



IE2012 - Systems Network and Programming(2023/FEB).

Sri Lanka Institute of Information Technology.

Year 2 Semester 1

Individual Assignment - 2023

Nanayakkara Y.D.T.D

IT21826368

<https://tryhackme.com/room/malwarereverseengineering>

Journal : Reverse Engineering and Malware Analysis.

Contents

1. What is Reverse Engineering?.....	3
1.1. What is Malware Analysis and Reverse engineering ?	3
1.2. Importance of Malware Analysis and Reverse Engineering.....	3
1.3. Stages	4
2. Process of Learning and Development : Journal	4

Welcome! This is the journal I used to write objectives, challenges and others when creating the tryhackme room on malware analysis and reverse engineering.

1. What is Reverse Engineering?

The process of analyzing a product, system, or technology to understand its design, functionality, and inner workings. It involves starting with the finished product and working backward to uncover the underlying principles, components, or code that were used to create it. The goal of reverse engineering is to gain knowledge about how something works, extract useful information, or create a replica or modified version of the original product.

Reverse engineering can be applied to various fields, including software, hardware, mechanical devices, and even biological systems.

Malware, short for malicious software, refers to any type of software or code specifically designed to cause harm, exploit vulnerabilities, or gain unauthorized access to computer systems, networks, or devices.

1.1. What is Malware Analysis and Reverse engineering ?

The process of analyzing and understanding malicious software, which referred as malware, with the goal of understanding its functionality, behavior and potential vulnerabilities.

Reverse engineering involves examine the code, structure and behavior of the malware to get an insight into its inner workings using tools like disassemblers, debuggers, de-compilers and network analyzers. Reverse Engineering and Malware Analysis Teach users about reverse engineering techniques and how to analyze malware samples to uncover their functionality and purpose. Scenario: Users must reverse-engineer a malware sample to identify its command and control server.

1.2. Importance of Malware Analysis and Reverse Engineering.

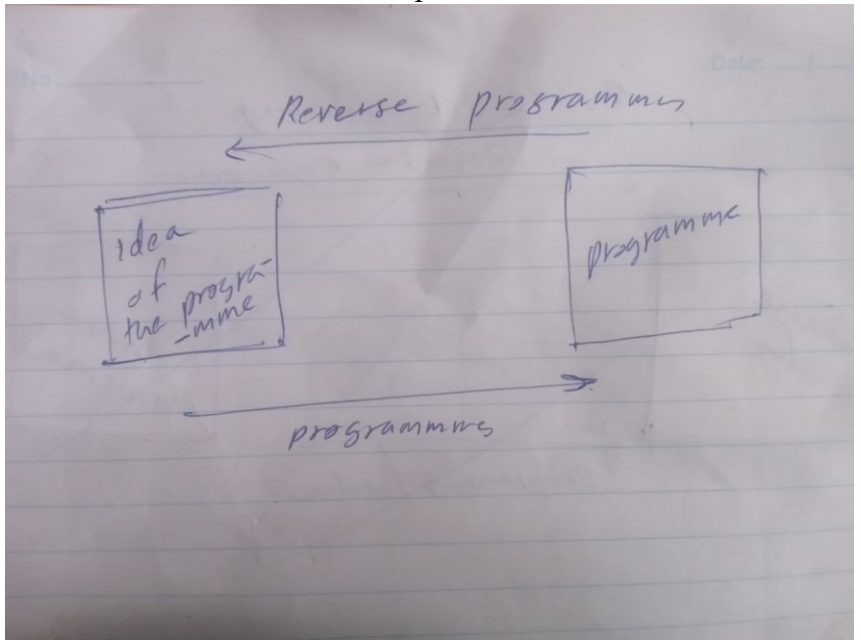
- Understanding the malware provides deep insights into inner working, behavior, and capabilities of malware and get a clear idea on nature of the threat we have to deal with.
- To build effective countermeasures for the malwares like antivirus signatures, intrusion detection rules, and firewall rules.
- To allow malware samples from extraction of indicators of compromise ((I.O.Cs). help to identify similar malware instances across network.
- To provide a response and forensics.
- For Security Research and innovation. leading to develop new advanced security solutions.

1.3. Stages

In malware reverse engineering there are steps we have to apply. they are;

1. Collection of the malware sample.
2. Creating an isolated controlled environment.
3. Conducting an initial analysis.
4. Conducting a static analysis.
5. Conducting a dynamic analysis.
6. Code reversing.
7. Documenting the malware's behavior.
8. Compare the analyzed malware with known samples and families.
9. Documenting the findings.

2. Process of Learning and Development : Journal

Date: 14/05/2023	Today's Goals	<ul style="list-style-type: none"> • Select the topic on creating the room. • Get an clear idea on the topic • Create the tryhackroom in the website.
	Goals Accomplished	<ul style="list-style-type: none"> • Topic selected. • Room Created. • I studied the clear idea on the topic.  <ul style="list-style-type: none"> •
	Challenges Faced	<ul style="list-style-type: none"> • when creating the room I was not familiar with the tryhackme developer room. • I do not knew the topic that much
	Solutions Developed	<ul style="list-style-type: none"> • Find it from documentations and watched some youtube videos • Researched using some websites, Archive.org, Commitees.

	References	<ul style="list-style-type: none"> • Tryhackme.com. • Youtube.com
Date: 16/05/2023	Today's Goals	<ul style="list-style-type: none"> • Acquiring more knowledge on malware analysis and reverse engineering. • Downloading the malware from a trusted source. • Implementing a isolated environment to contain the malware.
	Goals Accomplished	<ul style="list-style-type: none"> • Downloaded an elf file (linux). • Found malware sample library. • Implemented it on the VM.
	Challenges Faced	<ul style="list-style-type: none"> • Finding a trusted malware sample library • Implementing a controlled Virtual machine.
	Solutions Developed	<ul style="list-style-type: none"> • Research about the libraries. • Use virtual box for the implementation.
	References	<p>Computerphile :</p> <ul style="list-style-type: none"> • Reverse Engineering : https://youtu.be/9tZmSFjoOm4 • Malware : https://youtu.be/qjZuI0FT9Z8 • Malware and ML : https://youtu.be/rjYUeh3tlpc • Malware Library : bazaar.abuse.ch
Date: 17/05/2023	Today's Goals	<ul style="list-style-type: none"> • Creating tasks . • Finding the steps. • Making questions.
	Goals Accomplished	<ul style="list-style-type: none"> • Task were completed. • Some questions were made but not complete.
	Challenges Faced	<ul style="list-style-type: none"> • When creating the tasks I had the question on correct steps. • Creating questions for the basic was too complex.
	Solutions Developed	<ul style="list-style-type: none"> • See from the other rooms and got an idea. • Tasks were made using some YouTube tutorials and analysis reports.
	References	<ul style="list-style-type: none"> • https://www.malwarebytes.com/what-was-the-mirai-botnet
Date: 18/05/2023	Today's Goals	<ul style="list-style-type: none"> • Static analysis • Linux commands
	Goals Accomplished	<ul style="list-style-type: none"> • Created the static analysis part

	Challenges Faced	<ul style="list-style-type: none"> Steps and how to find the proper commands
	Solutions Developed	Had no solutions were made.
	References	<ul style="list-style-type: none"> https://intezer.com/blog/malware-analysis/elf-malware-analysis-101-initial-analysis/
Date: 19/05/2023	Today's Goals	<ul style="list-style-type: none"> Decompiling the code
	Goals Accomplished	<ul style="list-style-type: none"> Decompiled the code using a de-compiler. Tasks were completed.
	Challenges Faced	<ul style="list-style-type: none"> Understanding the ghidra interface. How to read the files. Structures were beginner to me.
	Solutions Developed	<p>Read the documentation. Watched some tutorials. Read some articles.</p>
	References	Mosly the Ghidra.org and youtube were used.
Date: 20/05/2023	Today's Goals	<ul style="list-style-type: none"> Dynamic analysis.
	Goals Accomplished	<ul style="list-style-type: none"> Completed the task.
	Challenges Faced	<ul style="list-style-type: none"> How to create a proper controlled Virtual machine. How to run the files and same time analysis it. How to see file activity. How to see network activity. Finding the tools to use to analyze.
	Solutions Developed	<ul style="list-style-type: none"> Found tutorials from the internet sites, communities and my batch mates.
	References	<ul style="list-style-type: none"> https://blogs.cisco.com/security/indicators-of-compromise-and-where-to-find-them https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ https://youtu.be/i2I37T23mpI https://www.youtube.com/watch?v=ddLB8A1ai_M
Date:	Today's Goals	<ul style="list-style-type: none"> Finalizing.

21/05/2023		
	Goals Accomplished	<ul style="list-style-type: none"> • None.
	Challenges Faced	<ul style="list-style-type: none"> • Faced some problems on the TryHackMe uploading section.
	Solutions Developed	<ul style="list-style-type: none"> • Contacted the support.
	References	None.
Date: 22/05/2023	Today's Goals	<ul style="list-style-type: none"> • Finalizing
	Goals Accomplished	None.
	Challenges Faced	<ul style="list-style-type: none"> • Files and images were not saved by the TryHackMe. • Have to redo it more than 3 times over and over.
	Solutions Developed	<ul style="list-style-type: none"> • No solutions were found.
	References	None.
Date: 24/05/2023	Today's Goals	<ul style="list-style-type: none"> • Finalizing • Completing the journal
	Goals Accomplished	<ul style="list-style-type: none"> • Room created
	Challenges Faced	<ul style="list-style-type: none"> • When uploading the Virtual machine it doesn't convert and be ready to use • Had to find solutions.
	Solutions Developed	<ul style="list-style-type: none"> • Emailed them did not got the answer • Uploaded as downloaded file
	References	None.

In the beginning I had no idea what I was doing on the assignment and the topic. When i began to study on them I understood more and more. I used the malware analysis and reverse engineering as the topic on my own interest about that sections. As Cybersecurity students we must start on those get a clear idea of everything when it comes to understanding or learning something. From the challenges I faced mostly the Virtual Machine

converting problem was the one that I had to postpone the whole assignment. There were said in discord server about their effort in fixing it but, I had to use the downloadable option because of the assignment deadline. Other than that this assignment was fun to do, I learned a lot about every section I was in.