LAB

5

Dynamic Malware Analysis Part 1

By the end of this section of the practical, you should be able to:

- Understand the techniques of dynamic malware analysis
- Used the tool to perform a dynamic analysis
- Interpret the output of dynamic analysis

5.1 Introduction

Dynamic Malware analysis is a process of analysing malware by executing the malware in an isolated environment and analyse it behaviour during the runtime. The aim of the analysis is to determine the function, behaviour and effect of the malware to the infected host. Dynamic analysis must be perform in a safe environment this is to ensure that the malware will not infecting the production machines. Any real machines must be airgapped**:** no network connection to the Internet or to other machines

Dynamic analysis tools to perform this analysis approach are:-

1. Process explore
2. Process Monitor (ProcMon)
3. Remnux
4. 2 virtual machine that have a windows XP and Remnux

Task 1

Dynamic Malware Analysis

This lab uses the files srvcp.exe (Caution: this is a live malware sample, handle it with care). Use the tools and techniques described in the chapter to gain information about the files and answer the questions below.

1. Setting up the analysis environment
    a. Open winxp x86 and Remnux in VMware
    b. Set the network configuration for the two guest OSes to be [Host Only] and set the network for each of the guest OSes with the setting below:-
        i. Winxp :
            - IP: 10.10.10.2/16
            - Gateway :10.10.0.254
        - Remnux:
            - IP:10.10.20.2/16
    c. Copy srvcp.exe in winxp
    d. Take Snapshot and name it as beforerunmalware
    e. Extract srvcp.exe (password will be given by instructor)
    f. Ping both guest OSes to check for connectivity
2. On Guest OS run Process explorer and ProcMon
3. On Remnux run wireshark and start capturing the network traffic
4. Run the extracted srvcp.exe.

5. Activate the process explorer and locate srvcp.exe, identify the process ID of the srvcp.exe.

6. Activate Procmon and click on filter menu. Filter the processes based on srvcp.exe process ID.

7. In Remnux Virtual Machine, start the irc server using terminal by using command ‘sudo inspircd start’ and observed the dns request from the wireshark output. Identify the domain request and the responses.

8. In the winxp Virtual Machine, go to C:/windows/system32/drivers/etc folder, edit files hosts by adding Remnux IP and the domain name obtain from Remnux’s wireshark at the end of the file e.g 10.10.10.20 www.XXX.com. Observed the changes happened in Remnux’s Wireshark output

9. Analyse and discuss the finding obtain from procmon and wireshark.

10. End your activity by restoring the snapshot beforerunmalware

Task 2

Dynamic Malware Analysis

With the help of task 1 analyse and report the behaviour of tnnbtib.zip. Do check the file to determine if the file is pack or not. Password(malware)