypertext Transfer Protocol
```

Chicken0248

[TryHackMe Write-up] Carnage

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

Aug 17, 2024 50

See more recommendations