Lab activity for learning purposes

No submission required

Network services emulation for Malware Analysis

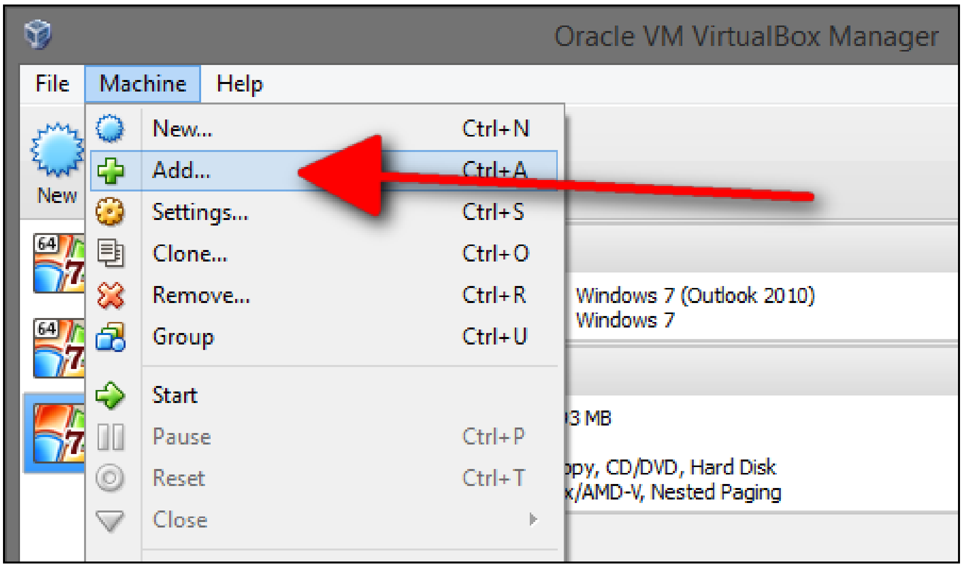
In this lab, you will perform dynamic analysis of some malware samples. Malware is often designed to communicate with external servers after infecting victim computers, in order to receive further command and control instructions, update itself, download further components, exfiltrate data etc. Because we are interested in exercising the malware to reveal as much of its network behavior as possible, it is necessary to provide the malware with emulated network services in a controlled environment.

Lab Setup

You should start with setting up a malware analysis lab by downloading and installing VirtualBox. Next, download the resources required for setting up the lab from the link below. These include two ready-made virtual machines (Windows XP and REMnux Linux). The malware samples have already been loaded in the XP machine.

Google Drive Folder

Download and extract both machine archives. Then in VirtualBox, use Machine > Add option to register both machines one by one.



Both VMs now need to be placed in an **isolated network**. Use the settings on the Virtual Box manager to change their network configurations from ‘NAT’ to ‘internal network’. Make sure that the network has the same name for both machines.

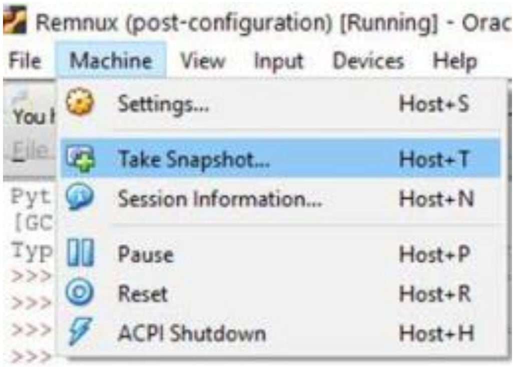
Next, on the XP machine, go to Control Panel > Network Connections > Local Area Connection > right click > properties > Select Internet Protocol (TCP/IP) > click ‘Properties’ button.

Configure the network interface with address 192.168.10.1, subnet mask 255.255.255.0, default gateway 192.168.10.2 and preferred DNS 127.0.0.1

On the Linux machine, use the following command to configure the interface with IP address 192.168.10.2. Here ‘`enp0s3`’ is the name of the network interface which can be found by using the command ‘`ifconfig`’.

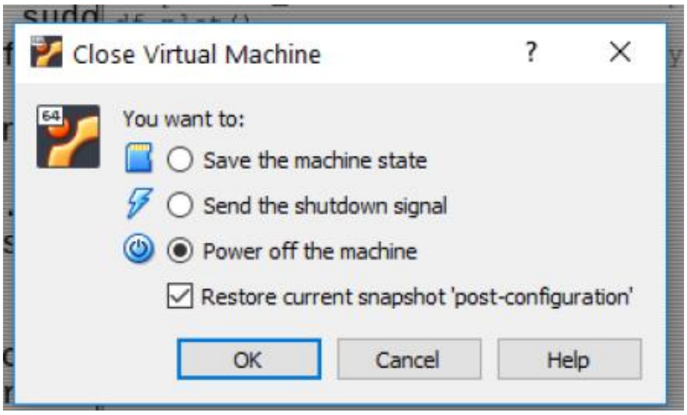
```
sudo ifconfig enp0s3 192.168.10.2 netmask 255.255.255.0 broadcast 192.168.10.255
```

After configuring both machines, create a snapshot of the current state of both of them. Go to ‘Machine’ menu on the VM:



Start Wireshark on the REMnux machine, open a command line terminal on the Windows VM and send ICMP packets to the machine (ping the linux machine from the windows machine). Verify the communications between the VMs from Wireshark’s packet capture.

Finally, clear up all operations performed since the last snapshot, which is a typical thing you should do during malware analysis to restore your analysis machine to a clean state (i.e. before the malware was executed). To return to the previous snapshot (which you took before sending packets between them), close the VM from the ‘X’ close button on the top right corner. A dialog box will come up that will allow you to check ‘Restore current snapshot…..’. When the VM restarts, it will return to the previous snapshot.



You want to:

○ Save the machine state

○ Send the shutdown signal

● Power off the machine

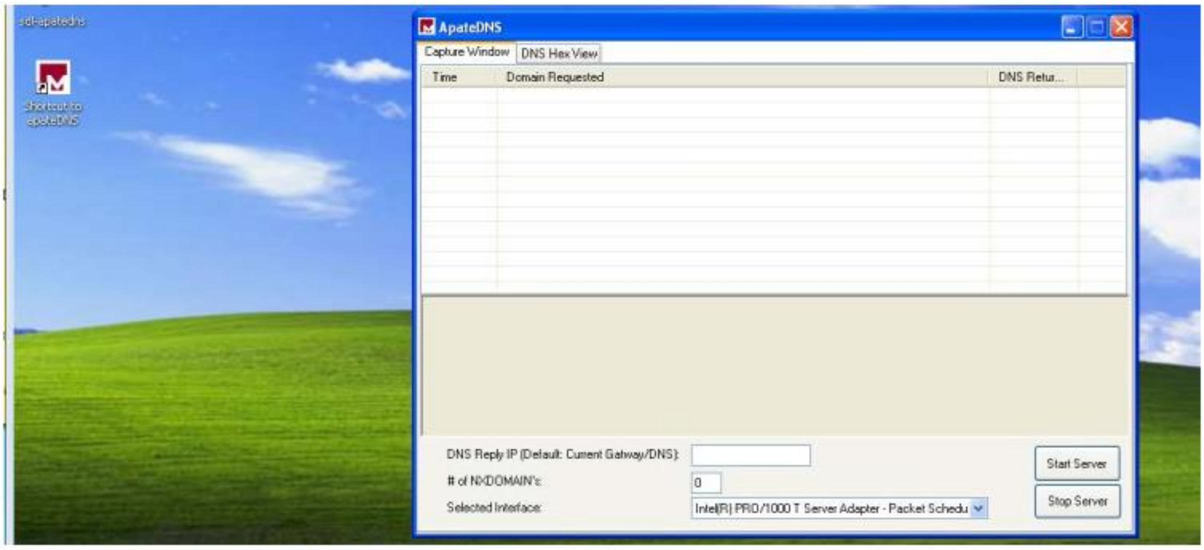
☑ Restore current snapshot 'post-configuration'

Analysis Preparation

Start both VMs and confirm connectivity between the two VMs (via pings).

On Windows XP, browse to Desktop > Tools > ApateDNS folder on and study the readme file to guide you on the tool's usage.

Press the 'Start server' button to start the ApateDNS listening on the localhost port 53. Make sure that the right network interface is selected from the 'Selected Interface' drop down menu. You can configure # of NXDOMAINS =0 in the first instance and then repeat the tasks with # of NXDOMAINS =3.



DNS Reply IP (Default: Current Gatway/DNS):
# of NXDOMAIN's: 0
Selected Interface: Intel(R) PRO/1000 T Server Adapter - Packet Schedu

On the REMnux machine, start iNetSim by typing at a terminal:

```
$ inetsim
```

Start Wireshark as well on the REMnux machine to capture packets on the network interface.

With ApateDNS, Wireshark and INetSim running, carry out the activities below and note/record any network behavior observed and tools have captured or logged. The INetSim logs can be found at:

```
$/var/log/inetsim/
```

The generated activity report for what has occurred during the iNetSim session is located at:

```
$/var/log/inetsim/report/
```

The report is saved in a file named in the format 'report.process_id.txt', after the session is closed. You may have to change file permissions in order to read it with your text editor.

Activities

Part-1: Using ApateDNS

1. Open a browser on the XP machine. Send a request for an image file from a hypothetical (or real) HTTP server. What happens when you do this?

2. Send another request for a web page through HTTPS. What do you notice?

3. Try downloading an executable (either .com or .exe file) from any website. What happens when you make this request?

4. On XP machine, there is a folder ‘Samples’ on the desktop, it contains a 7z file containing three malware samples. Extract the file (password: **infected**). Execute each of the samples and note/record their network behaviour as observed by you and/or logged with the tools.

   - Which domains are the samples trying to contact?
   - What http requests (if any) are being made and when do these requests occur?
   - From the logs, traffic capture and tool outputs, can you establish the sequence of events in the malware samples’ network activities?

Part-2: Using FakeNet

In this part, you will be using FakeNet instead of ApateDNS and INetSim, and therefore will not require the REMnux VM.

Close ApateDNS and revert your XP VM to a clean snapshot (before any malware was executed).

Locate FakeNet in the ‘Tools’ folder on the XP VM and run it. With FakeNet now launched and listening for DNS request on port 53, repeat all the activities your carried out with INetSim previously. Note all your observations (take screenshots). Execute each of the malware samples between snapshots and note down all your observations.

After executing each malware and observing its network behaviour as recorded by FakeNet, close the tool. When you close the tool, a PCAP file containing captured network traffic will be saved in the FakeNet folder.

Open the saved PCAP file in Wireshark to examine it (Wireshark portable is available in XP VM Tools folder).

Do your observations of the malware network behaviour with FakeNet match those of INetSim?

Compare and contrast the outputs that you have obtained from both tools.