MAL: Malware Introductory

Introduction

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

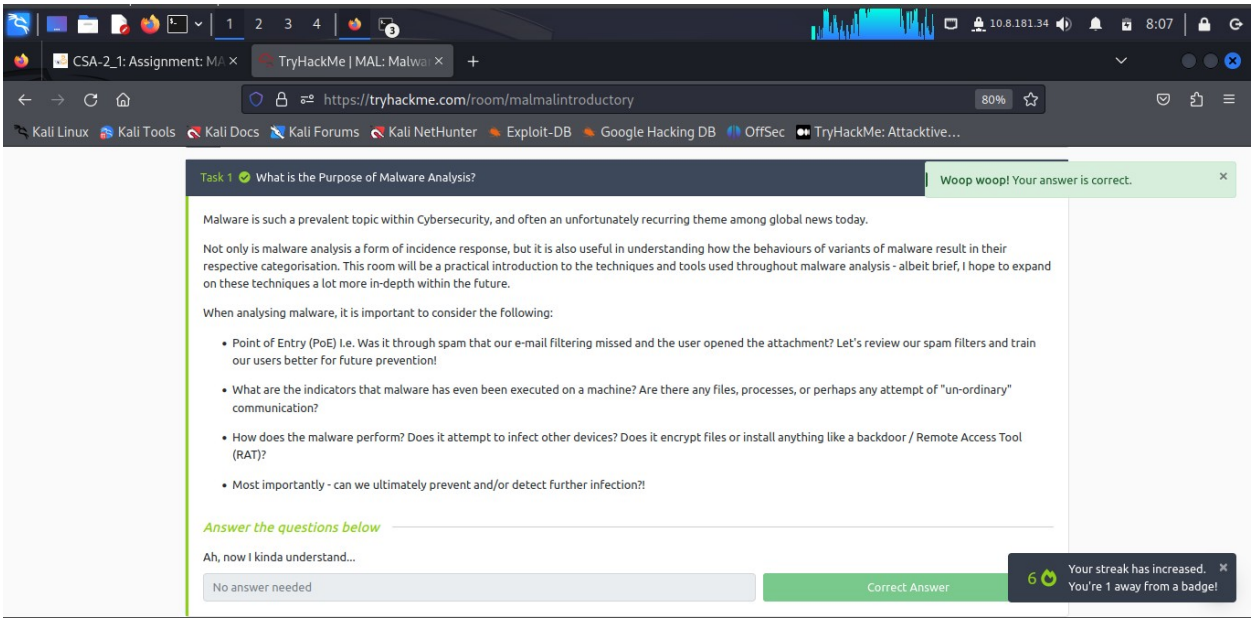
Activities

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?!



Task 2: Understanding Malware Campaigns

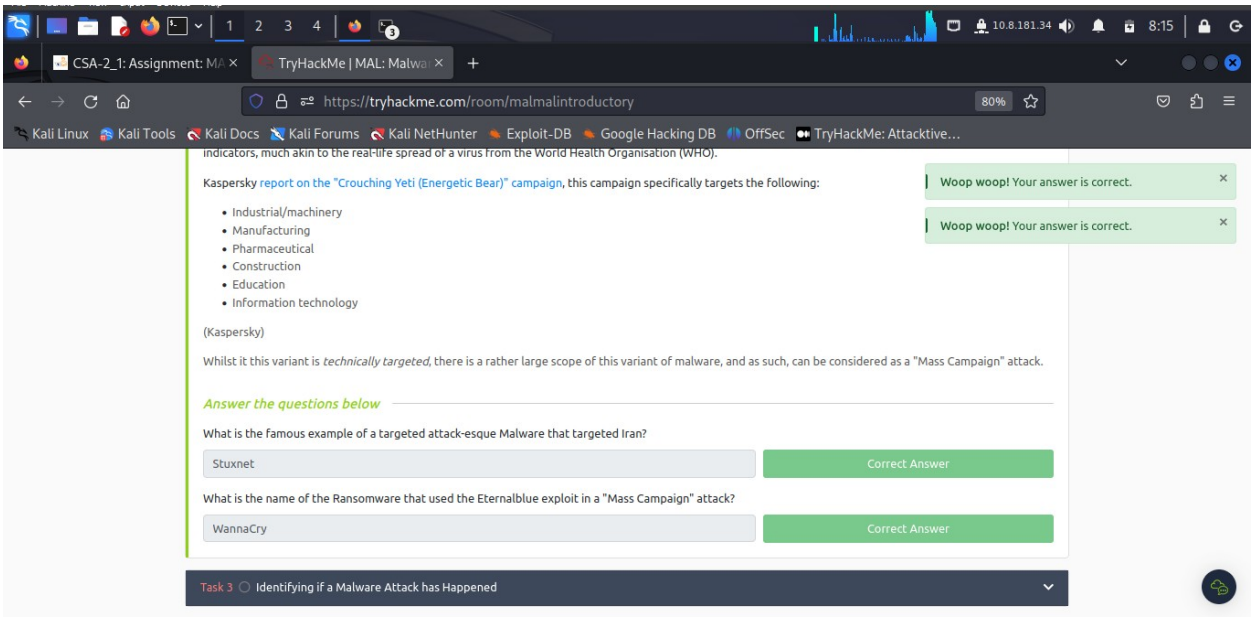
Attacks can generally be classified into two types: **Targeted** and **Mass Campaign**.

Targeted

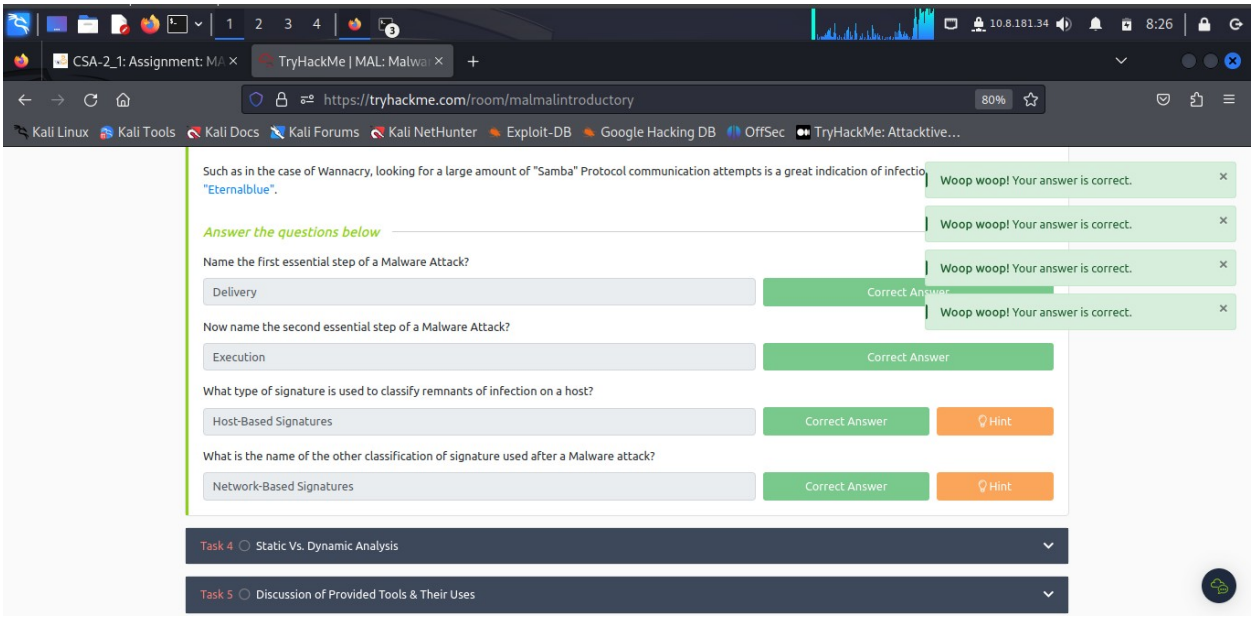
Malware attacks that occur created for a specific purpose against a specific target. A great example of this type of purpose could be the DarkHotel malware, whom is designed to steal information such as authentication details from government officials.

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.



Task 3: Identifying if a Malware Attack has Happened



Task 4: Static Vs. Dynamic Analysis

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

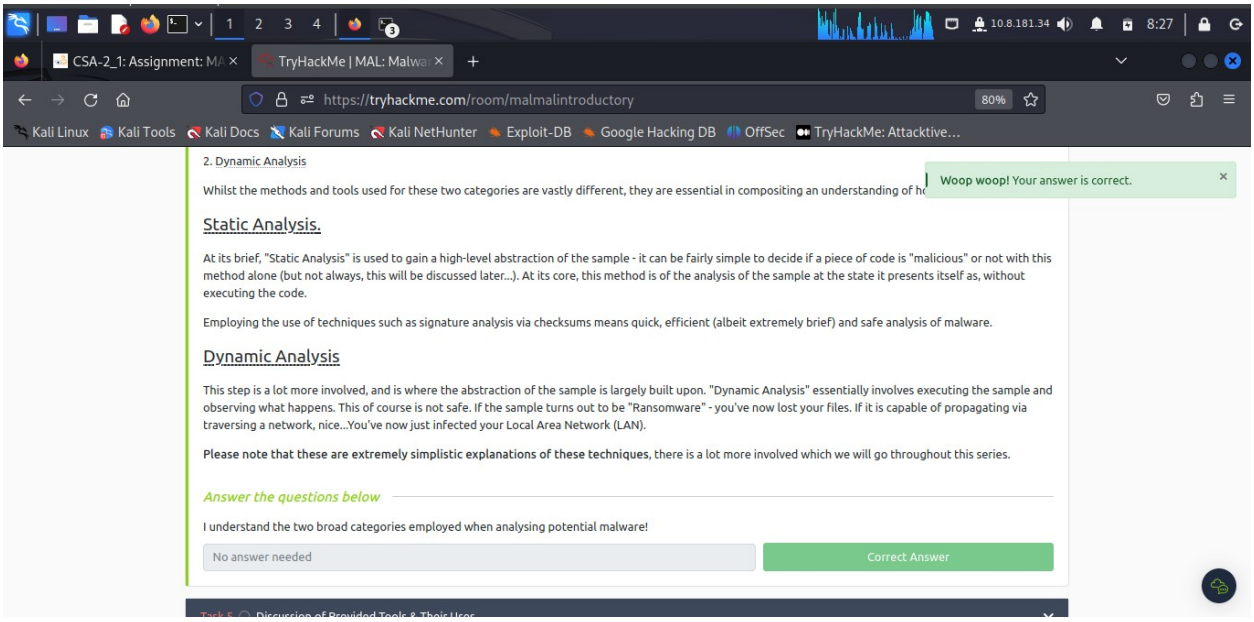
Static Analysis.

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.

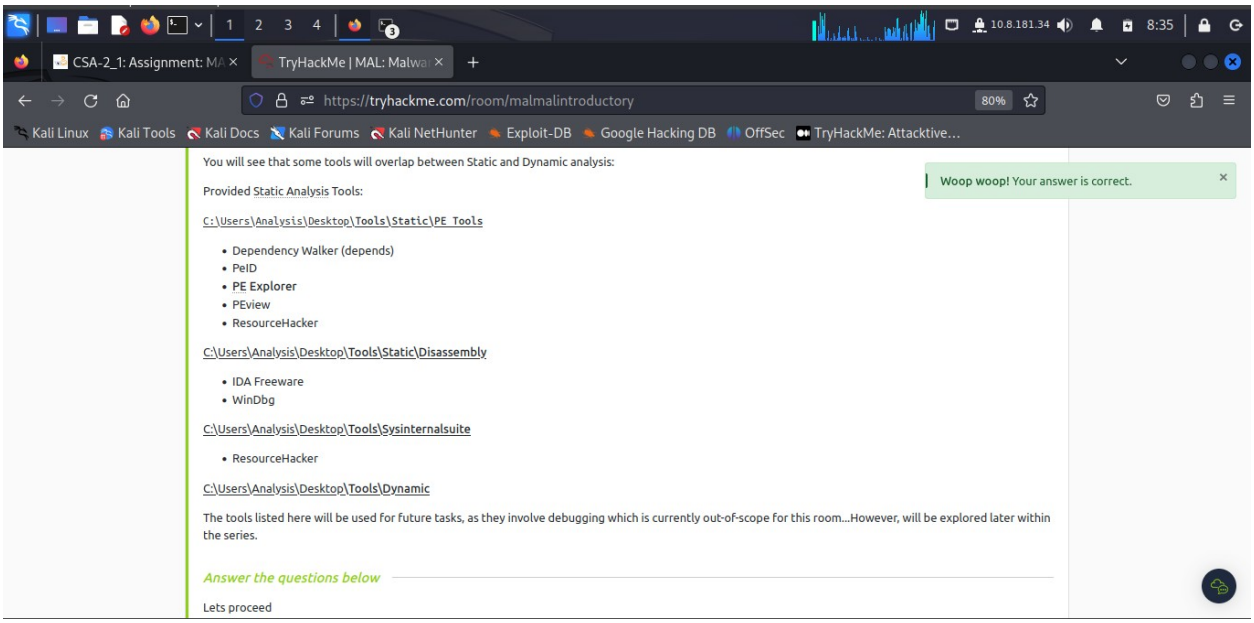
Dynamic Analysis

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.

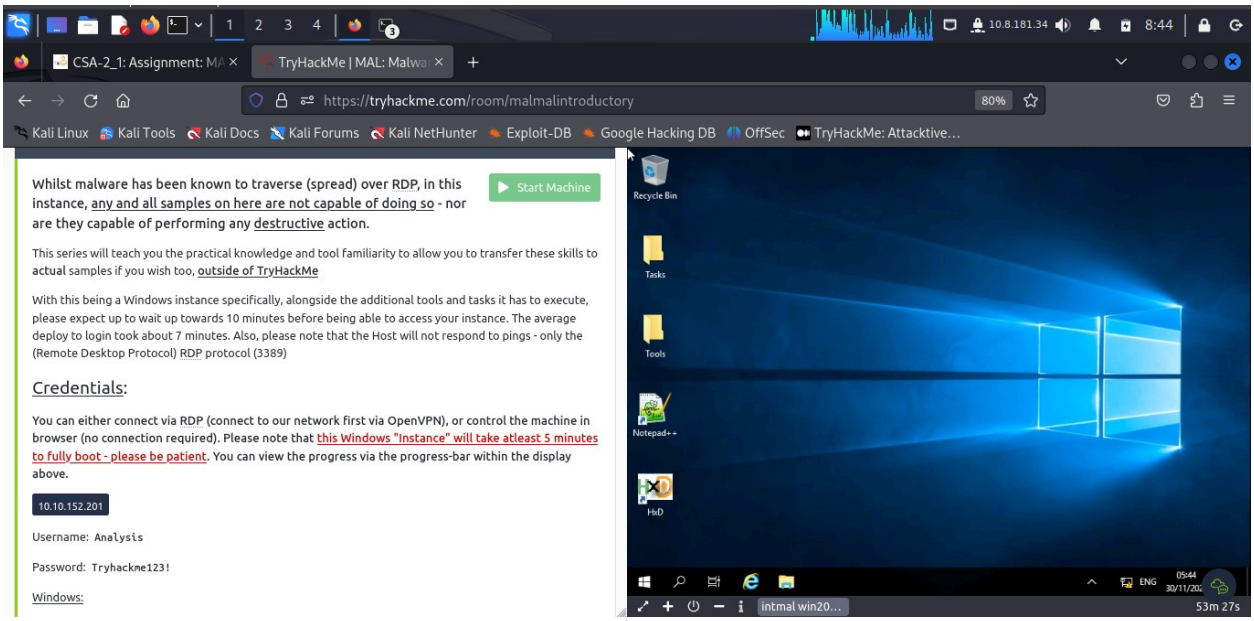


Task 5: Discussion of Provided Tools & Their Uses

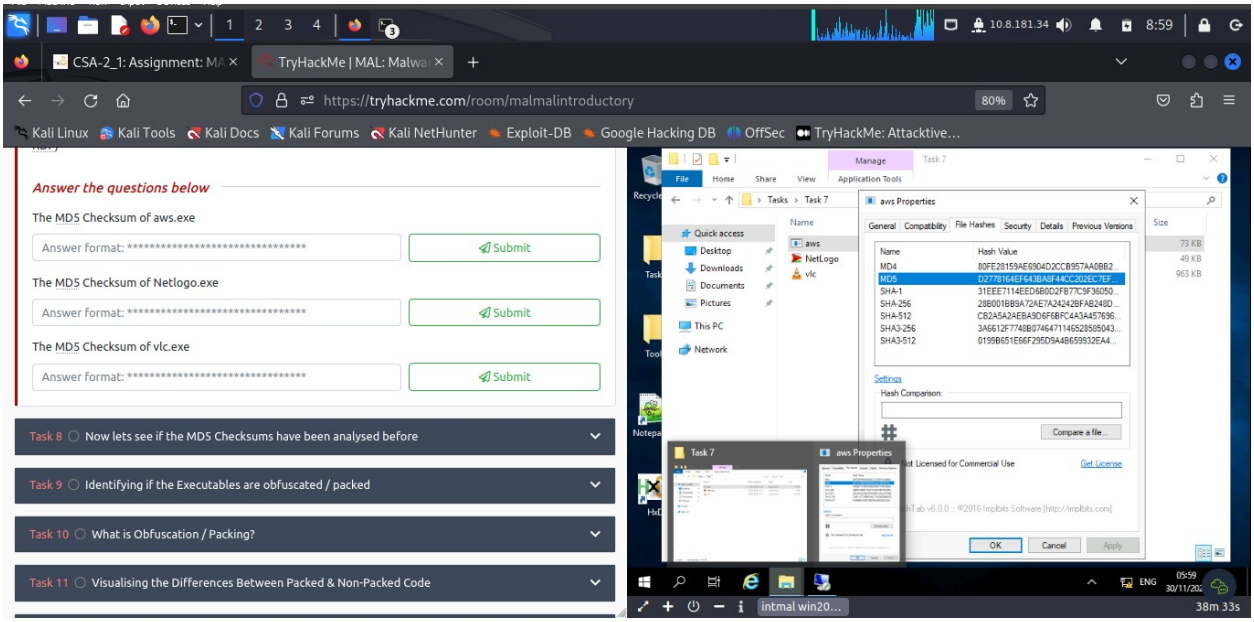
Tools overlapping between Static and Dynamic analysis:

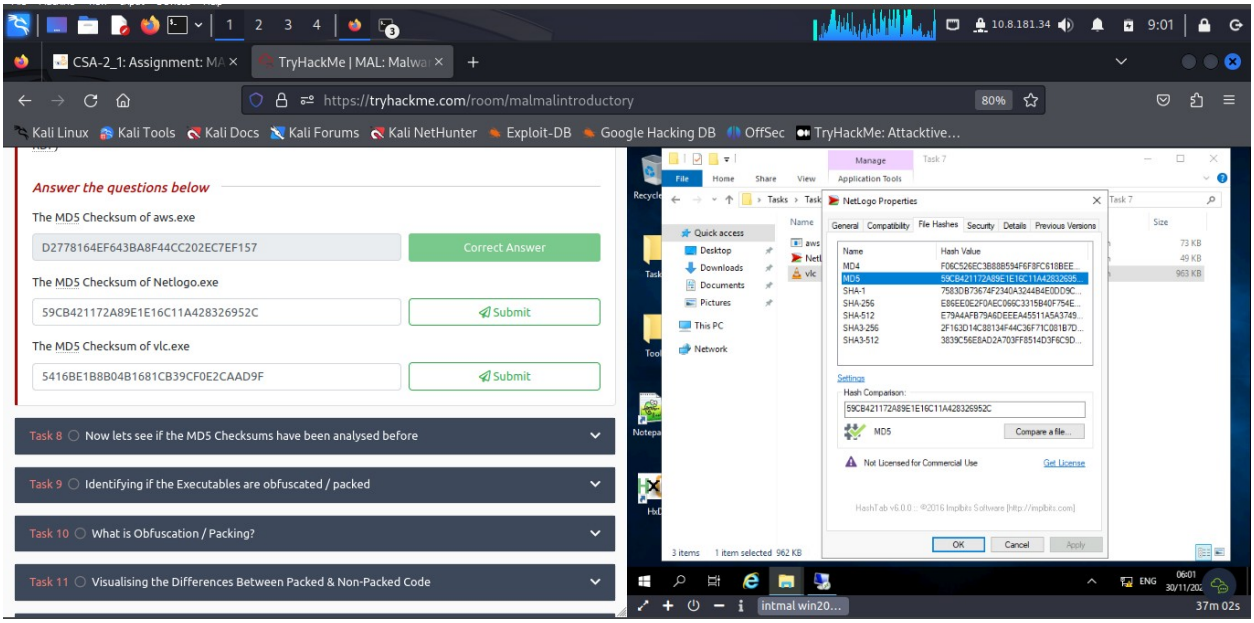


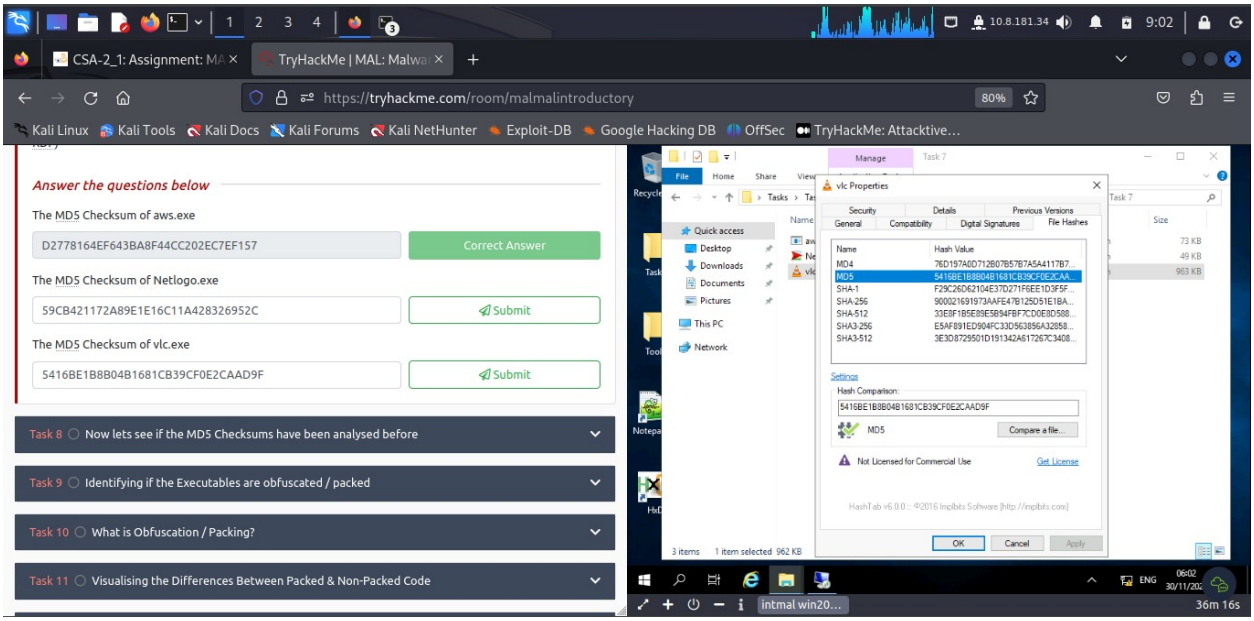
Task 6: Connecting to the Windows Analysis Environment (Deploy)

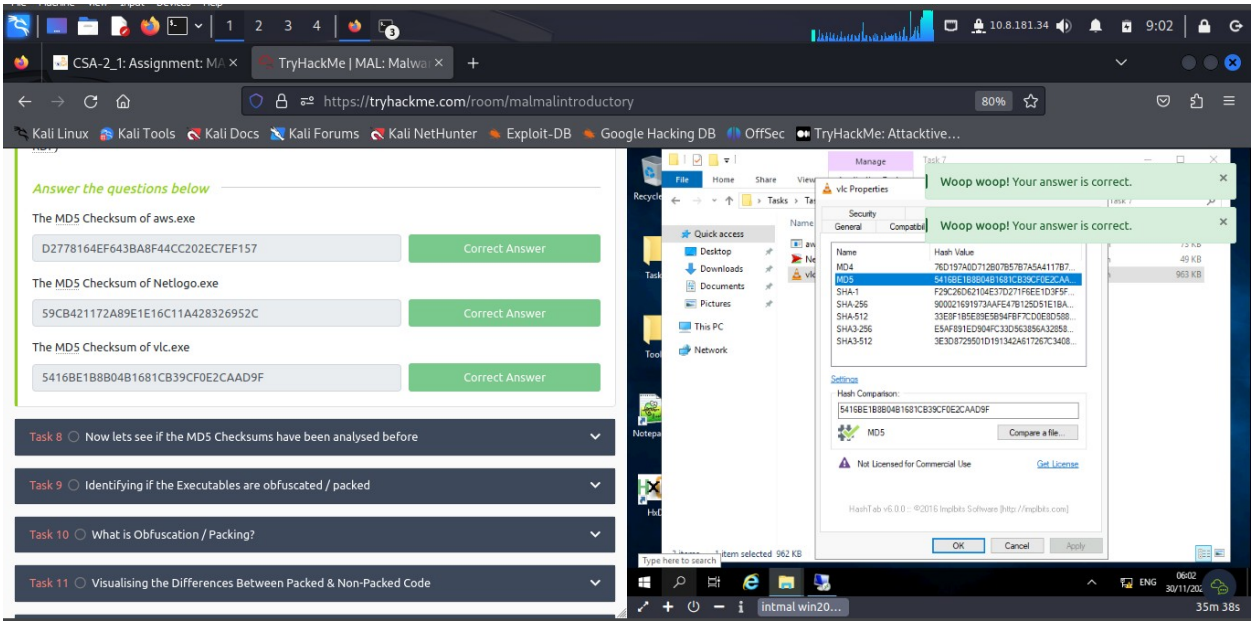


Task 7: Obtaining MD5 Checksums of Provided Files

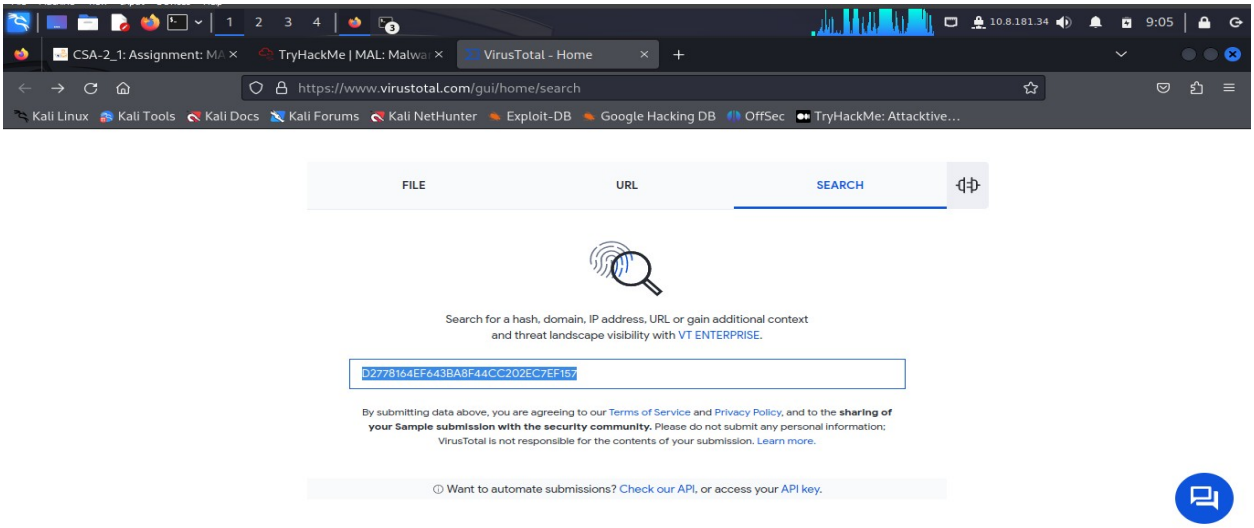


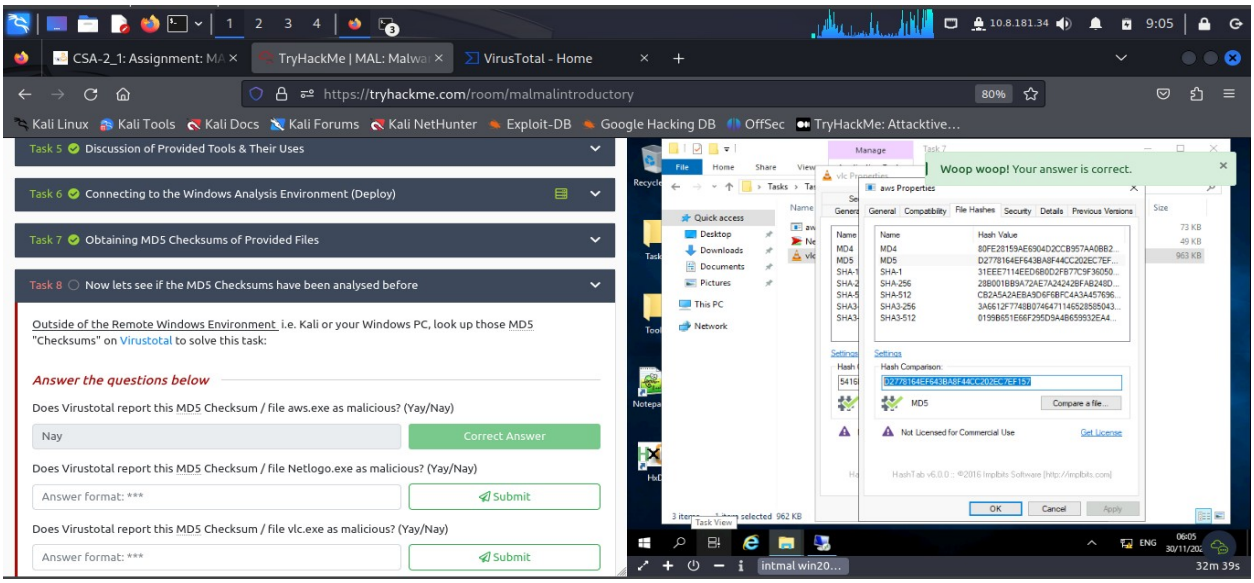


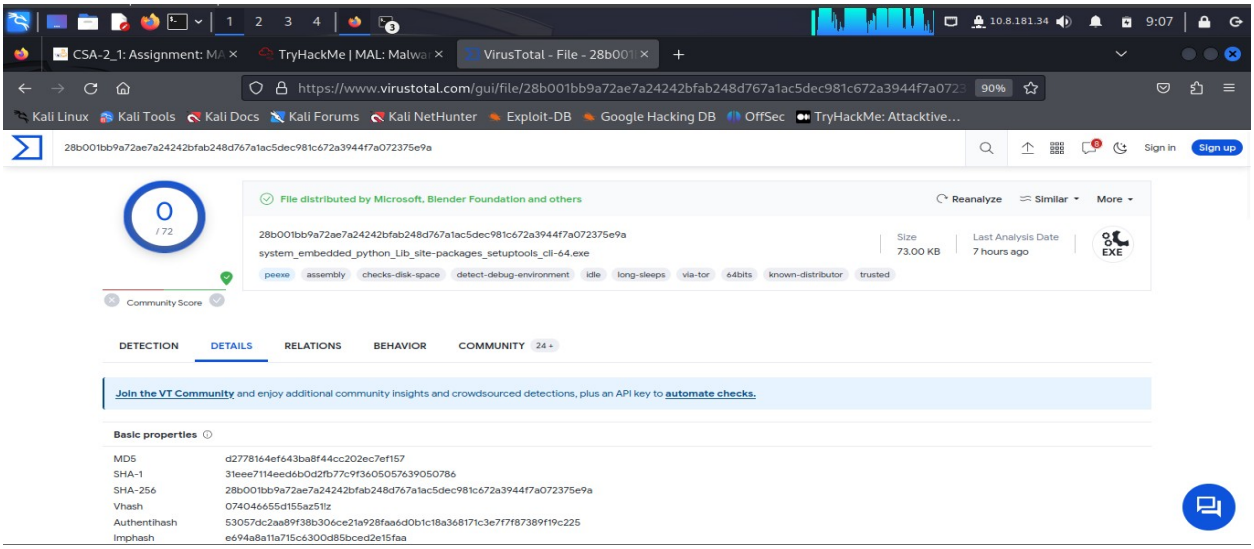


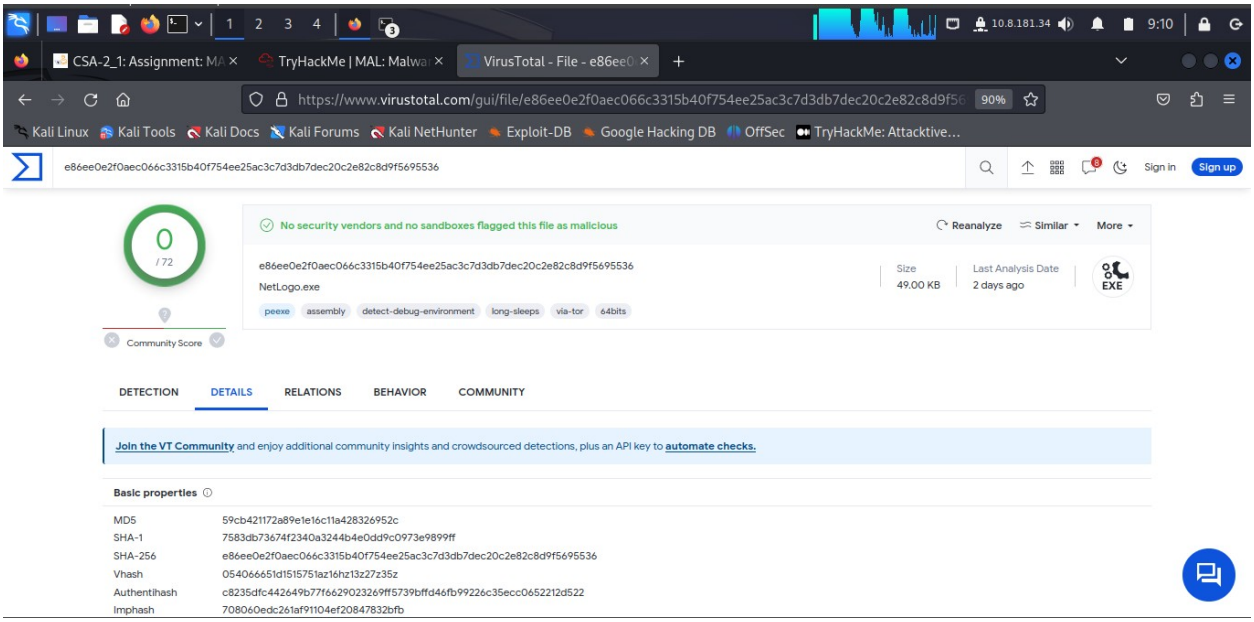


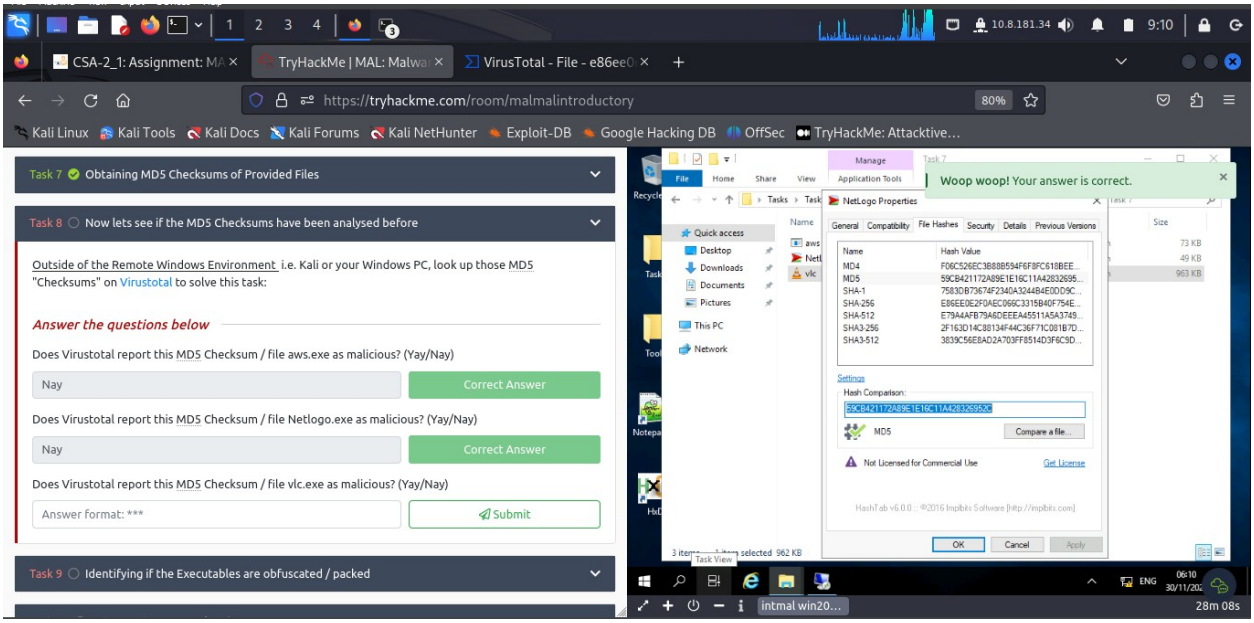
Task 8: Now let's see if the MD5 Checksums have been analysed before

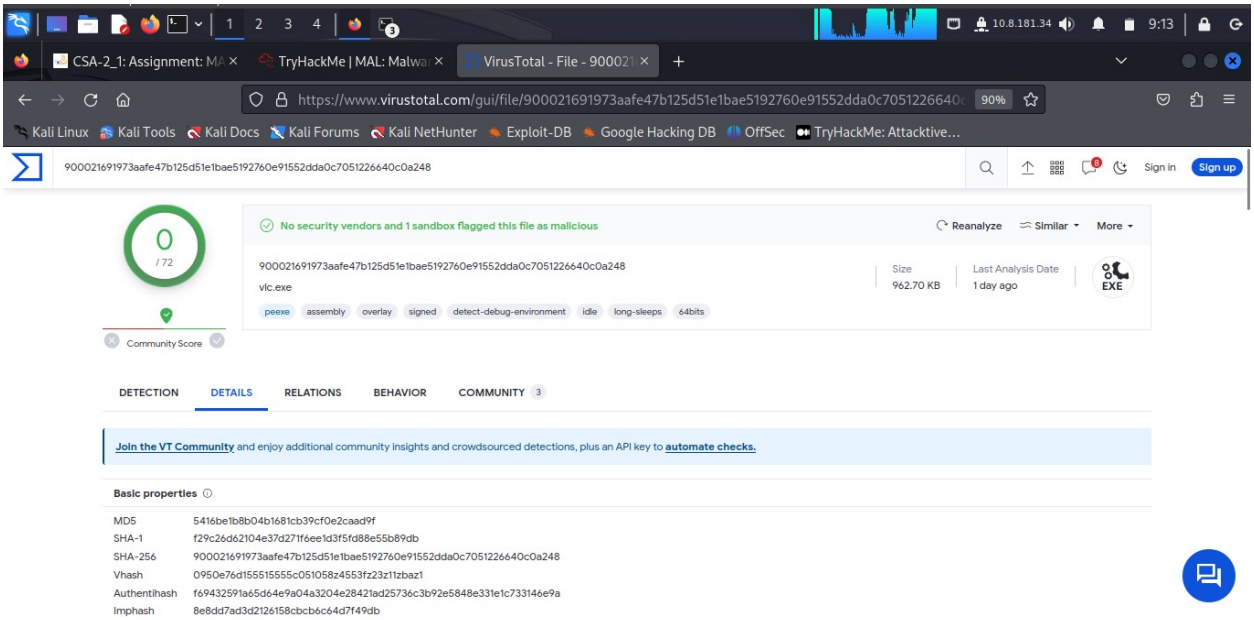

CSA-2_1: Assignment: MA
TryHackMe | MAL: Malwa
VirusTotal - Home
https://www.virustotal.com/gui/home/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TryHackMe: Attacktive...
FILE
URL
SEARCH
Search for a hash, domain, IP address, URL or gain additional context
and threat landscape visibility with VT ENTERPRISE.
D2778164EF643BA8F44CC202EC7EF157
By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, or access your API key.

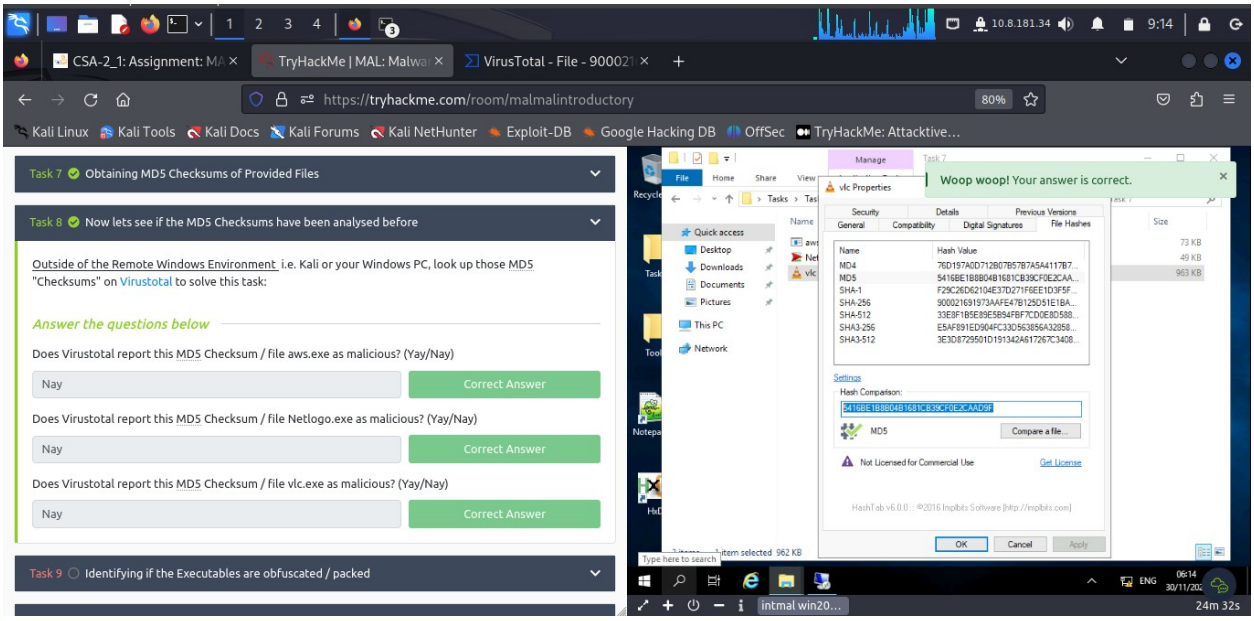

CSA-2_1: Assignment: MA
TryHackMe | MAL: Malwa
VirusTotal - Home
https://tryhackme.com/room/malmalintroductory
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TryHackMe: Attacktive...
Task 5 Discussion of Provided Tools & Their Uses
Task 6 Connecting to 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
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)
Nay
Correct Answer
Does Virustotal report this MD5 Checksum / file Netlogo.exe as malicious? (Yay/Nay)
Answer format: ***
Submit
Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)
Answer format: ***
Submit
Woop woop! Your answer is correct.
intmal win20...
32m 39s


CSA-2_1: Assignment: MA
TryHackMe | MAL: Malwa
VirusTotal - File - 28b001
https://www.virustotal.com/gui/file/28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TryHackMe: Attacktive...
28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a
Sign in
Sign up
0 / 72
File distributed by Microsoft, Blender Foundation and others
Reanalyze
Similar
More
28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a
system_embedded_python_Lib_site-packages_setuptools_cli-64.exe
Size 73.00 KB
Last Analysis Date 7 hours ago
EXE
peexe assembly checks-disk-space detect-debug-environment idle long-sleeps via-tor 64bits known-distributor trusted
Community Score
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 24
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5 d2778164ef643ba8f44cc202ec7ef157
SHA-1 31eee7114eed6b0d2fb77c9f360505763905078 6
SHA-256 28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a
Vhash 074046655d155az51lz
Authentihash 53057dc2aa89f38b306ce21a928faa6d0b1c18a368171c3e7f7f87389f19c225
Imphash e694a8a11a715c6300d85bced2e15faa


CSA-2_1: Assignment: MA
TryHackMe | MAL: Malwa
VirusTotal - File - e86ee0
https://www.virustotal.com/gui/file/e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f56
90%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TryHackMe: Attacktive...
e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536
Sign in
Sign up
0
/ 72
Community Score
No security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536
NetLogo.exe
peexe assembly detect-debug-environment long-sleeps via-tor 64bits
Size
49.00 KB
Last Analysis Date
2 days ago
EXE
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5 59cb421172a89e1e16c11a428326952c
SHA-1 7583db73674f2340a3244b4e0dd9c0973e9899ff
SHA-256 e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536
Vhash 054066651d1515751az16hz13z27z35z
Authentihash c8235dfc442649b77f6629023269ff5739bffd46fb99226c35ecc0652212d522
Imphash 708060edc261af91104ef20847832bfb

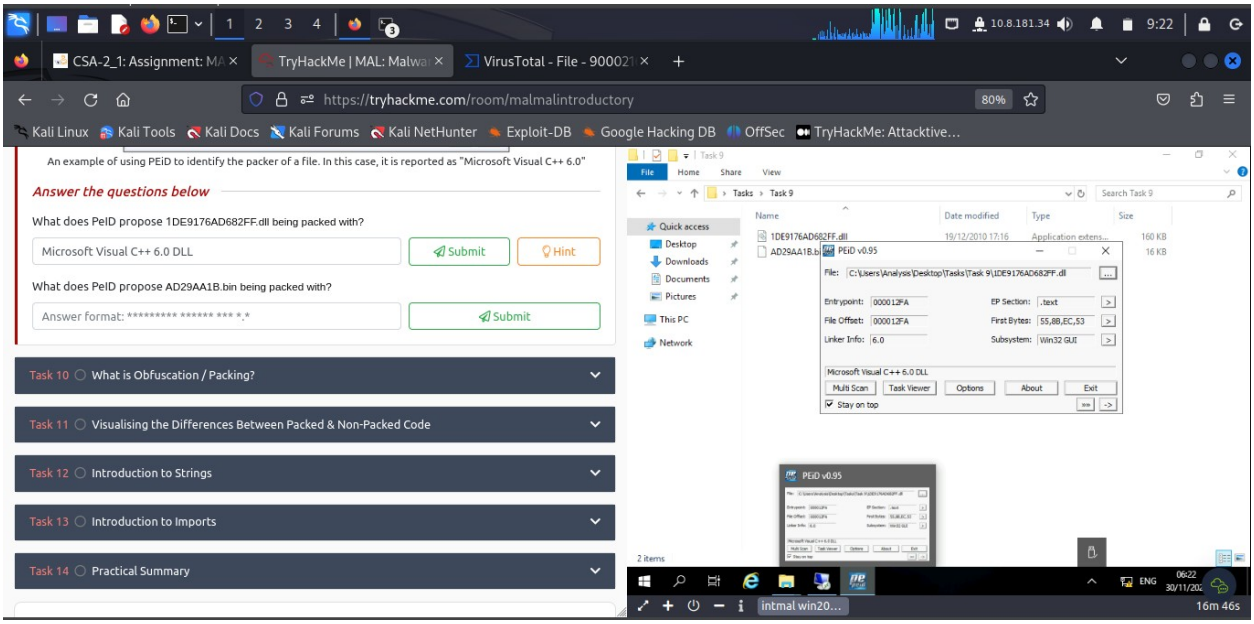

CSA-2_1: Assignment: MA
TryHackMe | MAL: Malwa
VirusTotal - File - e86ee0
https://tryhackme.com/room/malmalintroductory
80%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TryHackMe: Attacktive...
Task 7 Obtaining MD5 Checksums of Provided Files
Task 8 Now 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)
Nay
Correct Answer
Does Virustotal report this MD5 Checksum / file Netlogo.exe as malicious? (Yay/Nay)
Nay
Correct Answer
Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)
Answer format: ***
Submit
Task 9 Identifying if the Executables are obfuscated / packed
Woop woop! Your answer is correct.
NetLogo Properties
intmal win20...
28m 08s

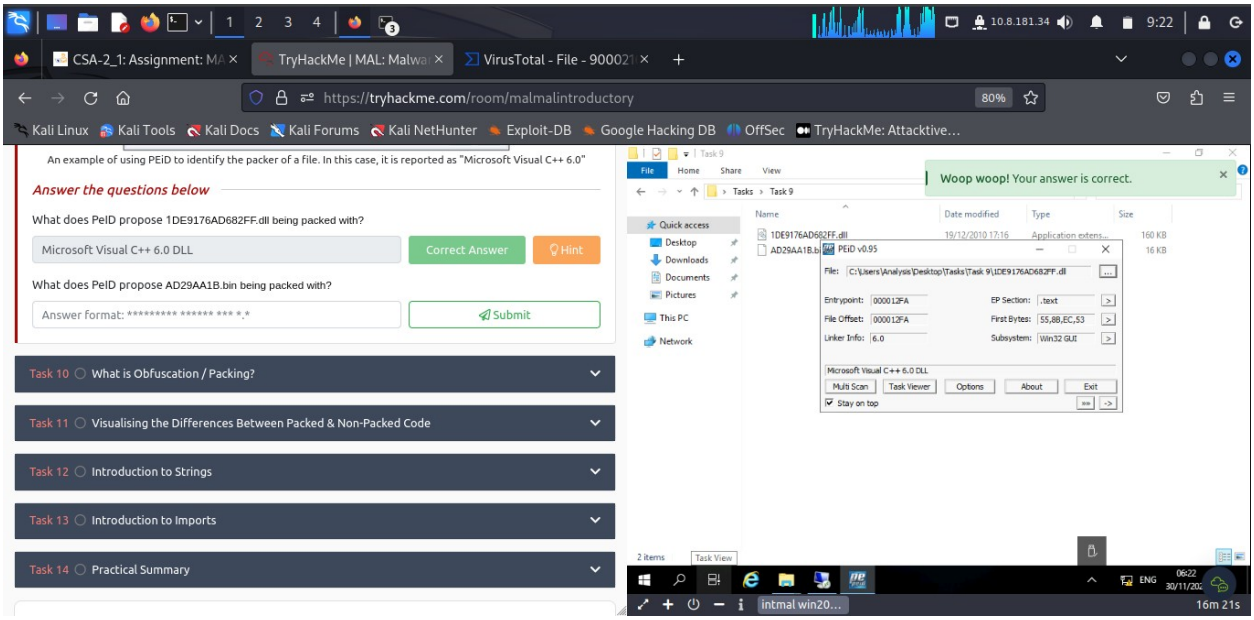


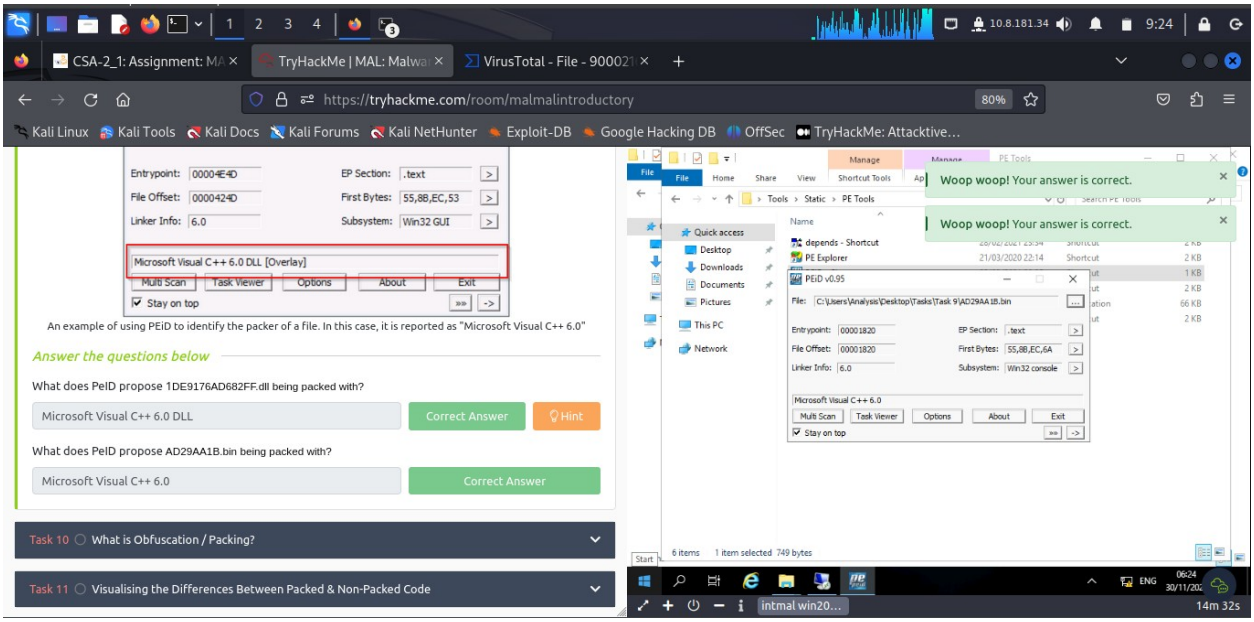


Task 9: Identifying if the Executables are obfuscated/packed

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.

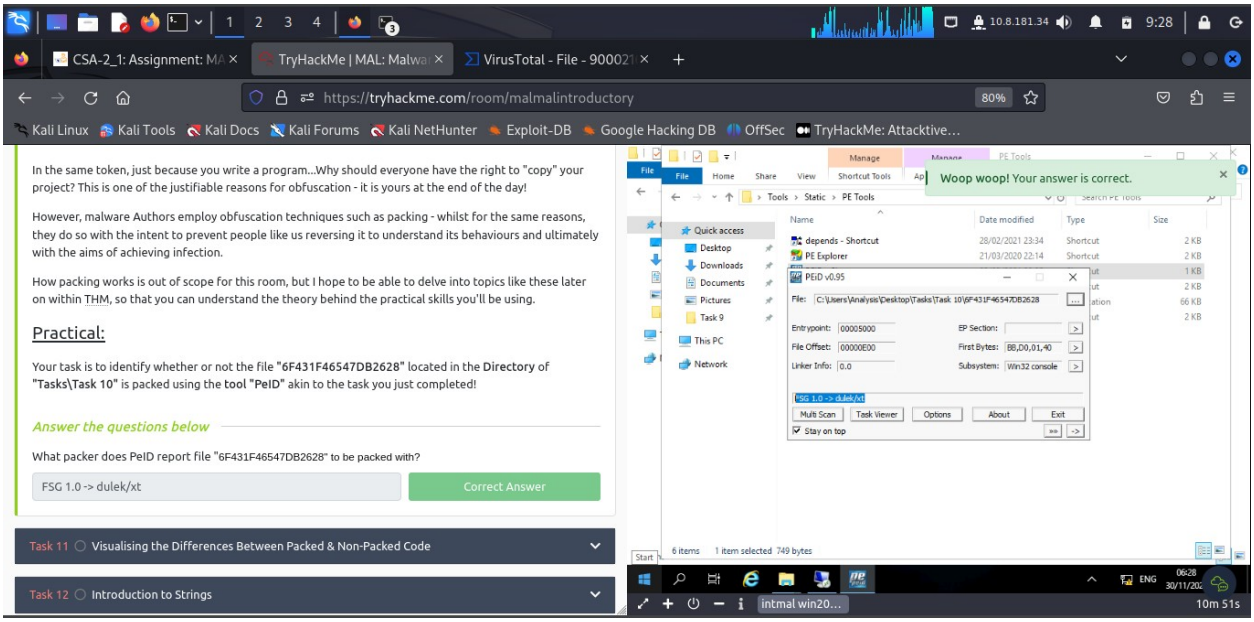

CSA-2_1: Assignment: MA
TryHackMe | MAL: Malwa
VirusTotal - File - 900021
https://tryhackme.com/room/malmalintroductory
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TryHackMe: Attacktive...
An example of using PEiD to identify the packer of a file. In this case, it is reported as "Microsoft Visual C++ 6.0"
Answer the questions below
What does PeID propose 1DE9176AD682FF.dll being packed with?
Microsoft Visual C++ 6.0 DLL
Submit
Hint
What does PeID propose AD29AA1B.bin being packed with?
Answer format: ********** ****** *** *.*
Submit
Task 10 What is Obfuscation / Packing?
Task 11 Visualising the Differences Between Packed & Non-Packed Code
Task 12 Introduction to Strings
Task 13 Introduction to Imports
Task 14 Practical Summary
PEiD v0.95
intmal win20...
16m 46s

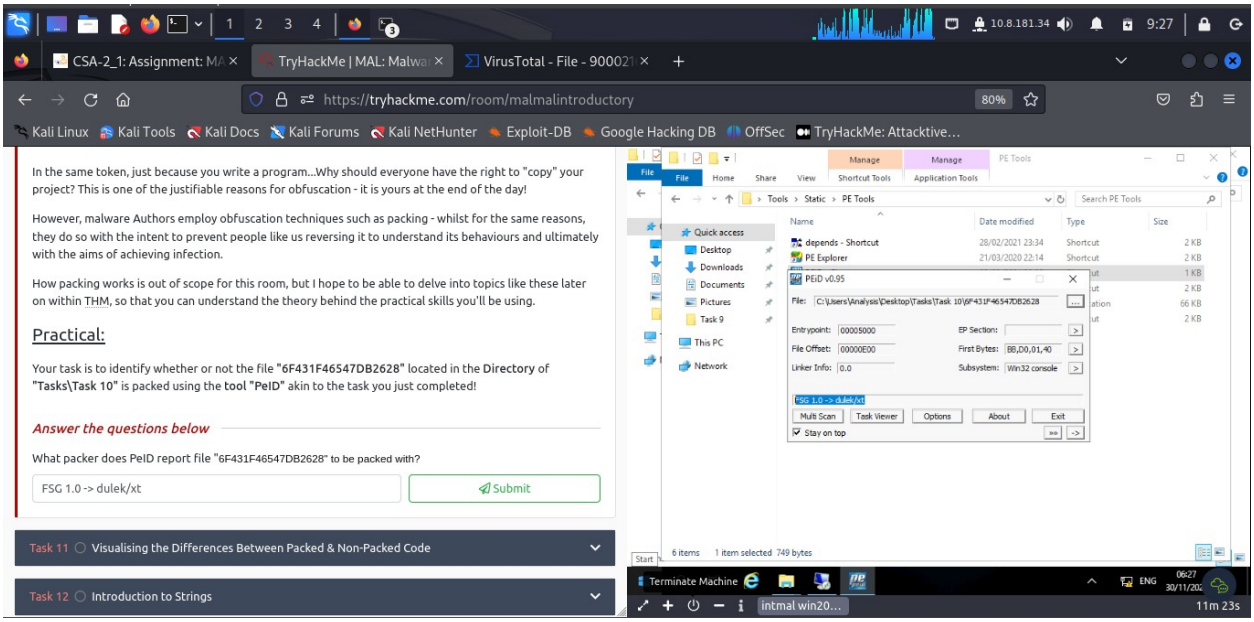

CSA-2_1: Assignment: MA
TryHackMe | MAL: Malwa
VirusTotal - File - 900021
https://tryhackme.com/room/malmalintroductory
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TryHackMe: Attacktive...
An example of using PEiD to identify the packer of a file. In this case, it is reported as "Microsoft Visual C++ 6.0"
Answer the questions below
What does PeID propose 1DE9176AD682FF.dll being packed with?
Microsoft Visual C++ 6.0 DLL
Correct Answer
Hint
What does PeID propose AD29AA1B.bin being packed with?
Answer format: ********** ****** *** *.*
Submit
Woop woop! Your answer is correct.
Task 10 What is Obfuscation / Packing?
Task 11 Visualising the Differences Between Packed & Non-Packed Code
Task 12 Introduction to Strings
Task 13 Introduction to Imports
Task 14 Practical Summary
PEiD v0.95
intmal win20...
16m 21s



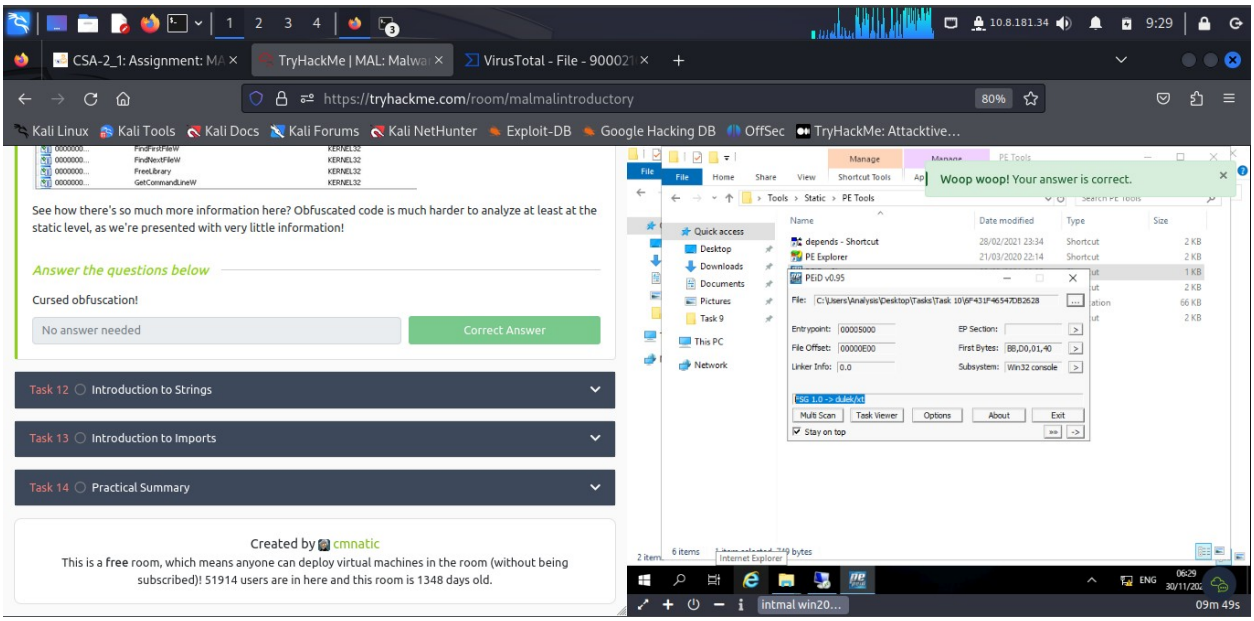
Task 10: What is Obfuscation/Packing

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



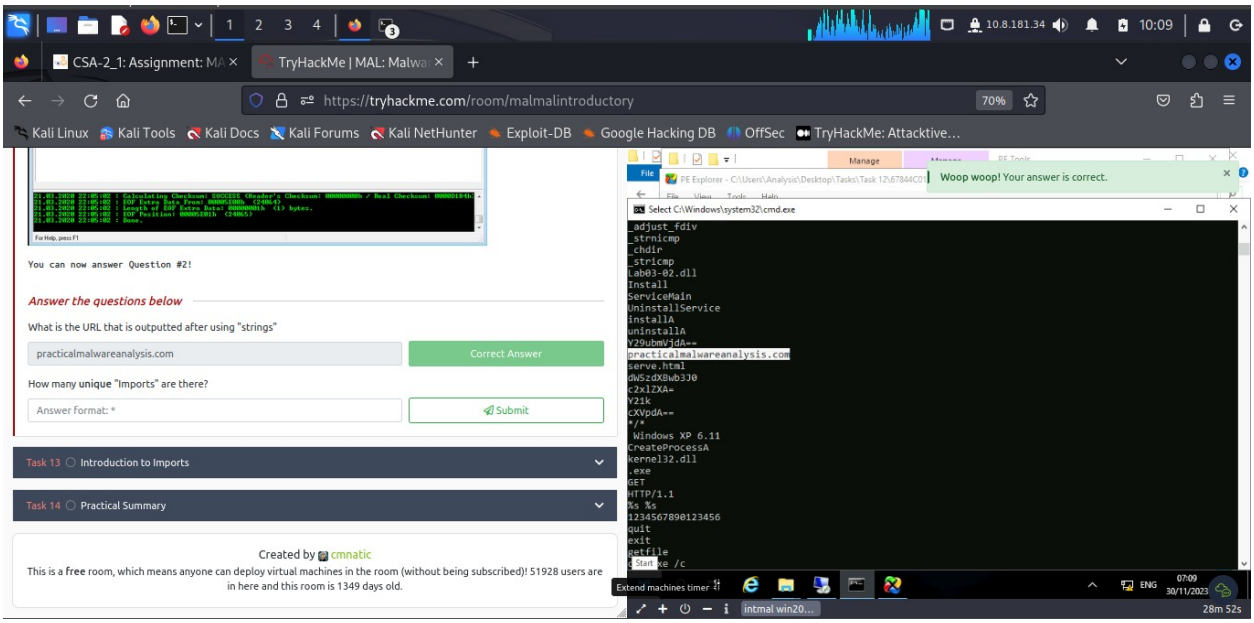


Task 11: Visualizing the Differences Between Packed & Non-Packed Code

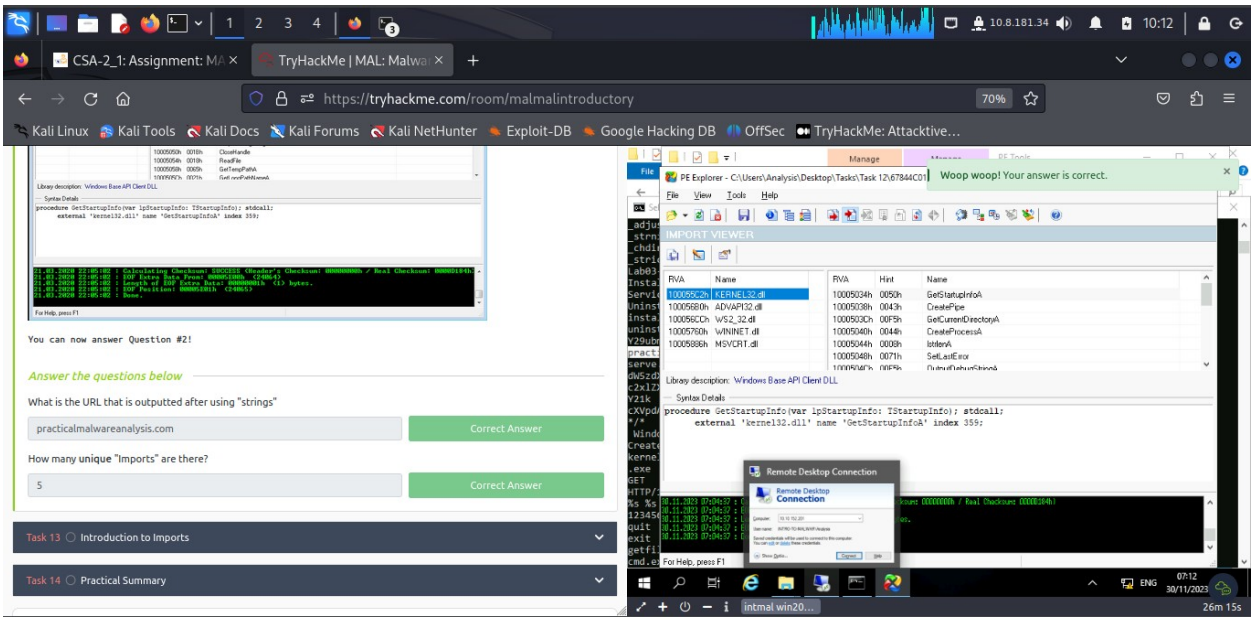


Task 12: Introduction to Strings

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

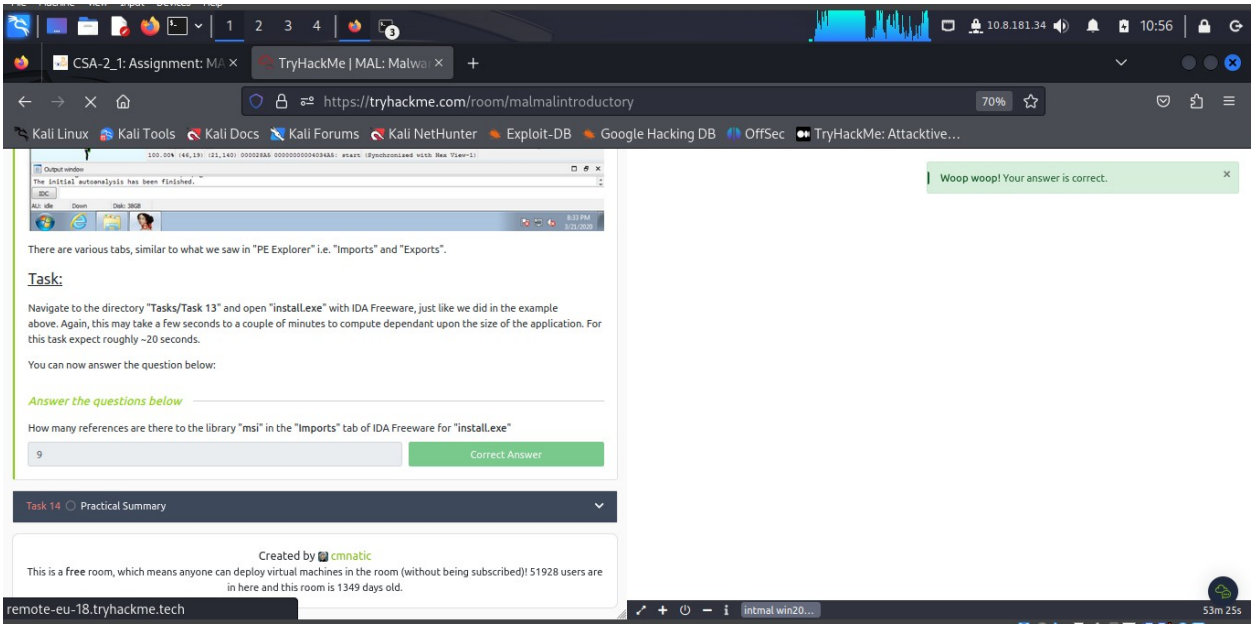


unique "Imports" available are **5**.

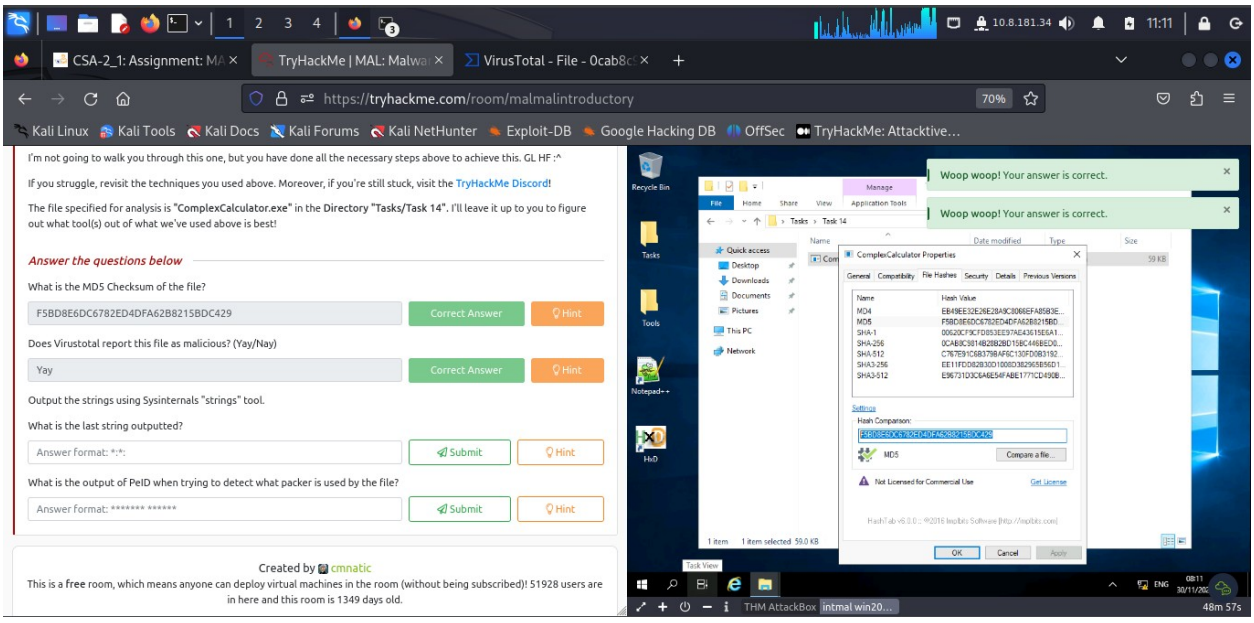


Task 13: Introduction to Imports

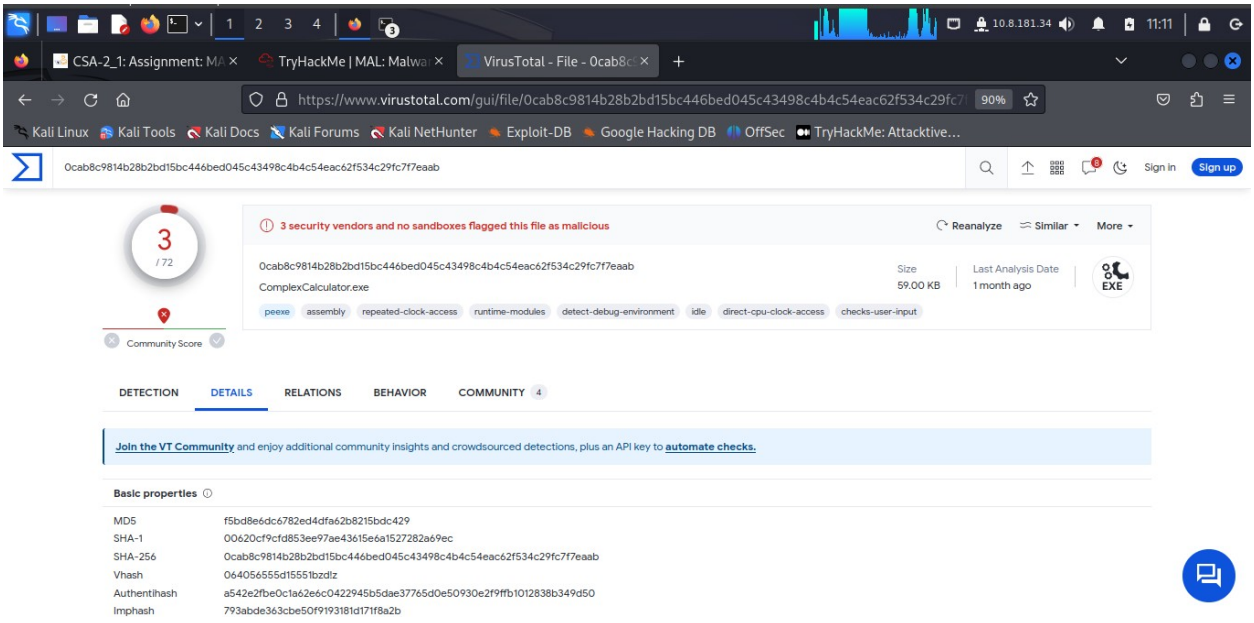
References available to the library "**msi**" in the "**Imports**" tab of IDA Freeware for "**install.exe** are **9**.



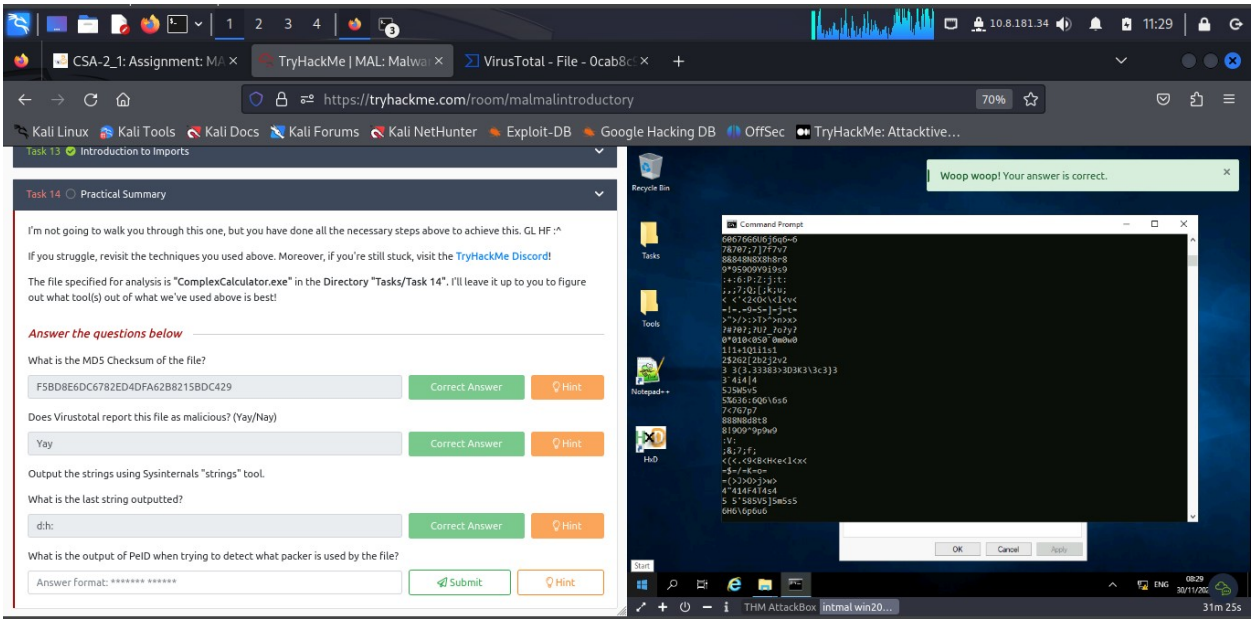
Task 14: Practical Summary



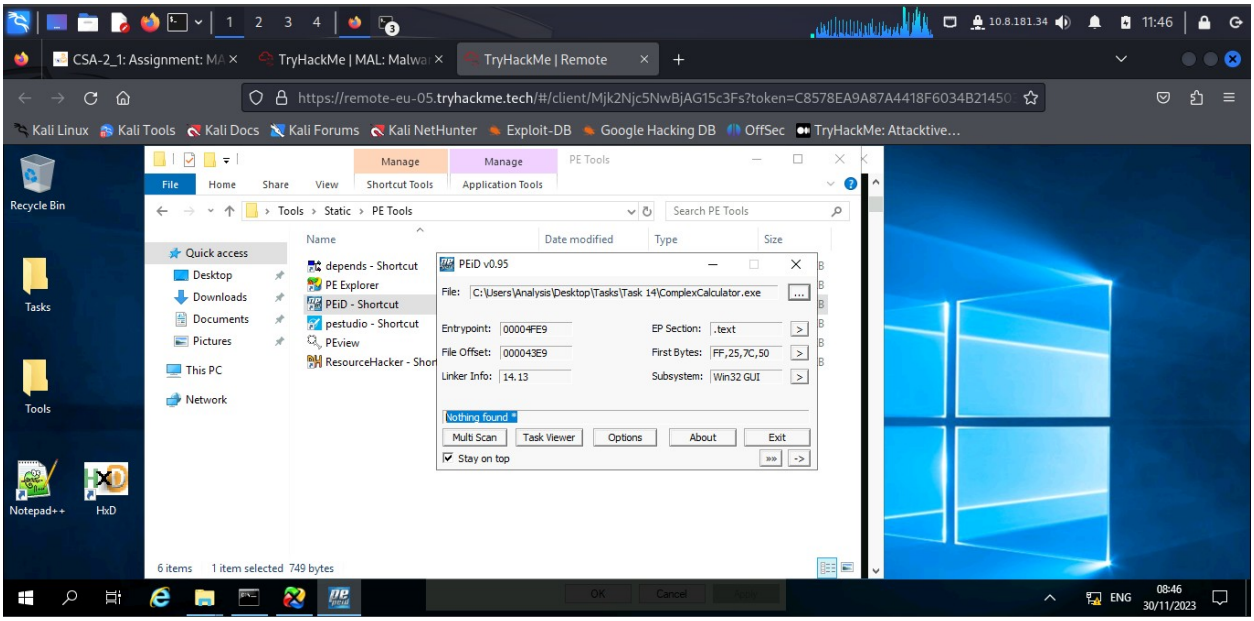
The Virustotal report this file as malicious, correct (**Yay**).

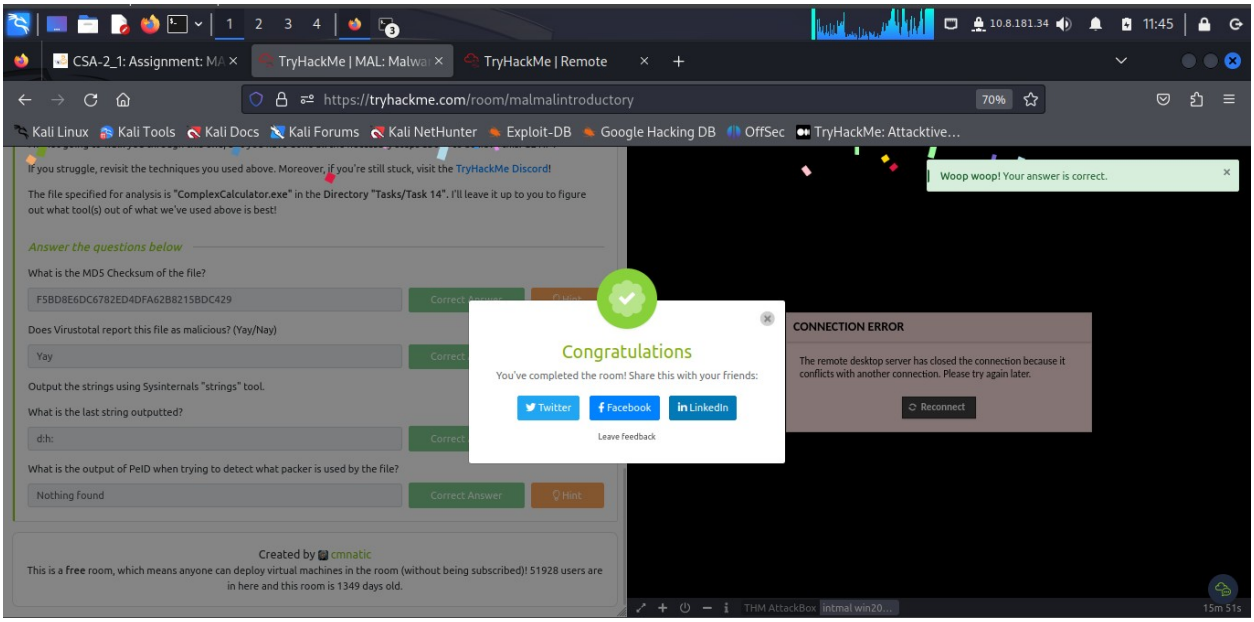


The last string outputted is **d:h:**



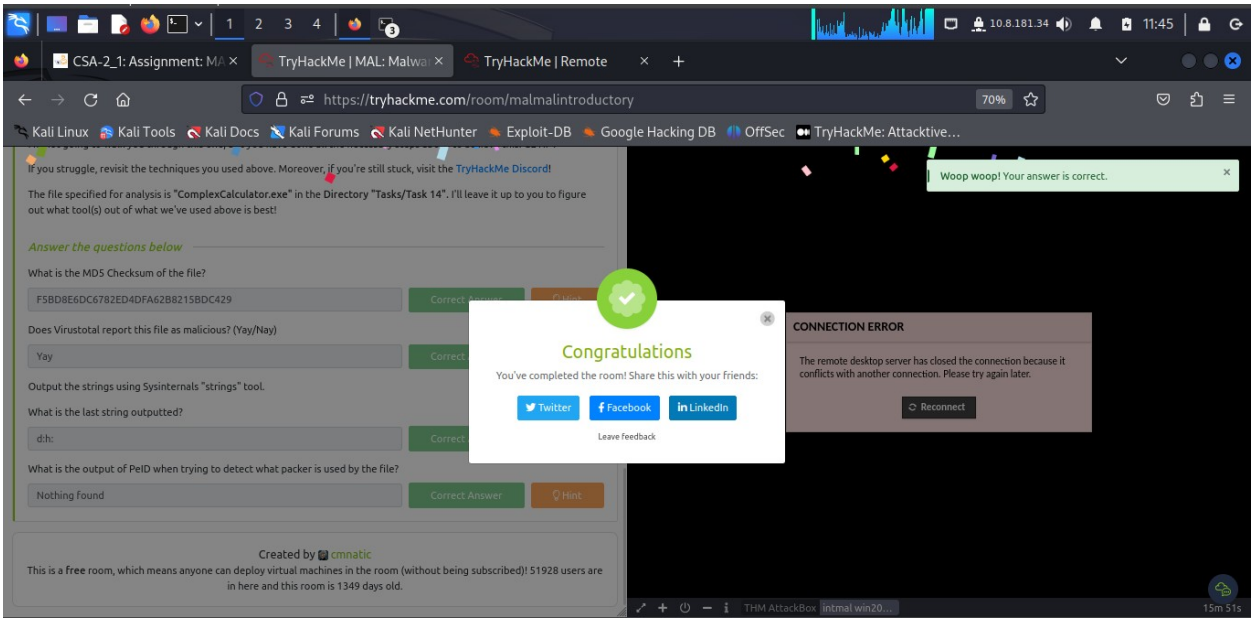
The output of PeID when trying to detect the packer used by the file is **Nothing found**.





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