LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No. 4**

**A.1 Aim:**

(A) To study AnyRun/Hybrid/Akamai or any online sandbox tool

(B)To carry out malware analysis using AnyRun /Hybrid or any online sandbox tool

**A.2 Prerequisite:**

Basics of malicious softwares, viruses, Trojan.

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** Appreciate the importance of malware analysis

**A.4 Theory:**

***Sandbox :*** In the world of cybersecurity, a sandbox environment is an isolated virtual machine in which potentially unsafe software code can execute without affecting network resources or local applications. Cybersecurity researchers use sandboxes to run suspicious code from unknown attachments and URLs and observe its behavior.

[***Malware analysis***](https://www.sentinelone.com/cybersecurity-101/malware-analysis/?utm_target=dsa-19959388920&utm_device=c&utm_medium=paid-search&utm_source=google&utm_campaign=15096095517&utm_content=557000860213&gclid=CjwKCAiArOqOBhBmEiwAsgeLmfRUKVMRxxaz2b1u0TzDERMV6gtlvc7pqw9pcLeOql9BSMXVJJlTshoCfoMQAvD_BwE&utm_target=dsa-19959388920&utm_device=c&utm_medium=paid-search&utm_source=google&utm_campaign=15096095517&utm_content=557000860213&gclid=CjwKCAiArOqOBhBmEiwAsgeLmfRUKVMRxxaz2b1u0TzDERMV6gtlvc7pqw9pcLeOql9BSMXVJJlTshoCfoMQAvD_BwE) plays an essential role in avoiding and understanding cyber attacks. When incident response teams are brought into an an incident involving malware, the team will typically gather and analyze one or more samples in order to better understand the attacker’s capabilities and to help guide their investigation. As organizations deal with an increasing number of attacks and breaches, analysts are always looking for ways to triage and understand samples faster and more efficiently.

Any online sandbox tool can be explored.

<https://any.run/cybersecurity-blog/category/malware-analysis/>

app.any.run/docs/#What-can-I-use-ANYRUN-for

Example : <https://www.youtube.com/watch?v=e0vzBHEAzYc>

<https://www.hybrid-analysis.com/>

<https://learn.akamai.com/en-us/webhelp/enterprise-threat-protector/enterprise-threat-protector/GUID-FB14F4B8-045F-4C1F-8E10-B02E653510C0.html>

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)***

|  |  |
| --- | --- |
| Roll. No. A016 A018 A022 | Name: Varun K, Simran K, Kartik P. |
| Class: B.Tech CSBS | Batch: 1 |
| Date of Experiment: | Date of Submission: |
| Grade: | |

**B.1 Introduction about the suspicious files presenting for analyze by student:**

***1. Refer your experiment no. 1 suspicious file and analyze it on sandbox environment.***

***Or***

***2. Any kind of malware/Trojan/virus file and analyze it on sandbox environment.***

A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka "Windows VBScript Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.

**B.2 Input and Output:**

***(Paste your program input and output in following format, If there is error then paste the specific error in the output part. In case of error with due permission of the faculty extension can be given to submit the error free code with output in due course of time. Students will be graded accordingly.)***

**Input:**

Any of existing case.

<https://app.any.run/tasks/1163fe3b-7060-4d16-be54-05aa99202999/>

A screenshot of a computer screen

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated Graphical user interface

Description automatically generated A screenshot of a computer

Description automatically generated

**Output:**

Output screenshots

Graphical user interface, text, application

Description automatically generated



**B.3 Observations and learning:**

***(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)***

Hence, We were able to run the file containing Trojan Virus and was detect on ANY RUN Application.

Chart

Description automatically generated with medium confidence

**B.4 Conclusion:**

*(****Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.3)***

Hence we were able to perform the lab successfully with the detection of Trojan Virus on a HTML File with ASCII Text.

**B.5 Questions of Curiosity**

***(To be answered by student based on the practical performed and learning/observations)***

Q1: What is malware Analysis? And how it is performed?

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor. Malware or malicious software is any computer software intended to harm the host operating system or to steal sensitive data from users, organizations, or companies. Malware may include software that gathers user information without permission.

Stages of Malware Analysis:

1. Static Properties Analysis

Static properties include strings embedded in the malware code, header details, hashes, metadata, embedded resources, etc. This type of data may be all that is needed to create IOCs, and they can be acquired very quickly because there is no need to run the program to see them. Insights gathered during the static properties analysis can indicate whether a deeper investigation using more comprehensive techniques is necessary and determine which steps should be taken next.

2. Interactive Behavior Analysis

Behavioral analysis is used to observe and interact with a malware sample running in a lab. Analysts seek to understand the sample’s registry, file system, process, and network activities. They may also conduct memory forensics to learn how the malware uses memory. If the analysts suspect that the malware has a certain capability, they can set up a simulation to test their theory. Behavioral analysis requires a creative analyst with advanced skills. The process is time-consuming and complicated and cannot be performed effectively without automated tools.

3. Fully Automated Analysis

Fully automated analysis quickly and simply assesses suspicious files. The analysis can determine potential repercussions if the malware were to infiltrate the network and then produce an easy-to-read report that provides fast answers for security teams. Fully automated analysis is the best way to process malware at scale.

4. Manual Code Reversing

In this stage, analysts reverse-engineer code using debuggers, disassemblers, compilers, and specialized tools to decode encrypted data, determine the logic behind the malware algorithm  and understand any hidden capabilities that the malware has not yet exhibited. Code reversing is a rare skill and executing code reversals takes a great deal of time. For these reasons, malware investigations often skip this step and therefore miss out on a lot of valuable insights into the nature of the malware.