

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



MAL: Malware Introductory TryHackMe Walkthrough



Rich · [Follow](#)

4 min read · Nov 19, 2023

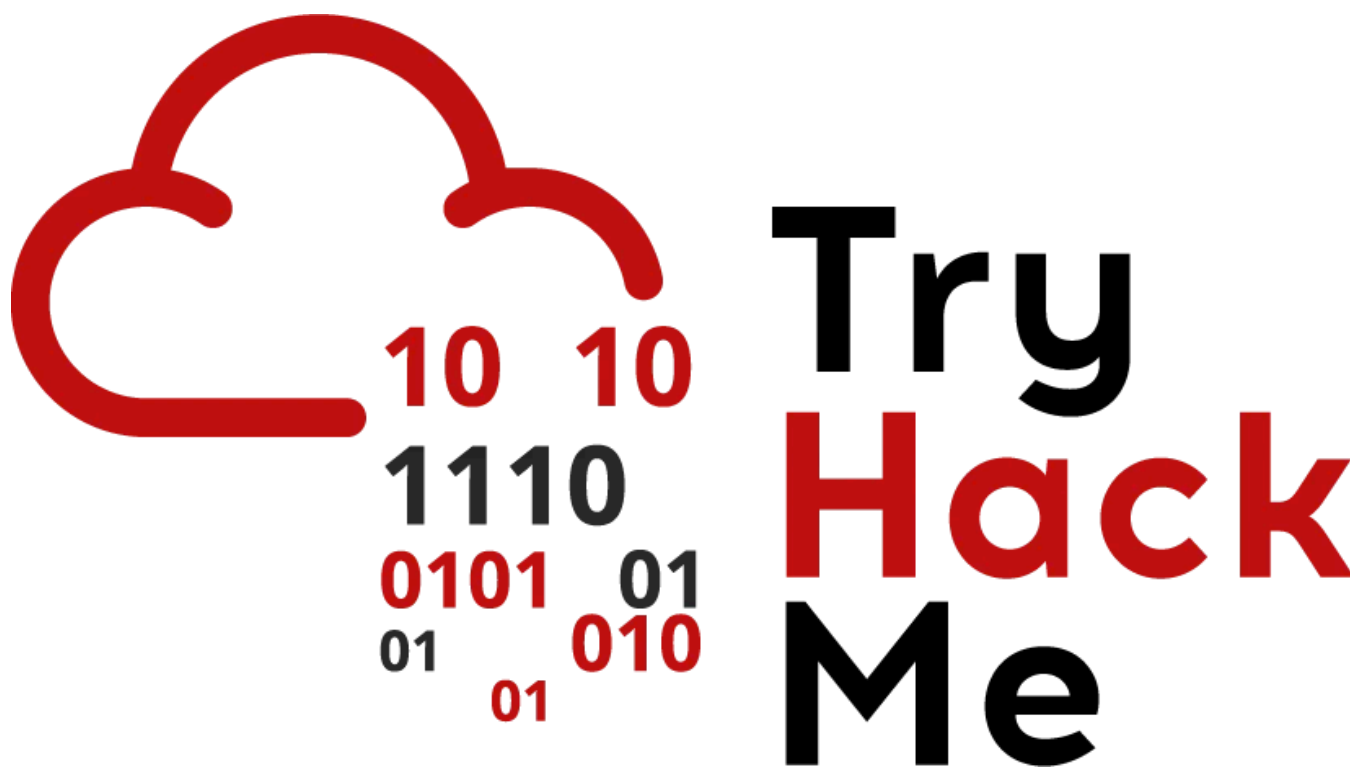


Listen



Share

... More



TL;DR Walkthrough of the [TryHackMe MAL: Malware Introductory room](#), part of the Cyber Defense Pathway.

THM Walkthroughs:

A full list of our TryHackMe walkthroughs and cheatsheets is [here](#).

Background

I saw a couple other writeups on Google, but most of them only had the questions & answers without explaining how to find the information. Hence I decided I'd bother writing up what we did.

The first few tasks just involve some reading and or Googling. The last few tasks are hands on. If I skip a Task here it's because all you have to do is hit a button, there's no answer needed.

On an admin note, I have been having issues with TryHackMe's US VPN servers lately. OpenVPN would connect, then immediately show an error code. TryHackMe's website would show me as connected but I couldn't even ping THM's VM. As a result I have been using their EU servers. One can do this simply by downloading the *.ovpn files from [here](#). I downloaded the ones for my account into a folder on Kali and simply saved them with filenames denoting the geographical location.

So without further ado let's get into it.

— — Task 2 — -

What is the famous example of a targeted attack-esque Malware that targeted Iran?

Stuxnet

What is the name of the Ransomware that used the Eternalblue exploit in a "Mass Campaign" attack?

Wannacry

— — Task 3 — -

Name the first essential step of a Malware Attack?

Delivery

Now name the second essential step of a Malware Attack?

Execution

What type of signature is used to classify remnants of infection on a host?

Host-Based Signatures

What is the name of the other classification of signature used after a Malware attack?

Network-Based Signatures

— — Task 7 — —

As always start by connecting with xfreerdp.

```
xfreerdp /v:10.10.244.56 /u:analysis /p:Tryhackme123! /dynamic-resolution
```

```
Set-Location 'C:\users\Analysis\Desktop\Tasks\Task 7'  
Get-ChildItem  
Get-FileHash .\* -Algorithm MD5
```

```
PS C:\Users\Analysis> Set-Location 'C:\users\Analysis\Desktop\Tasks\Task 7'  
PS C:\users\Analysis\Desktop\Tasks\Task 7> Get-ChildItem  
  
Directory: C:\users\Analysis\Desktop\Tasks\Task 7  
  
Mode                LastWriteTime         Length Name  
----                -  
-a-----         13/02/2020    22:37           74752 aws.exe  
-a-----         13/02/2020    22:37           50176 NetLogo.exe  
-a-----         13/02/2020    22:37          985800 vlc.exe  
  
PS C:\users\Analysis\Desktop\Tasks\Task 7> Get-FileHash .\* -Algorithm MD5  
  
Algorithm      Hash                                     Path  
-----  
MD5            D2778164EF643BA8F44CC202EC7EF157      C:\users\Analysis\Desktop\Tasks\Task 7\aws.exe  
MD5            59CB421172A89E1E16C11A428326952C      C:\users\Analysis\Desktop\Tasks\Task 7\NetLogo.exe  
MD5            5416BE1B8B04B1681CB39CF0E2CAAD9F      C:\users\Analysis\Desktop\Tasks\Task 7\vlc.exe  
  
PS C:\users\Analysis\Desktop\Tasks\Task 7>
```

The MD5 Checksum of aws.exe

D2778164EF643BA8F44CC202EC7EF157

The MD5 Checksum of Netlogo.exe

59CB421172A89E1E16C11A428326952C

The MD5 Checksum of vlc.exe

5416BE1B8B04B1681CB39CF0E2CAAD9F

Task 8 is all 'Nay'. Just copy/paste the hashes into VirusTotal.

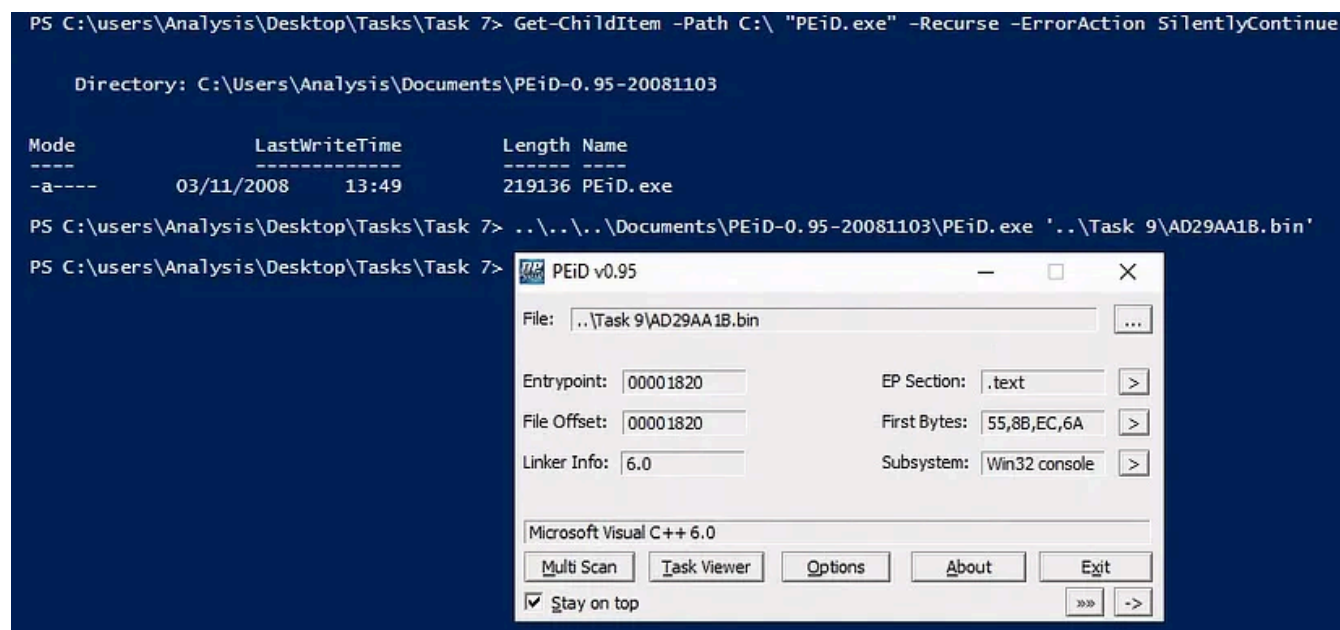
— — Task 9 — —

What does PeiD propose 1DE9176AD682FF.dll being packed with?

What does PeiD propose AD29AA1B.bin being packed with?

I had to search for PeiD as THM didn't mention where it was saved.

```
Get-ChildItem -Path C:\ "PEiD.exe" -Recurse -ErrorAction SilentlyContinue  
  
..\..\..\Documents\PEiD-0.95-20081103\PEiD.exe '..\Task 9\AD29AA1B.bin'
```



We got Microsoft Visual C++ 6.0 DLL for both.

— — Task 10 — —

What packer does PeiD report file "6F431F46547DB2628" to be packed with?

```
..\..\..\Documents\PEiD-0.95-20081103\PEiD.exe '..\Task 10\6F431F46547DB2628'
```

FSG 1.0 -> dulek/xt

— — Task 12 — -

What is the URL that is outputted after using “strings”

Strings.exe refused to run properly in PowreShell_ISE, so I had to use PowerShell.exe for this question. I was not amused. I have gotten quite used to command completion, suggestions for command options that I can just Tab to complete, any syntax errors of mine getting underlined in red, etc etc.

```
PowerShell.exe
```

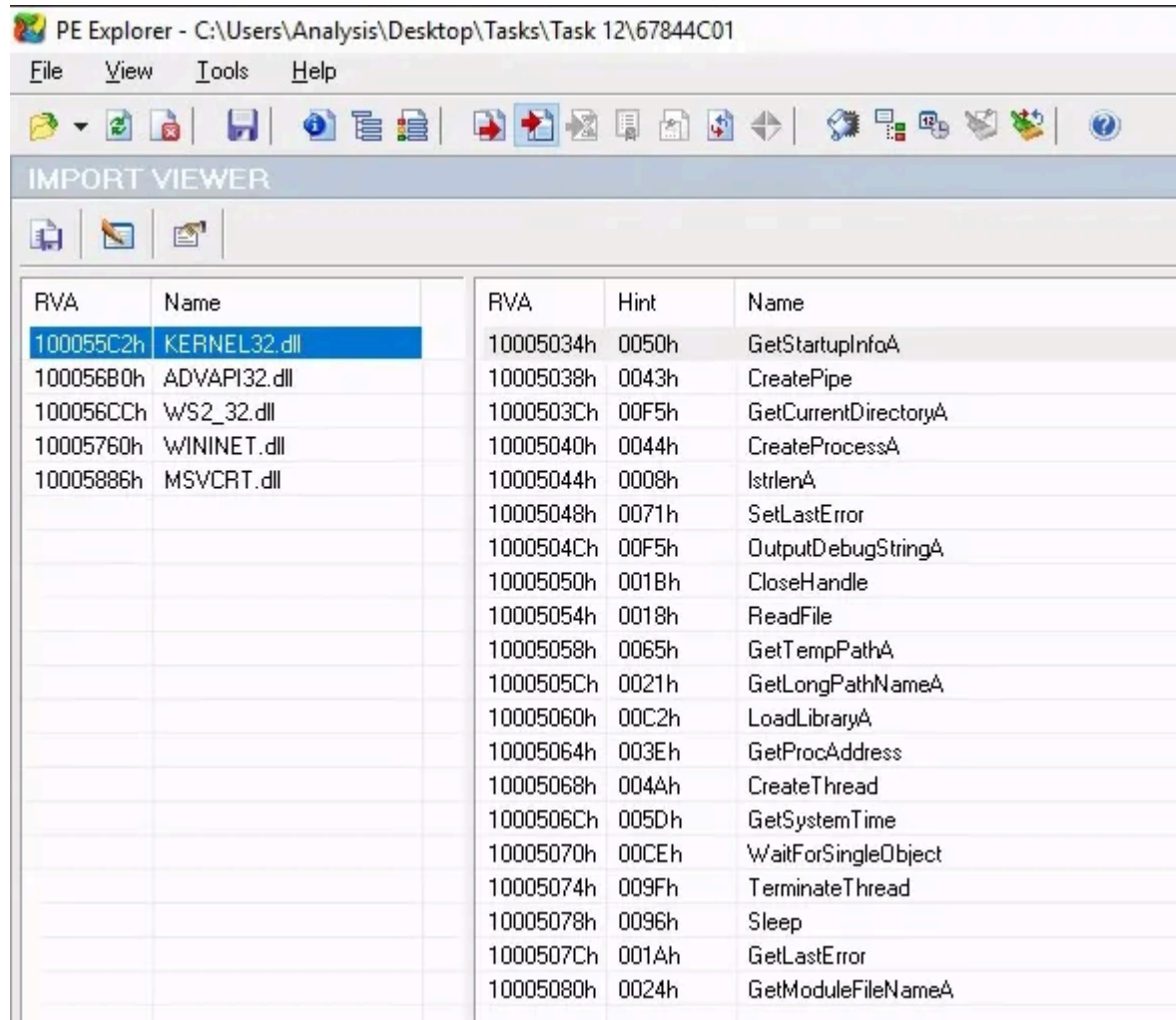
```
C:\Users\\Analysis\Desktop\Tools\SysinternalsSuite\strings.exe "C:\Users\Analysis
```

practicalmalwareanalysis.com

How many unique “Imports” are there?

Have to use the GUI PE Explorer to open the file -> View -> Imports

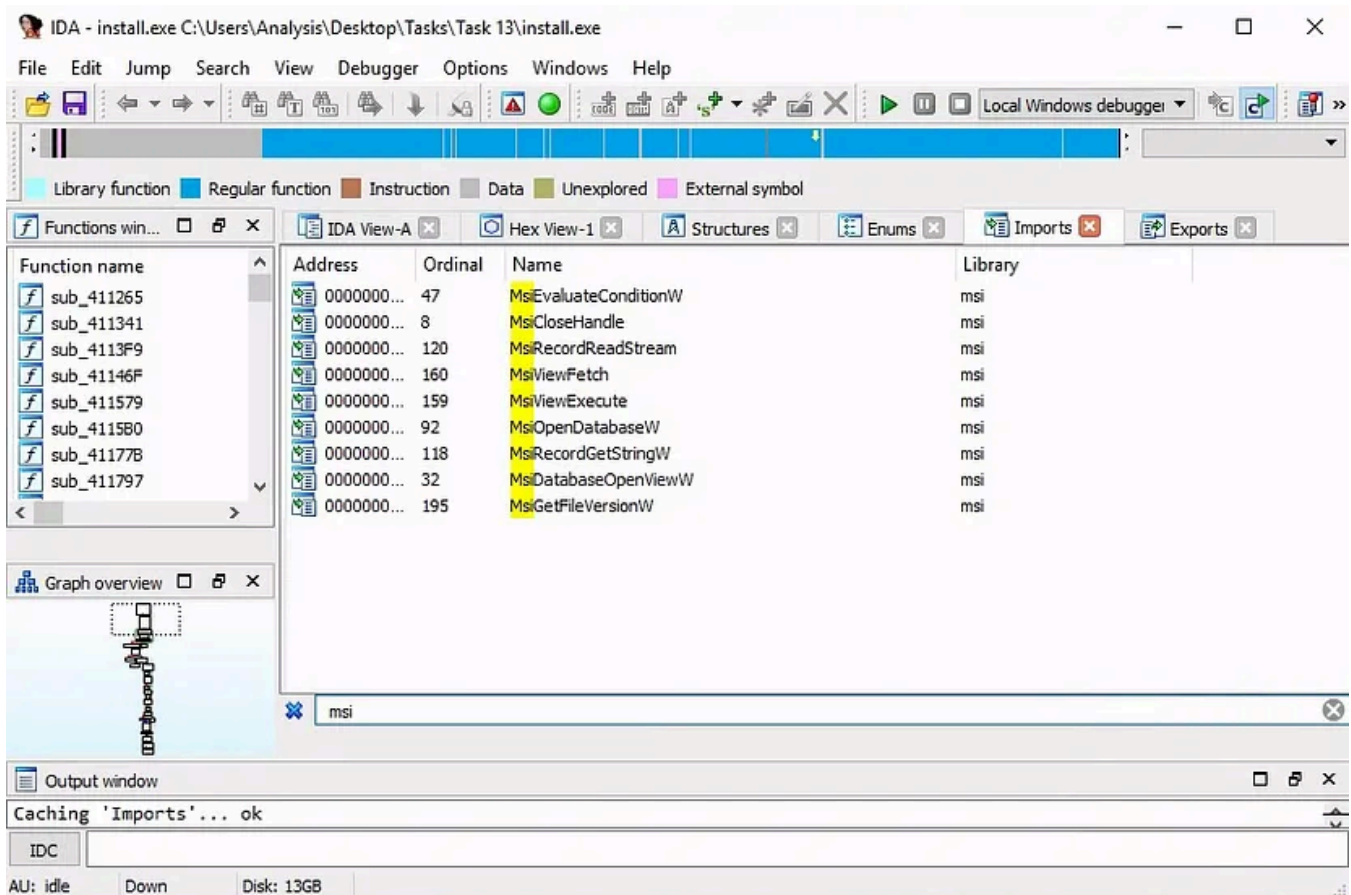
5



— — Task 13 — —

How many references are there to the library “msi” in the “Imports” tab of IDA Freeware for “install.exe”

Open in IDA -> Imports tab -> Ctrl + F “msi”



— — Task 14 — —

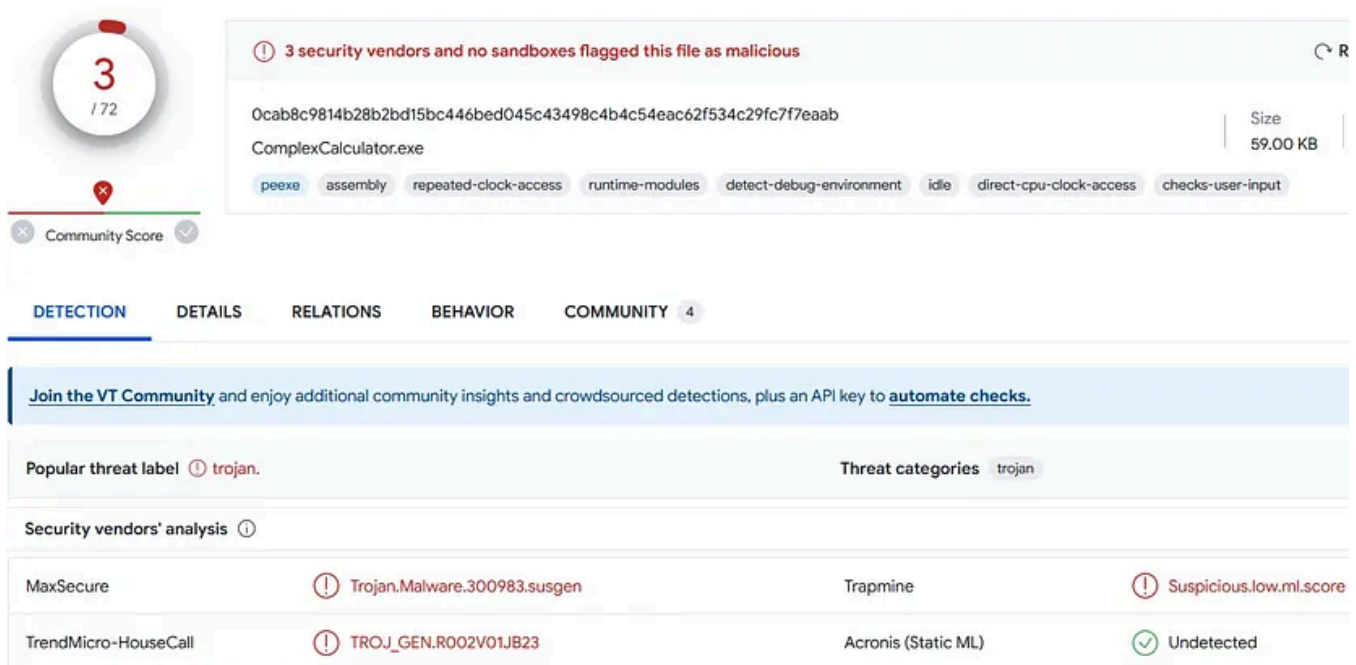
What is the MD5 Checksum of the file?

```
Set-Location 'C:\Users\Analysis\Desktop\Tasks\Task 14'  
  
Get-FileHash .\ComplexCalculator.exe -Algorithm MD5
```

F5BD8E6DC6782ED4DFA62B8215BDC429

Does Virustotal report this file as malicious? (Yay/Nay)

Yay



3 / 172

3 security vendors and no sandboxes flagged this file as malicious

0cab8c9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab

Size: 59.00 KB

ComplexCalculator.exe

peexe assembly repeated-clock-access runtime-modules detect-debug-environment idle direct-cpu-clock-access checks-user-input

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 4

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label: trojan. Threat categories: trojan

Security vendors' analysis

Vendor	Detection	Category	Status
MaxSecure	Trojan.Malware.300983.susgen	Trapmine	Suspicious.low.ml.score
TrendMicro-HouseCall	TROJ_GEN.R002V01JB23	Acronis (Static ML)	Undetected

Output the strings using Sysinternals “strings” tool.

What is the last string outputted?

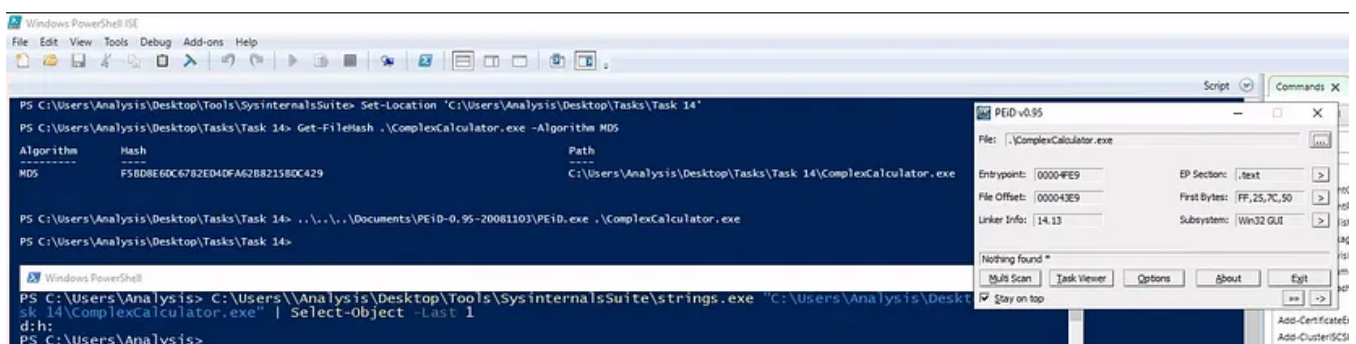
PowerShell.exe

C:\Users\Analysis\Desktop\Tools\SysinternalsSuite\strings.exe "C:\Users\Analysis\Desktop\Tools\SysinternalsSuite\strings.exe"

d:h:

What is the output of PeID when trying to detect what packer is used by the file?

Nothing found



Windows PowerShell

```
PS C:\Users\Analysis\Desktop\Tools\SysinternalsSuite> Set-Location "C:\Users\Analysis\Desktop\Tasks\Task 14"
PS C:\Users\Analysis\Desktop\Tasks\Task 14> Get-FileHash .\ComplexCalculator.exe -Algorithm MD5
```

Algorithm	Hash	Path
MD5	F5BD8E6DC6782ED4DF62B821580C429	C:\Users\Analysis\Desktop\Tasks\Task 14\ComplexCalculator.exe

```
PS C:\Users\Analysis\Desktop\Tasks\Task 14> ..\..\..\Documents\PEID-0.95-20081103\PEID.exe .\ComplexCalculator.exe
PS C:\Users\Analysis\Desktop\Tasks\Task 14>
```

Windows PowerShell

```
PS C:\Users\Analysis> C:\Users\Analysis\Desktop\Tools\SysinternalsSuite\strings.exe "C:\Users\Analysis\Desktop\Tools\SysinternalsSuite\strings.exe" | Select-Object -Last 1
d:h:
PS C:\Users\Analysis>
```

PeID v0.95

File: C:\ComplexCalculator.exe

Entrypoints: 00004FE9 BP Section: .text

File Offset: 000043E9 First Bytes: FF,25,7C,50

Linker Info: 14.13 Subsystem: Win32 GUI

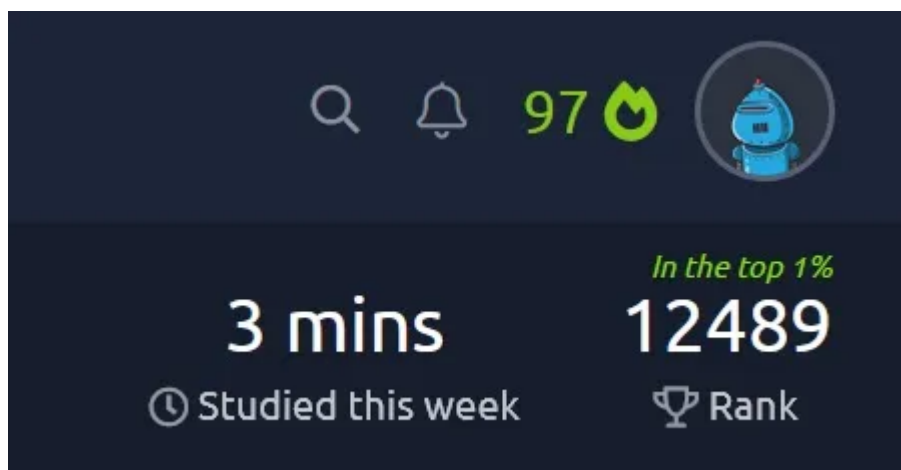
Nothing found *

Stay on top

Summary

This was a good little room. I should really get back to writing my boring paper for college now, I needed to take a break and do something in the CLI. TryHackMe is always good for that. I also need to finish this pathway eventually as I am going to use it as the last CPEs I need to renew some certifications.

On a happy note, I just got back into the TryHackMe Top 1% following the change in how they calculate this.

[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.

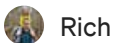


No responses yet

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



[Open in app ↗](#)

Medium

 Search

1110
0101 01
01 010
01

Hack
Me



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



10 10
1110
0101 01
01 010
01

Try
Hack
Me



Rich

Tempest TryHackMe Walkthrough

TL;DR walkthrough of the TryHackMe Tempest room.

Jun 14, 2024 52 1



them to hack us!

MIMIKATZ



Rich

Mimikatz Cheatsheet

TL;DR Mimikatz cheatsheet of things I have found useful in CRTTP 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

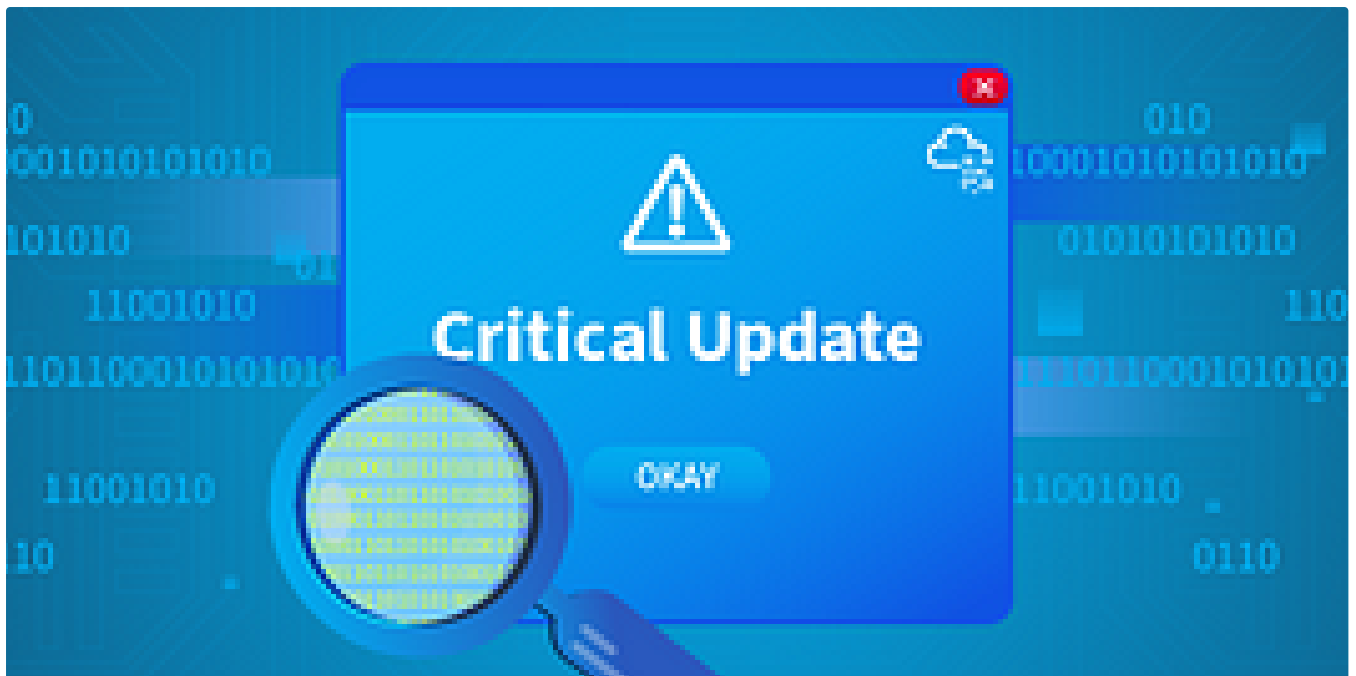


Nov 5, 2024



60





 In T3CH by Axoloth

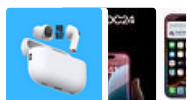
TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

★ Jul 21, 2024 🖱 104

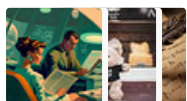


Lists



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



 In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

★ Nov 28, 2024 🖱 50



```
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#
```

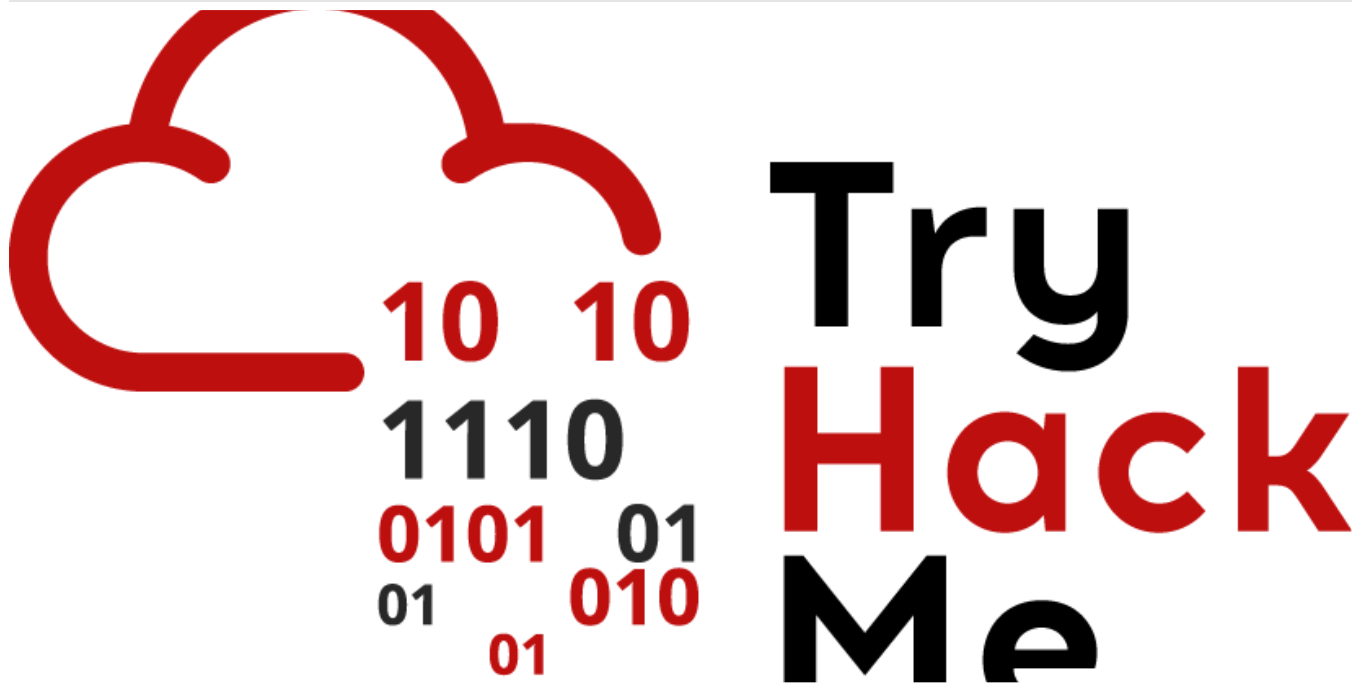
 Dan Molina

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



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



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 16:44:41.970037	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