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 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.	Name:
Class	Batch:
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.

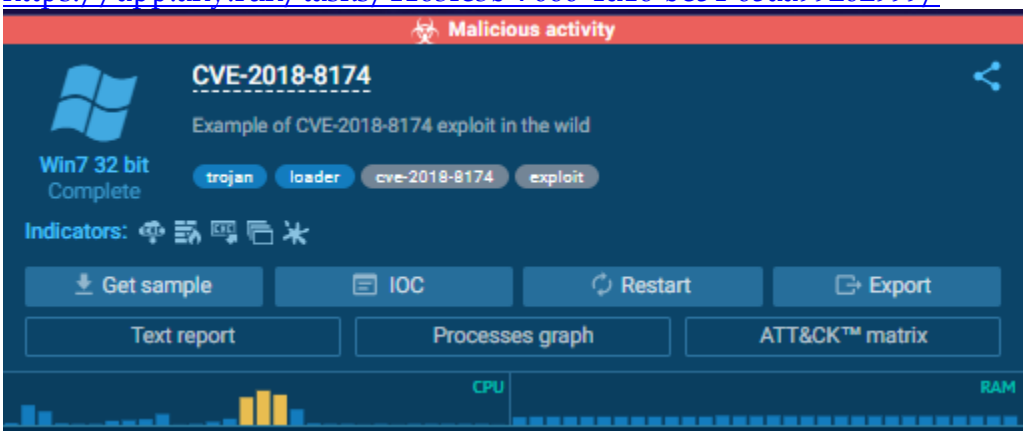
B.2 Input and Output:

(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.

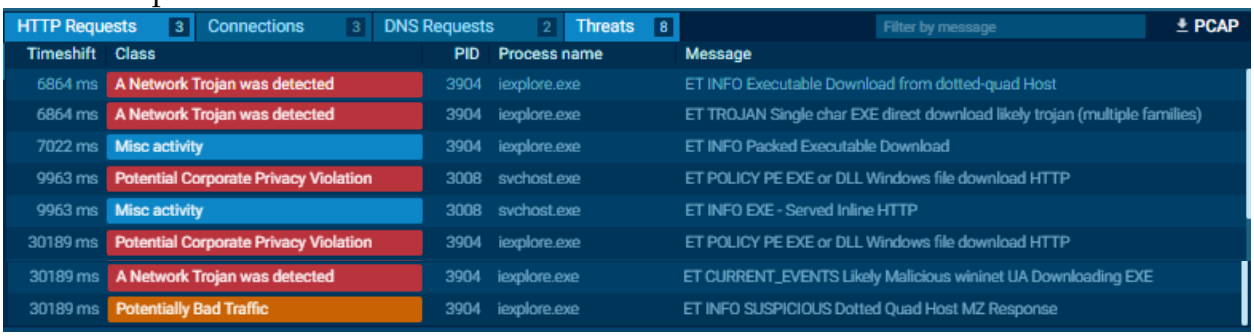
https://app.any.run/tasks/1163fe3b-7060-4d16-be54-05aa99202999/




Processes
Filter by PID or name
Only important
3472 iexplore.exe C:\Users\admin\Desktop\CVE_2018_8174.html
1k 175 74
3904 iexplore.exe SCODEF:3472 CREDAT:79873
1k 153 98
3008 svchost.exe PE
427 37 96
2968 puasy.exe PE
698 68 47
1920 taskkill.exe /f /im Steam.exe
182 3 82
3424 taskkill.exe /f /im Steam.exe
182 3 82
3744 taskkill.exe /f /im SteamService.exe
182 4 82
2280 taskkill.exe /f /im SteamService.exe
182 3 82
2776 taskkill.exe /f /im steamwebhelper.exe
182 4 82
2068 taskkill.exe /f /im steamwebhelper.exe
182 3 82
3536 taskkill.exe /f /im Client.exe
182 3 82
1400 taskkill.exe /f /im Client.exe
182 3 82
3420 taskkill.exe /f /im TslGame.exe
182 3 82
4068 taskkill.exe /f /im TslGame.exe
182 3 82

Output:

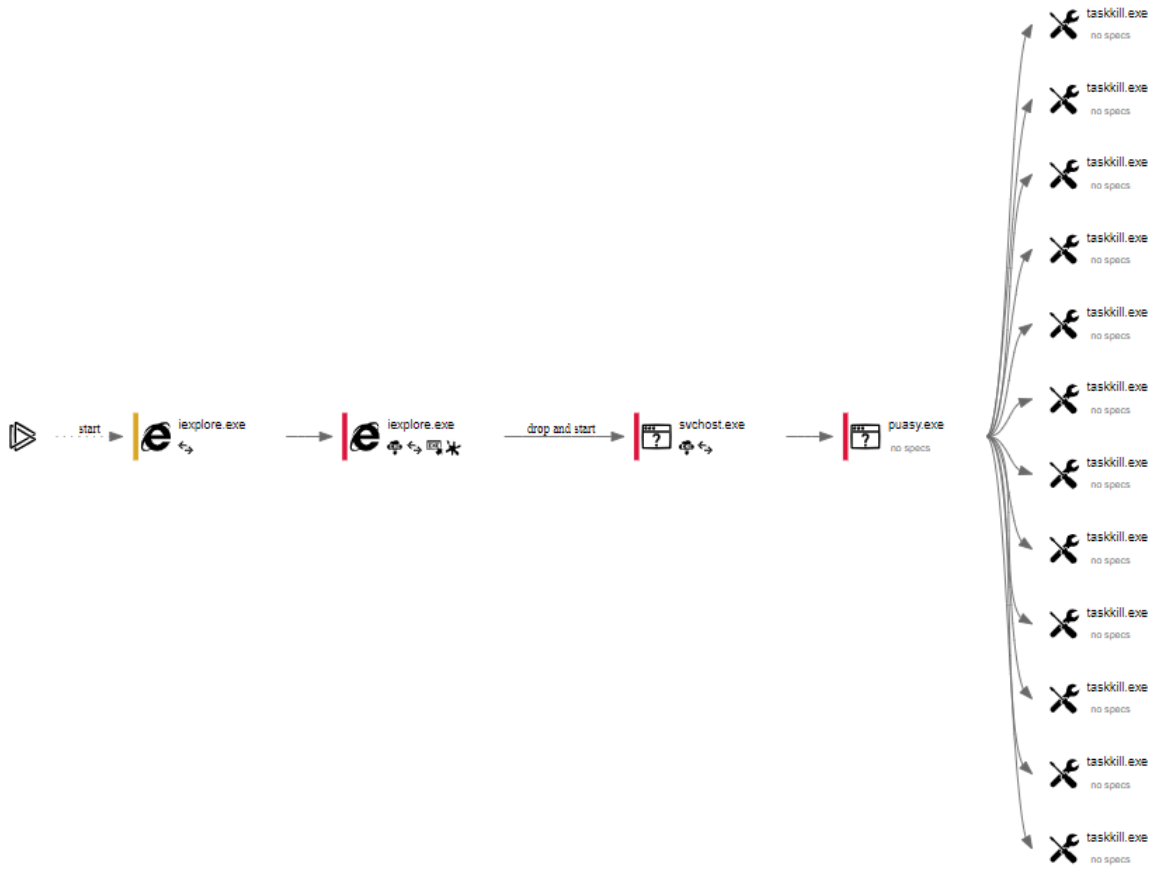
Output screenshots



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.



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?