

MAL: Malware Introductory

Introduction

In this section of the study the learner dives into understanding the purpose of malware analysis.

Activities

Task 1: What is the Purpose of Malware Analysis?

Malware analysis a form of incidence response useful in understanding how the behaviours of variants of malware result in their respective categorisation.

It is important to consider the following:

- Point of Entry (PoE) i.e. Was it through spam that our e-mail filtering missed and the user opened the attachment? Let's review our spam filters and train our users better for future prevention!
- What are the indicators that malware has even been executed on a machine? Are there any files, processes, or perhaps any attempt of "un-ordinary" communication?
- How does the malware perform? Does it attempt to infect other devices? Does it encrypt files or install anything like a backdoor / Remote Access Tool (RAT)?
- Most importantly - can we ultimately prevent and/or detect further infection?!

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The browser title bar says 'TryHackMe | MAL: Malware'. The address bar shows the URL 'https://tryhackme.com/room/malmalintroductory'. Below the browser, a dock contains icons for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and TryHackMe: Attackive... .

The main content area displays a task card:

Task 1 ✓ What is the Purpose of Malware Analysis?

Malware is such a prevalent topic within Cybersecurity, and often an unfortunately recurring theme among global news today. Not only is malware analysis a form of incidence response, but it is also useful in understanding how the behaviours of variants of malware result in their respective categorisation. This room will be a practical introduction to the techniques and tools used throughout malware analysis - albeit brief, I hope to expand on these techniques a lot more in-depth within the future.

When analysing malware, it is important to consider the following:

- Point of Entry (PoE) i.e. Was it through spam that our e-mail filtering missed and the user opened the attachment? Let's review our spam filters and train our users better for future prevention!
- What are the indicators that malware has even been executed on a machine? Are there any files, processes, or perhaps any attempt of "un-ordinary" communication?
- How does the malware perform? Does it attempt to infect other devices? Does it encrypt files or install anything like a backdoor / Remote Access Tool (RAT)?
- Most importantly - can we ultimately prevent and/or detect further infection?!

Answer the questions below

Ah, now I kinda understand...

6 Your streak has increased. You're 1 away from a badge!

Task 2: Understanding Malware Campaigns

Attacks can generally be classified into two types: **Targeted** and **Mass Campaign**.

Targeted

Malware attacks that occur created for a specific purpose against a specific target. A great example of this type of purpose could be the [DarkHotel](#) malware, whom is designed to steal information such as authentication details from government officials.

Mass Campaign

The most common type of attacks. The entire purpose of this type of Malware is to infect as many devices as possible and perform whatever it may - regardless of target.

The screenshot shows a Kali Linux desktop environment with a web browser open to the TryHackMe room 'malmalintroductory'. The browser tabs include 'Assignment: MAl' and 'TryHackMe | MAL: Malwa'. The page content discusses targeted malware like 'Crouching Yeti' and lists industries targeted by Stuxnet. It also mentions the WannaCry ransomware attack. Two questions are shown: 'What is the famous example of a targeted attack-esque Malware that targeted Iran?' (Answer: Stuxnet) and 'What is the name of the Ransomware that used the Eternalblue exploit in a "Mass Campaign" attack?' (Answer: WannaCry). Both answers are marked as correct. The task bar at the bottom indicates 'Task 3' is active.

Task 3: Identifying if a Malware Attack has Happened

The screenshot shows a continuation of the TryHackMe challenge. It discusses the WannaCry attack and the 'Eternalblue' exploit. The task involves identifying the steps of a malware attack. The first question asks for the first step: 'Name the first essential step of a Malware Attack?' (Answer: Delivery), which is marked as correct. The second question asks for the second step: 'Now name the second essential step of a Malware Attack?' (Answer: Execution), which is also marked as correct. Other questions listed but not yet answered include: 'What type of signature is used to classify remnants of infection on a host?' (Host-Based Signatures) and 'What is the name of the other classification of signature used after a Malware attack?' (Network-Based Signatures). The task bar at the bottom indicates 'Task 4' is active.

Task 4: Static Vs. Dynamic Analysis

Two categories used when analysing malware are **Static Analysis** and **Dynamic Analysis**

Static Analysis.

Used to gain a high-level abstraction of the sample - it can be fairly simple to decide if a piece of code is "malicious" or not with this method alone. At its core, this method is of the analysis of the sample at the state it presents itself as, without executing the code.

Employing the use of techniques such as signature analysis via checksums means quick, efficient and safe analysis of malware.

Dynamic Analysis

This is where the abstraction of the sample is largely built upon. **Dynamic Analysis** essentially involves executing the sample and observing what happens. This of course is not safe. If the sample turns out to be "Ransomware". If it is capable of propagating via traversing a network, now Local Area Network (LAN) is just infected.

2. Dynamic Analysis

Whilst the methods and tools used for these two categories are vastly different, they are essential in compositing an understanding of how malware operates.

Static Analysis.

At its brief, "Static Analysis" is used to gain a high-level abstraction of the sample - it can be fairly simple to decide if a piece of code is "malicious" or not with this method alone (but not always, this will be discussed later...). At its core, this method is of the analysis of the sample at the state it presents itself as, without executing the code.

Employing the use of techniques such as signature analysis via checksums means quick, efficient (albeit extremely brief) and safe analysis of malware.

Dynamic Analysis

This step is a lot more involved, and is where the abstraction of the sample is largely built upon. "Dynamic Analysis" essentially involves executing the sample and observing what happens. This of course is not safe. If the sample turns out to be "Ransomware" - you've now lost your files. If it is capable of propagating via traversing a network, nice...You've now just infected your Local Area Network (LAN).

Please note that these are extremely simplistic explanations of these techniques, there is a lot more involved which we will go throughout this series.

Answer the questions below

I understand the two broad categories employed when analysing potential malware!

No answer needed Correct Answer

Task 5: Discussion of Provided Tools & Their Uses

Tools overlapping between Static and Dynamic analysis:

You will see that some tools will overlap between Static and Dynamic analysis:

Provided Static Analysis Tools:

- C:\Users\Analysis\Desktop\Tools\Static\PE Tools
 - Dependency Walker (depends)
 - PeID
 - PE Explorer
 - PEView
 - ResourceHacker
- C:\Users\Analysis\Desktop\Tools\Static\Disassembly
 - IDA Freeware
 - WinDbg
- C:\Users\Analysis\Desktop\Tools\Sysinternalsuite
 - ResourceHacker
- C:\Users\Analysis\Desktop\Tools\Dynamic

The tools listed here will be used for future tasks, as they involve debugging which is currently out-of-scope for this room...However, will be explored later within the series.

Answer the questions below

Lets proceed

Task 6: Connecting to the Windows Analysis Environment (Deploy)

Whilst malware has been known to traverse (spread) over RDP, in this instance, any and all samples on here are not capable of doing so - nor are they capable of performing any destructive action.

This series will teach you the practical knowledge and tool familiarity to allow you to transfer these skills to actual samples if you wish too, outside of TryHackMe

With this being a Windows instance specifically, alongside the additional tools and tasks it has to execute, please expect up to wait up towards 10 minutes before being able to access your instance. The average deploy to login took about 7 minutes. Also, please note that the Host will not respond to pings - only the (Remote Desktop Protocol) RDP protocol (3389)

Credentials:

You can either connect via RDP (connect to our network first via OpenVPN), or control the machine in browser (no connection required). Please note that this Windows "instance" will take atleast 5 minutes to fully boot - please be patient. You can view the progress via the progress-bar within the display above.

10.10.152.201

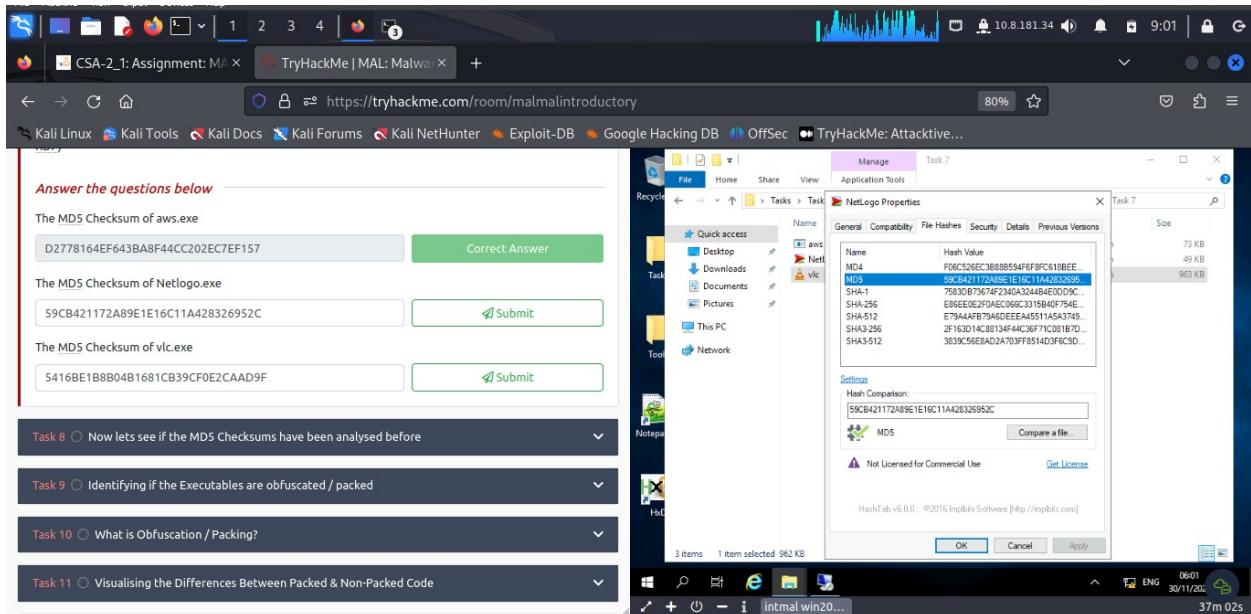
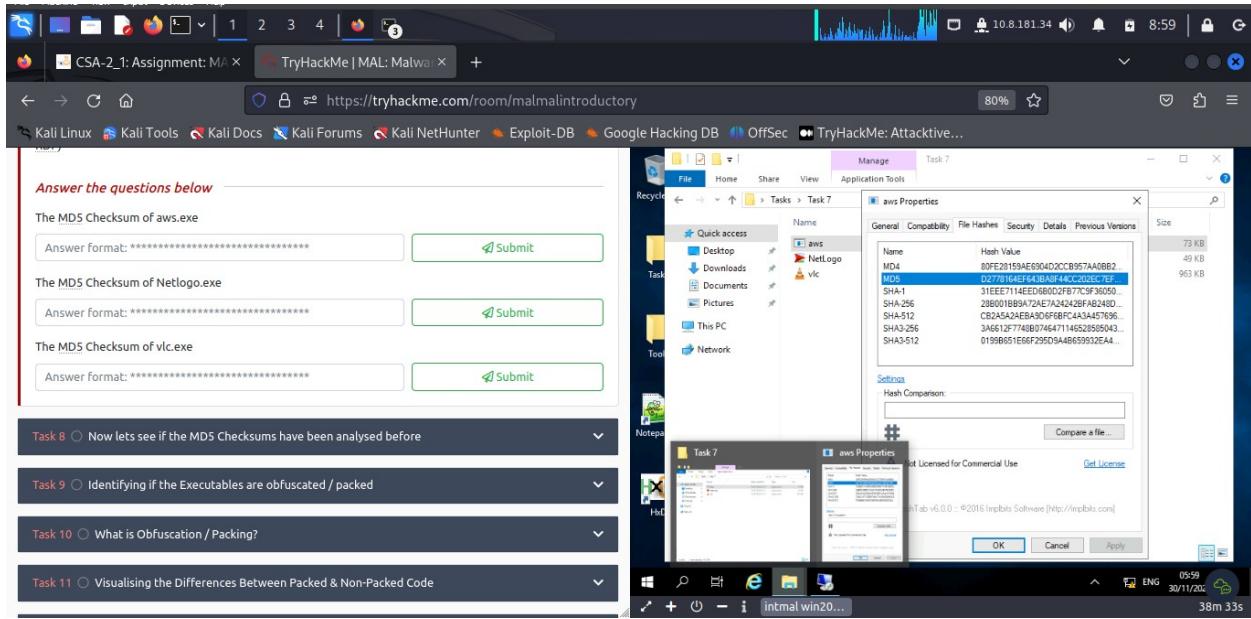
Username: Analysis

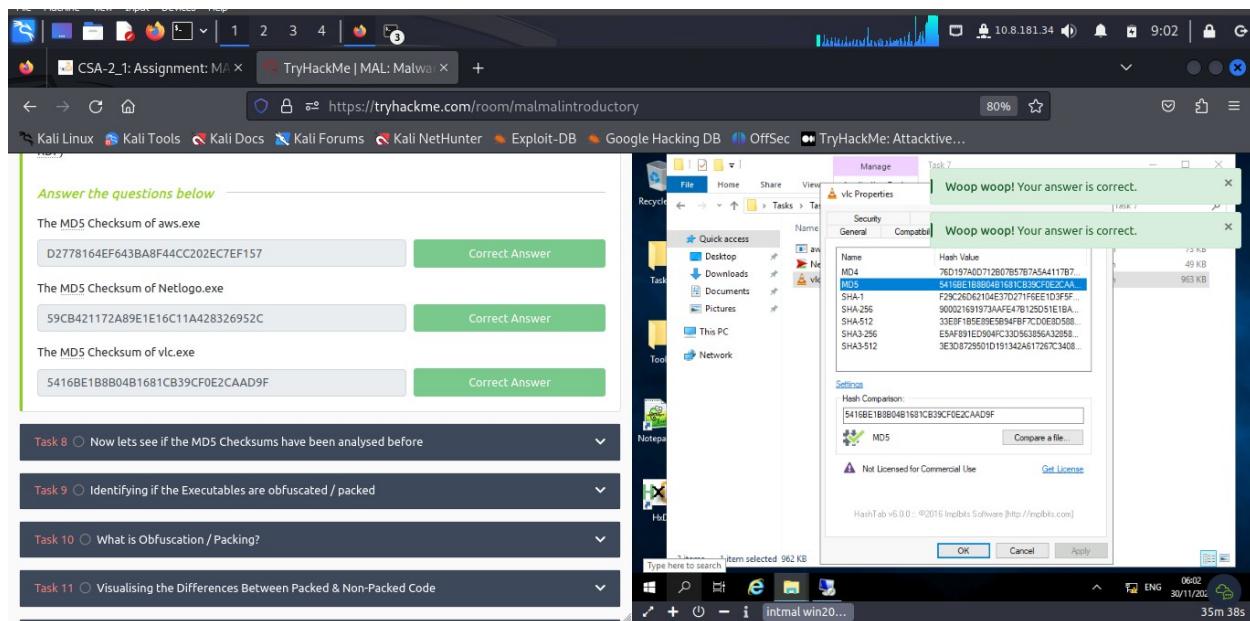
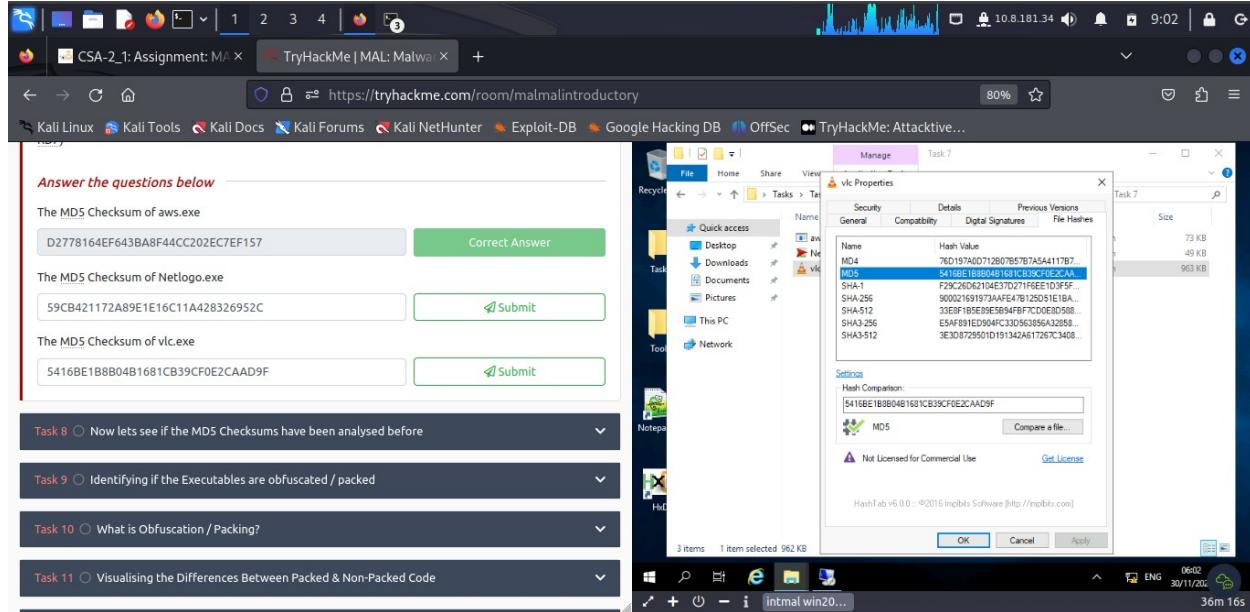
Password: Tryhackme123!

Windows:

Start Machine

Task 7: Obtaining MD5 Checksums of Provided Files





Task 8: Now let's see if the MD5 Checksums have been analysed before

The screenshot shows a browser window with multiple tabs open. The active tab is 'VirusTotal - Home' at <https://www.virustotal.com/gui/home/search>. The search bar contains the file hash 'D2778164EF643BA8F44CC202EC7EF157'. Below the search bar, there's a message: 'Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with VT ENTERPRISE.' A blue speech bubble icon in the bottom right corner says 'Want to automate submissions? Check our API, or access your API key.'

This screenshot shows a browser window with a task list and a file properties dialog. The task list includes:

- Task 5: Discussion of Provided Tools & Their Uses
- Task 6: Connecting to the Windows Analysis Environment (Deploy)
- Task 7: Obtaining MD5 Checksums of Provided Files
- Task 8: Now lets see if the MD5 Checksums have been analysed before

Below the tasks, there's a note: "Outside of the Remote Windows Environment, i.e. Kali or your Windows PC, look up those MD5 "Checksums" on Virustotal to solve this task." There are three answer fields:

- Does Virustotal report this MD5 Checksum / file aws.exe as malicious? (Yay/Nay) Answer: Nay
- Does Virustotal report this MD5 Checksum / file Netlogo.exe as malicious? (Yay/Nay) Answer format: ***
- Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay) Answer format: ***

A file properties dialog for 'aws' is open, showing various hash values (MD4, MD5, SHA-1, SHA-256, SHA-512, SHA-3, SHA-3-512) and their corresponding hex values.

This screenshot shows a browser window displaying a detailed analysis of a file on VirusTotal. The file hash is '28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a'. The analysis summary indicates it's 'File distributed by Microsoft, Blender Foundation and others'. Key details include:

- Detection: 24+
- Size: 73.00 KB
- Last Analysis Date: 7 hours ago
- File Type: EXE

The 'DETAILS' tab is selected, showing basic properties:

Property	Value
MDS	d2778164ef643ba8f44cc202ec7ef157
SHA-1	31eee714ee6dbb0d2fb77c9f3605057639050786
SHA-256	28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a
Vhash	074046655d155a2f12
Authentihash	53057c2aa89f38b306ce21a92faad4001c18a36817c3e7f87389f19c225
ImpHash	e6948a1a715c6300d85bc0ed2e15faa

A blue speech bubble icon in the bottom right corner says 'Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.'

No security vendors and no sandboxes flagged this file as malicious

e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536
NetLogo.exe

peexe assembly detect-debug-environment long-sleeps via-tor 64bits

Size: 49.00 KB | Last Analysis Date: 2 days ago | EXE

MD5	59cb421172a89e1e16c11a428326952c
SHA-1	7583db7367412340a324404e0dd9c0973e989ff
SHA-256	e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536
Vhash	054066651d1515751az16hz13z27z35z
Authentihash	c8235dfc442649b77f6629023269ff5739bffd46fb99226c35ecc0652212d522
Imphash	708060edc261af91104ef208478326fb

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Task 7 ✓ Obtaining MD5 Checksums of Provided Files

Task 8 ○ Now lets see if the MD5 Checksums have been analysed before

Outside of the Remote Windows Environment, i.e. Kali or your Windows PC, look up those MD5 "Checksums" on [VirusTotal](#) to solve this task!

Answer the questions below

Does Virustotal report this MD5 Checksum / file aws.exe as malicious? (Yay/Nay)

Correct Answer

Does Virustotal report this MD5 Checksum / file NetLogo.exe as malicious? (Yay/Nay)

Correct Answer

Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)

Submit

Task 9 ○ Identifying if the Executables are obfuscated / packed

NetLogo Properties

General Compatibility File Hashes Security Details Previous Versions

Name	Hash Value
MD4	FOGCS56EC3B888594P6FBC610BEE...
MD5	59CB421172A89E1E16C11A42832695...
SHA-1	7583DB7367412340A324404E0DD9C09...
SHA-256	E86EE0E2F0AEC066C3315B40F754EE25AC...
SHA-384	E794AD79A4C4D4A5D45A54A54A54A54...
SHA-512	2F153D14C38134F14C36F71C381B7D...
SHA-32	3039C56E3D20A703F8514D3F9C9D...

File Hashes

Hash Comparison:

HashTab v6.0.0 - ©2016 Ingibit Software [<http://ingibit.com>]

OK Cancel Apply

No security vendors and 1 sandbox flagged this file as malicious

900021691973aafe47b125d51e1bae5192760e91552dda0c7051226640c0a248
vlc.exe

Size: 962.70 KB | Last Analysis Date: 1 day ago | EXE

Basic properties

MD5	5416be1b8b04b1681cb39cf0e2caad9f
SHA-1	f29c2d62104e37d271f6ed1d3f5fd8e55b89db
SHA-256	900021691973aafe47b125d51e1bae5192760e91552dda0c7051226640c0a248
Vhash	0950e7d155515555c051058z4553f22321lzbaz1
Authentihash	f69432591a65d6e9a04a3204e28421ad25736c3b92e5848e331e1c733146e9a
ImpHash	8e8dd7ad3d2126158cbc6c64d7f49db

Task 7 Obtaining MDS Checksums of Provided Files

Task 8 Now lets see if the MDS Checksums have been analysed before

Outside of the Remote Windows Environment, i.e. Kali or your Windows PC, look up those MDS "Checksums" on VirusTotal to solve this task:

Answer the questions below

Does VirusTotal report this MDS Checksum / file aws.exe as malicious? (Yay/Nay)

Nay Correct Answer

Does VirusTotal report this MDS Checksum / file Netlogo.exe as malicious? (Yay/Nay)

Nay Correct Answer

Does VirusTotal report this MDS Checksum / file vlc.exe as malicious? (Yay/Nay)

Nay Correct Answer

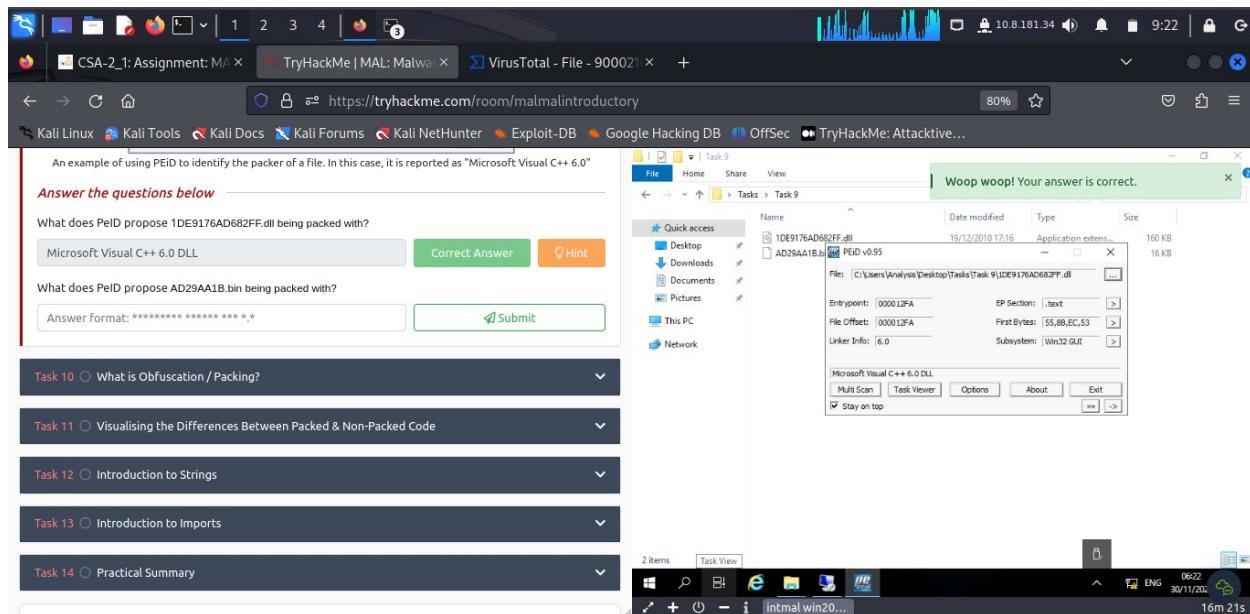
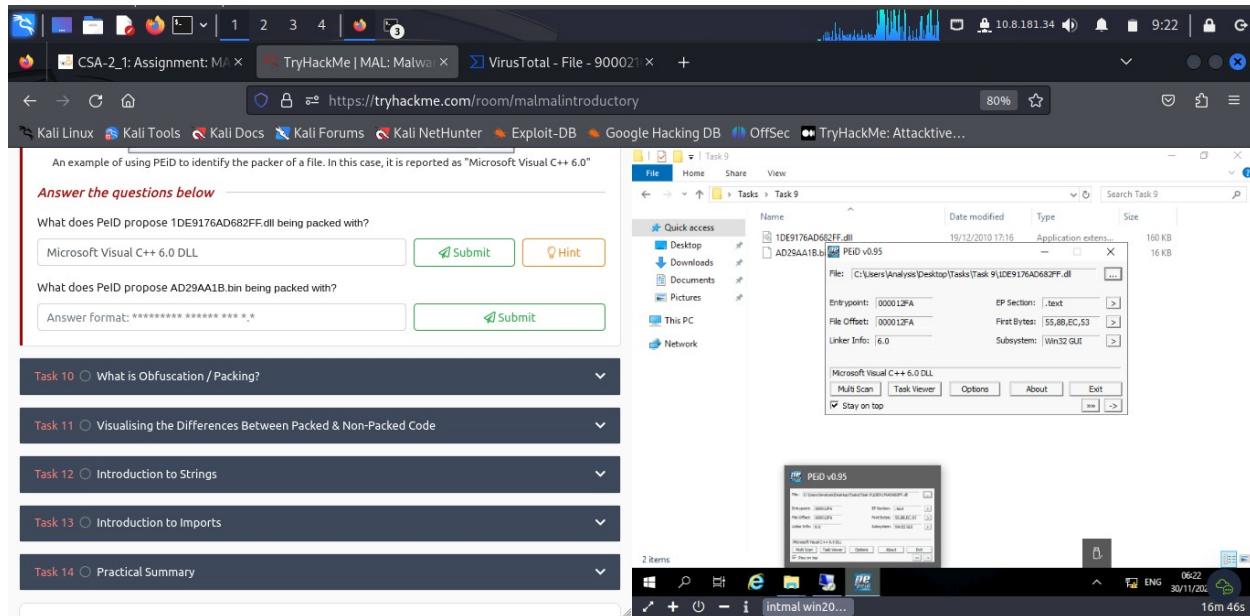
Task 9 Identifying if the Executables are obfuscated / packed

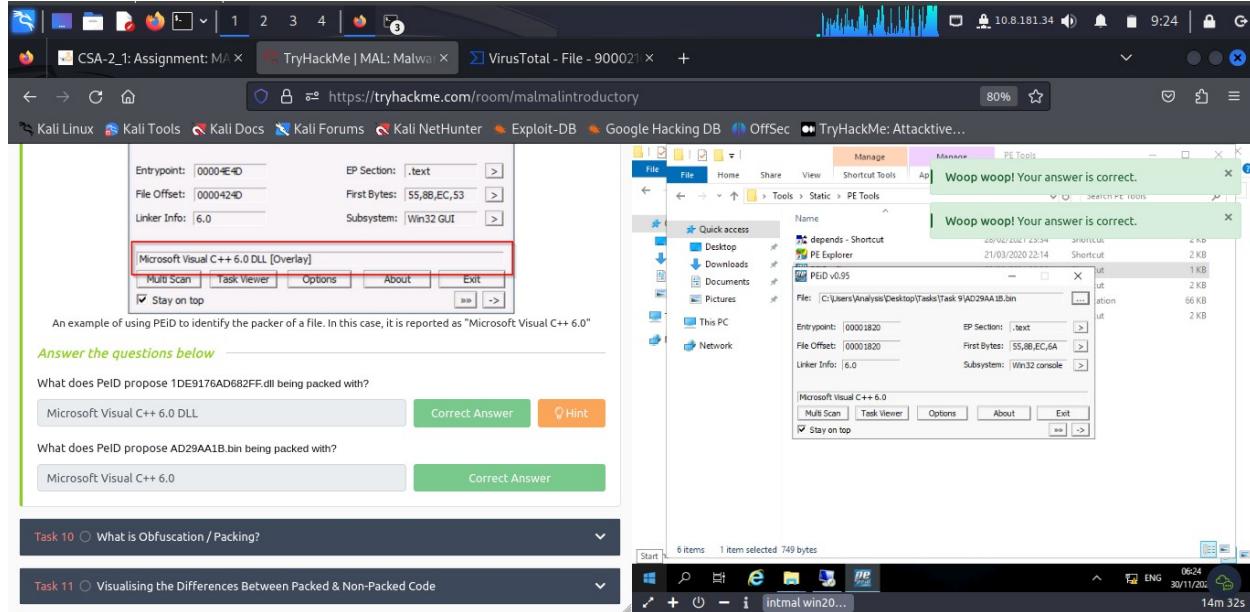
File Explorer showing 'aws.exe' properties:

Name	Hash Value
MD4	76D197A0D712B07B57B7A54A117B7...
MD5	5416BE1B8B04B1681CB39CF0E2CAAD9F...
SHA-1	E29C2D62104E37D271F6ED1D3F5FD8E55B89DB...
SHA-256	900021691973AAFE47B125D51E1BAE5192760E91552DDA0C7051226640C0A248...
SHA-512	32E3F165E39E58A58A59F7C20E8D10B80...
SHA3-256	E5AF891ED904FC3D0563856A32658...
SHA3-512	3E3D07295D1D1913424617267C340B...

Task 9: Identifying if the Executables are obfuscated/packed

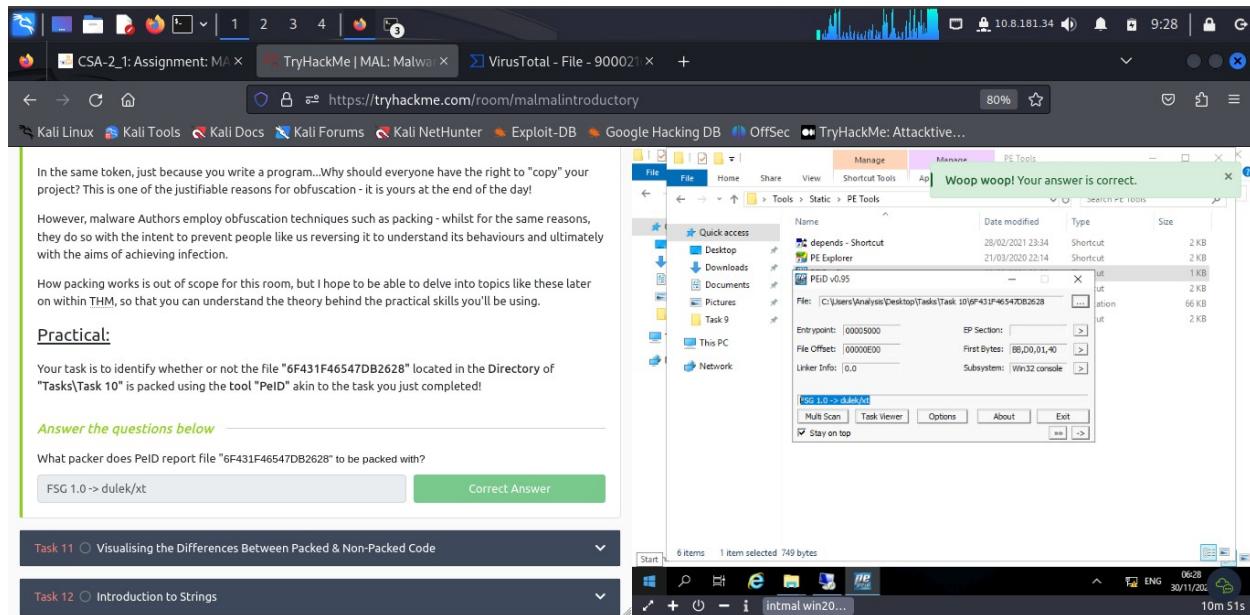
Because a file doesn't have the ".exe" extension, doesn't mean it isn't an actual executable! For instance, it can have the ".jpg" extension and still be an executable piece of code.

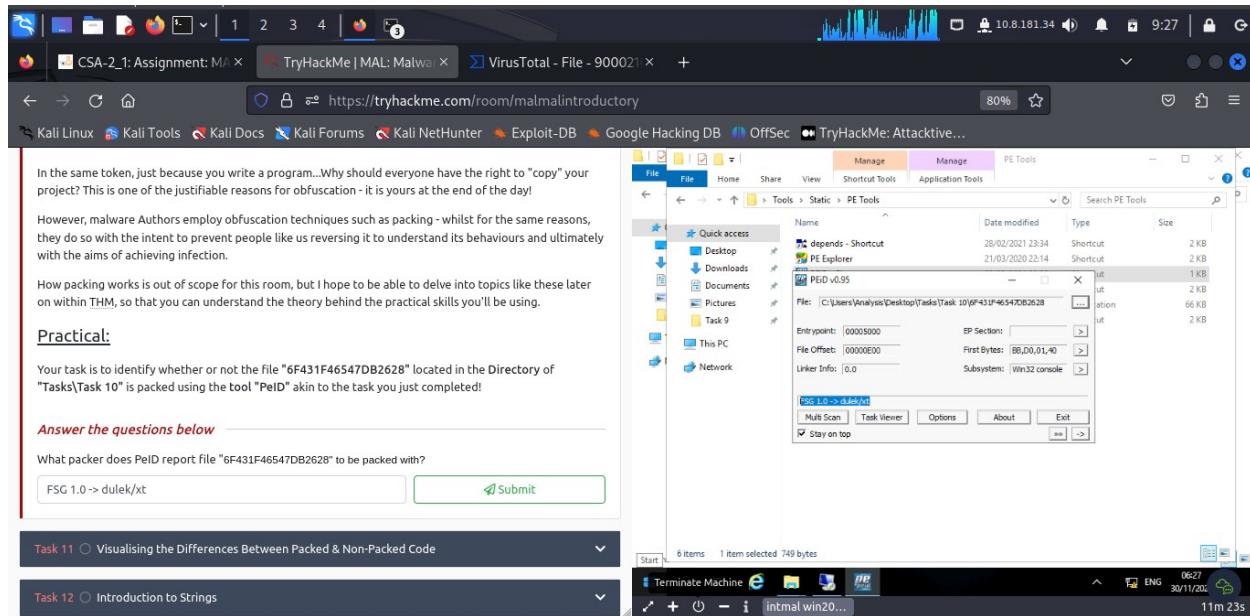




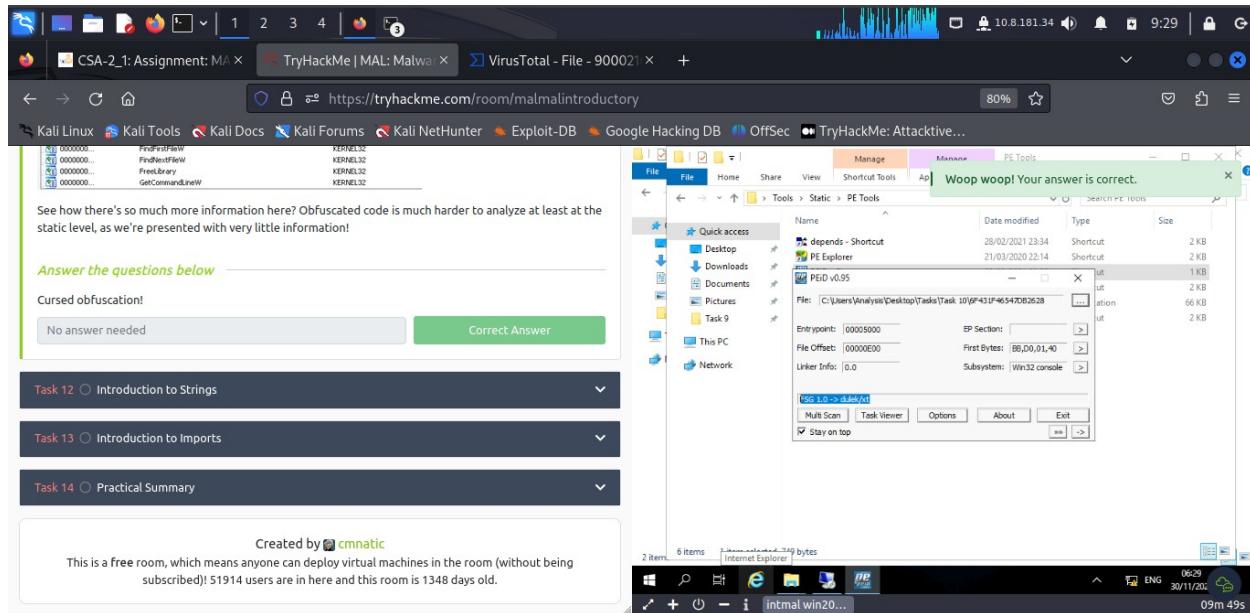
Task 10: What is Obfuscation/Packing

Packing is one form of obfuscation that malware Authors employ to prevent the analysis of programmes.





Task 11: Visualizing the Differences Between Packed & Non-Packed Code



Task 12: Introduction to Strings

The URL that is outputted after using "strings" is **practicalmalwareanalysis.com**

For Help, press F1

You can now answer Question #2!

Answer the questions below

What is the URL that is outputted after using "strings"

practicalmalwareanalysis.com

Correct Answer

How many unique "Imports" are there?

Answer format: *

Submit

Task 13 ○ Introduction to Imports

Task 14 ○ Practical Summary

Created by cmnatic

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 51928 users are in here and this room is 1349 days old.

Extend machines timer

07:09 30/11/2023 28m 52s

unique "Imports" available are 5.

For Help, press F1

You can now answer Question #2!

Answer the questions below

What is the URL that is outputted after using "strings"

practicalmalwareanalysis.com

Correct Answer

How many unique "Imports" are there?

5

Correct Answer

Task 13 ○ Introduction to Imports

Task 14 ○ Practical Summary

Remote Desktop Connection

Administrator

Administrator@DESKTOP-1QHJL9K

Local

General

Send password when connecting to this computer

For Help, press F1

07:12 30/11/2023 26m 15s

Task 13: Introduction to Imports

References available to the library "msi" in the "Imports" tab of IDA Freeware for "install.exe" are 9.

The initial autanalysis has been finished.

There are various tabs, similar to what we saw in "PE Explorer" i.e. "Imports" and "Exports".

Task:

Navigate to the directory "Tasks/Task 13" and open "install.exe" with IDA Freeware, just like we did in the example above. Again, this may take a few seconds to a couple of minutes to compute dependant upon the size of the application. For this task expect roughly ~20 seconds.

You can now answer the question below:

Answer the questions below

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

9

Correct Answer

Task 14 Practical Summary

Created by cmnatic

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 51928 users are in here and this room is 1349 days old.

remote-eu-18.tryhackme.tech 53m 25s

Task 14: Practical Summary

I'm not going to walk you through this one, but you have done all the necessary steps above to achieve this. GL HF:^)

If you struggle, revisit the techniques you used above. Moreover, if you're still stuck, visit the TryHackMe Discord!

The file specified for analysis is "ComplexCalculator.exe" in the Directory "Tasks/Task 14". I'll leave it up to you to figure out what tool(s) out of what we've used above is best!

Answer the questions below

What is the MD5 Checksum of the file?

F5BDE6DC6782ED4DF62B8215BDC429

Correct Answer

Hint

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

Yay

Correct Answer

Hint

Output the strings using Sysinternals "strings" tool.

What is the last string outputted?

Answer format: *.*:

Submit

Hint

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

Answer format: *****

Submit

Hint

Created by cmnatic

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 51928 users are in here and this room is 1349 days old.

VirusTotal - File - 0cab8c

ComplexCalculator Properties

General Compatibility File Hashes Security Details Previous Versions

Name	Hash Value
MD4	E819E3E3E5E5A43B9EF48D0E...
MD5	F8A8C9A8A8A8A8A8A8A8A8A8A8A...
SHA-1	05202FC7CD533D74A341552A1...
SHA-256	0CA4B03814B20B2D195C4468E20...
SHA-512	C71791C5B379B4FC150FD08192...
SHA-226	E11FF1D2D233091000D1502958501...
SHA3-512	E9172103C9A654FABE177C14450B...

MD5

Not Licensed for Commercial Use

Hachoir v3.0.0 - ©2015 Infolabs Software (http://infolabs.com)

OK Cancel Apply

Task View THM AttackBox intmal win20... 48m 57s

The Virustotal report this file as malicious, correct (Yay).

3 security vendors and no sandboxes flagged this file as malicious

Ocab8c9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab

ComplexCalculator.exe

MD5: f5bd8e6dc6782ed4dfa62b8215bdc429
SHA-1: 00620c9fcfd853ee97e43615e6a1527282a69ec
SHA-256: Ocabc9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab
Vhash: 064056555d15551bd0
Authenticodehash: a542e2bbe0ca16a2eccc0422945b5dae37765d0e50930e2f9ffb1012838b349d50
ImpHash: 793abde3a3cbe50f9193181d171f8a2b

The last string outputted is d:h:

Woop woop! Your answer is correct.

d:h

Answer the questions below

What is the MD5 Checksum of the file? F5BDBE6EDC6782ED4DFa62B8215BDC429

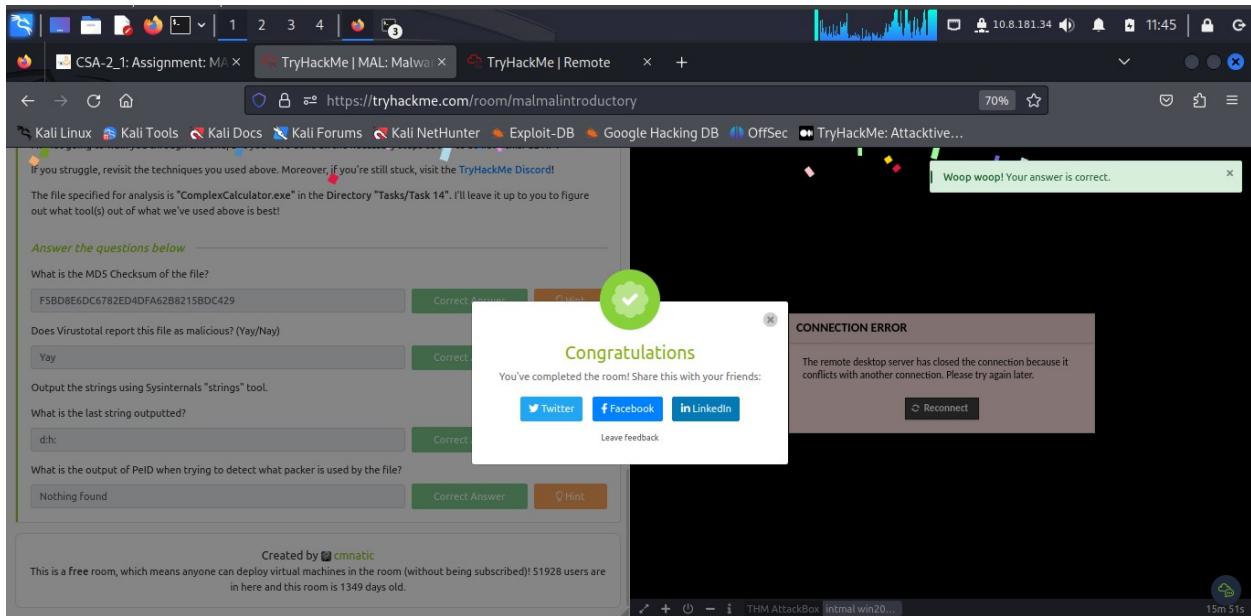
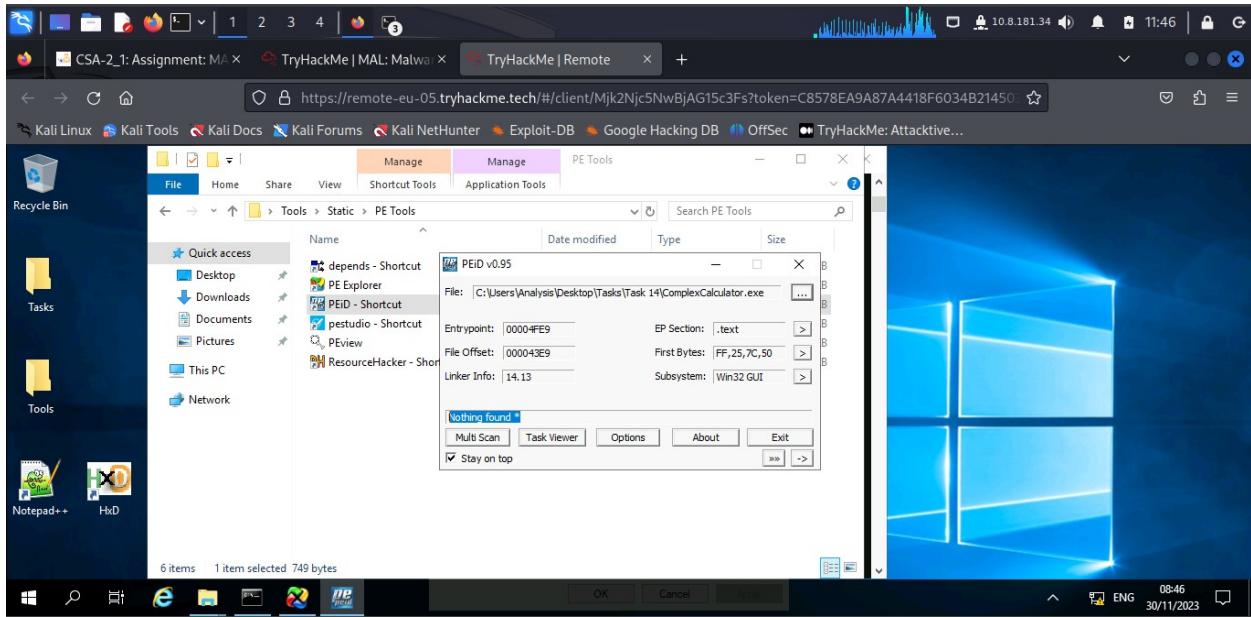
Does Virustotal report this file as malicious? (Yay/Nay) Yay

Output the strings using Sysinternals "strings" tool.

What is the last string outputted? d:h

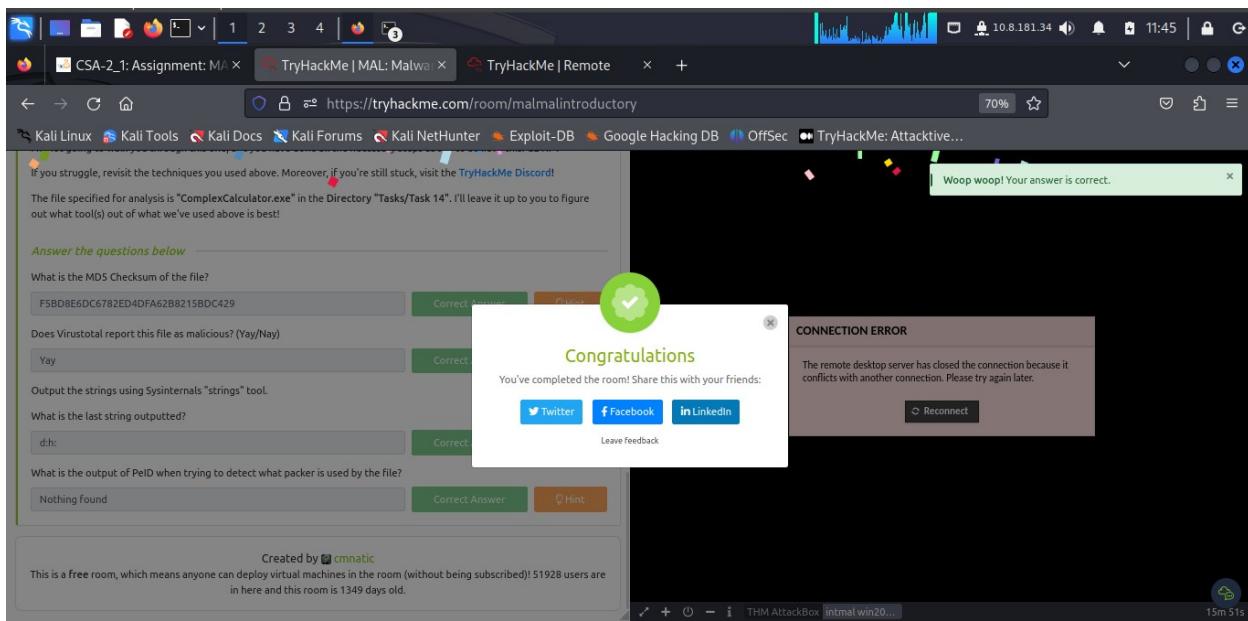
What is the output of PeID when trying to detect what packer is used by the file? Answer Format: *****

The output of PeID when trying to detect the packer used by the file is **Nothing found**.



Conclusion

This task took the learner through analyzing malware and using tools like PE Explorer, PEiD, IDA and to achieve the goal of recognizing types of files which can be harm in disguise; this knowledge is critical for aspiring Security Analyst to know the files available in a given computer device.



Completion Link: <https://tryhackme.com/room/malmalintroductory>