TryHackMe: MAL: Malware Introductory Walkthrough

Malware Introductory TryHackMe Room Walkthrough - How to solve it.

February 22, 2021 · doreox

This room covers the basics and some tools used to perform Malware Analysis.

To access the room you can click here:
https://tryhackme.com/room/malmalintroductory

Task 1 - What is the Purpose of Malware Analysis?

No answer needed.

Task 2 - Understanding Malware Campaigns

1. What is the famous example of a targeted attack-esque Malware that targeted Iran?
   Answer: Stuxnet
2. What is the name of the Ransomware that used the Eternalblue exploit in a “Mass Campaign” attack?
   Answer: Wannacry

Task 3 - Identifying if a Malware Attack has Happened

1. Name the first essential step of a Malware Attack?
   Answer: Delivery
2. Now name the second essential step of a Malware Attack?
   Answer: Execution
3. What type of signature is used to classify remnants of infection on a host?
   Answer: Host-Based Signatures
4. What is the name of the other classification of signature used after a Malware attack?
   Answer: Network-Based Signatures

Task 4 - Static Vs. Dynamic Analysis

No answer needed.

Task 5 - Discussion of Provided Tools & Their Uses

No answer needed.

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

No answer needed.

Task 7 - Obtaining MD5 Checksums of Provided Files

1. The MD5 Checksum of aws.exe
   Answer: D2778164EF643BA8F44CC202EC7EF157
2. The MD5 Checksum of Netlogo.exe
   Answer: 59CB421172A89E1E16C11A428326952C
3. The MD5 Checksum of vlc.exe
   Answer: 5416BE1B8B04B1681CB39CF0E2CAAD9F

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

1. Does Virustotal report this MD5 Checksum / file aws.exe as malicious? (Yay/Nay)
   Answer: Nay
2. Does Virustotal report this MD5 Checksum / file Netlogo.exe as malicious? (Yay/Nay)
   Answer: Nay
3. Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)
   Answer: Nay

Task 9 - Identifying if the Executables are obfuscated / packed

1. What does PeID propose 1DE9176AD682FF.dll being packed with?
   Answer: Microsoft Visual C++ 6.0 DLL
2. What does PeID propose AD29AA1B.bin being packed with?

Answer: Microsoft Visual C++ 6.0

Task 10 - What is Obfuscation / Packing?

1. What packer does PeID report file “6F431F46547DB2628” to be packed with?
   Answer: FSG 1.0 -> dulek/xt

Task 11 - Visualising the Differences Between Packed & Non-Packed Code

No answer needed.

Task 12 - Introduction to Strings

1. What is the URL that is outputted after using “strings”
   Answer: practicalmalwareanalysis.com
2. How many **unique** “Imports” are there?
   Answer: 5

Task 13 - Introduction to Imports

1. How many references are there to the library “msi” in the “Imports” tab of IDA Freeware for “install.exe”
   Answer: 9

Task 14 - Practical Summary

1. What is the MD5 Checksum of the file?
   Answer: f5bd8e6dc6782ed4dfa62b8215bdc429
2. Does Virustotal report this file as malicious? (Yay/Nay)
   Answer: Yay
3. Output the strings using Sysinternals “strings” tool.
   What is the last string outputted?
   Answer: d:h:
4. What is the output of PeID when trying to detect what packer is used by the file?
   Answer: Nothing Found

TryHackMe

« PREV
TryHackMe: Nmap Walkthrough

NEXT »
TryHackMe: Introductory Networking Walkthrough