IT Forensics Tutorial 8

Topics:

- Network Forensics Tools
  - Wireshark
- Network Security Device
  - Firewall
  - Source and Destination NAT

Covered Learning Outcomes:

- explain the motivations and landscape of network forensic investigations in an IT context
- become familiar with some of the network forensic tools
- deduce information and explain the events from captured traffic in a network forensic investigation

Instructions:

- Individual and group activities.

Files and access required:

- For this week's activity you need an account on https://www.hackthebox.eu. In order to join `hackthebox` you need to solve a hacking riddle. Give it a try however if you find it too difficult, there are guides and videos available online.
- lu16d-coremu-v1.3.ova virtual machine (username: `muni` and password: `muni`) available via:
  - **https://cloudstor.aarnet.edu.au/plus/s/vhxKjdq5Jmk8Fis**
  - See Appendix A for instruction on importing and setting up the VM

Activity A - Understanding Source and Destination NAT

Make sure you have setup a shared folder between your host (laptop or PC) and the Lubuntu virtual machine. Download the `IT_Forensics_w8.imn` file from moodle. This file is a CORE Network Emulator (henceforth core) configuration file. Start the Lubuntu virtual machine, open core, and from the File menu open the `IT_Forensics_w8.imn` file from the mounted shared folder inside the VM. In this setup `ns-argos` is the Authoritative Name Server for the domain `argos.edu`. The node `sphinx` is the Authoritative Name Server for the domain `delos.edu`. The node `Internet` serves as a DNS Cache Resolver between the two aforementioned domains

Tasks

1. Run the emulation and open a Wireshark window on the `eth0` interface of the node `Internet` (right click, move mouse over Wireshark and select `eth0`), another Wireshark window on `eth1` interface of the node `phoenix`, and the final Wirehark window on the `eth0` interface of the node `selene`. Open a terminal on the node `selene` and type the following command:

```
lynx www.delos.edu
```

Stop the capture in all three Wireshark windows. You can save these files for further analysis.

a) Open a terminal on node `Internet` and execute the following command:

```
ip route
```

Dose this node have any routes for the networks behind the node `phoenix`?

b) Observe the packets captured in all three Wireshark windows and explain how the node `selene` is able to visit the page hosted on the node `www-delos`. Can you make sense of this process? (Hint: some sort of NAT is being performed)

2. Close or minimise the Wireshark windows from previous sub task. Open a Wireshark window on `eth0` interface of the node `Internet`, and a second window on the `eth1` interface of the node `phoenix`. Open a terminal on the node `apollo` and enter the following command:

```
lynx www.argos.edu
```

a) Observe the packets in the two Wireshark windows and explain how the node `apollo` is able to visit the page hosted on the node `www-argos`. Can you make sense of this process? (Hint: some sort of NAT is being performed)

You can save these files for further analysis.

3. Stop the emulation, open the configuration window of the node `phoenix`, then locate `Firewall` service, click on the wrench icon to open the edit window. You will find 11 sets of commands. For each set briefly explain the purpose of the set of commands.

4. Does Source and Destination NAT have any relevance to network forensics investigations?

5. Install `nmap` tool using the following command:

```
sudo apt install nmap
```

Run the configuration. Open a Wireshark window on interface `eth2` of the node `phoenix`. Perform a port scan operation from the node `apollo` for the address range `10.1.3.40` to `10.1.3.60`. Share you observations with the class.

Activity B

Log in to your account on https://www.hackthebox.eu inside the VM and click on *Labs* (on the left pane) then *Challenges*, and then click on *Forensics* and open `MarketDump` challenge.

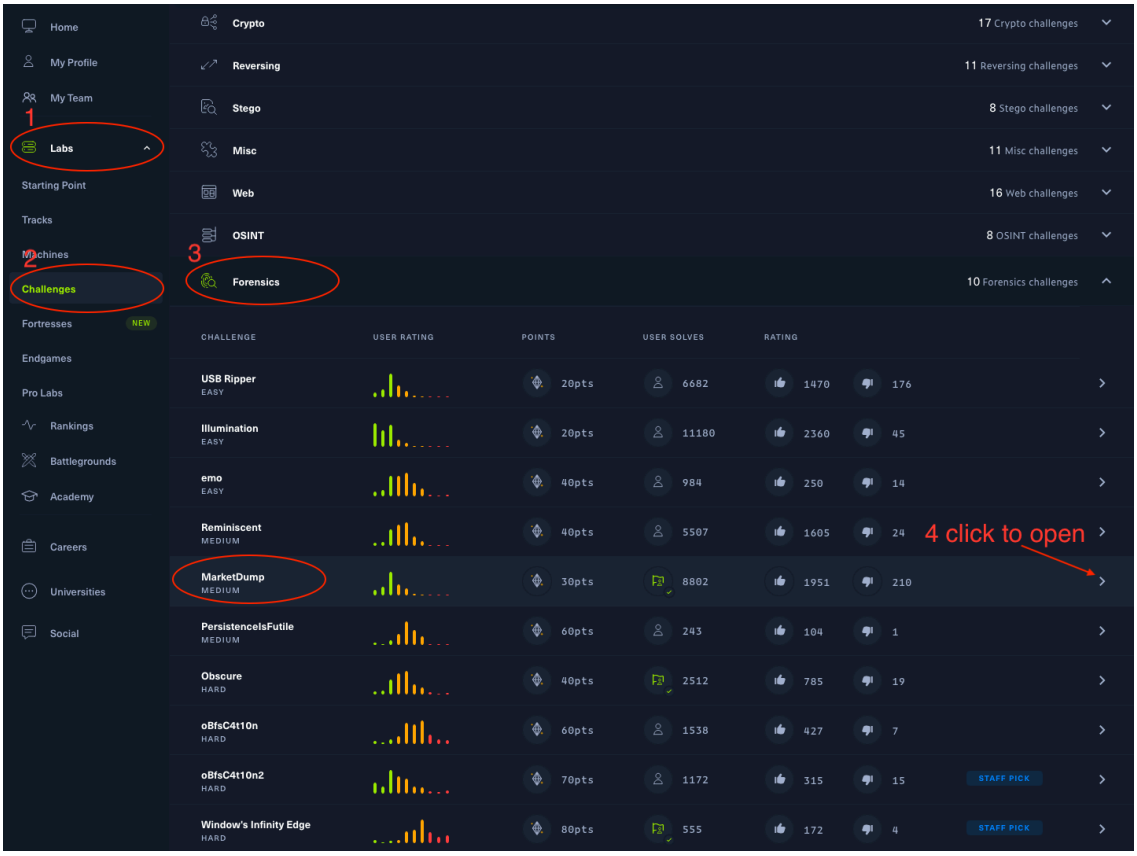

Figure 1: Log in to `hackthebox` and navigate to Labs → Challenges → Forensics → MarketDump

Read the description of the challenge and then download the zip file and extract the packet capture file. The password for the zip file is `hackthebox`. Open the `pcap` file in Wireshark.

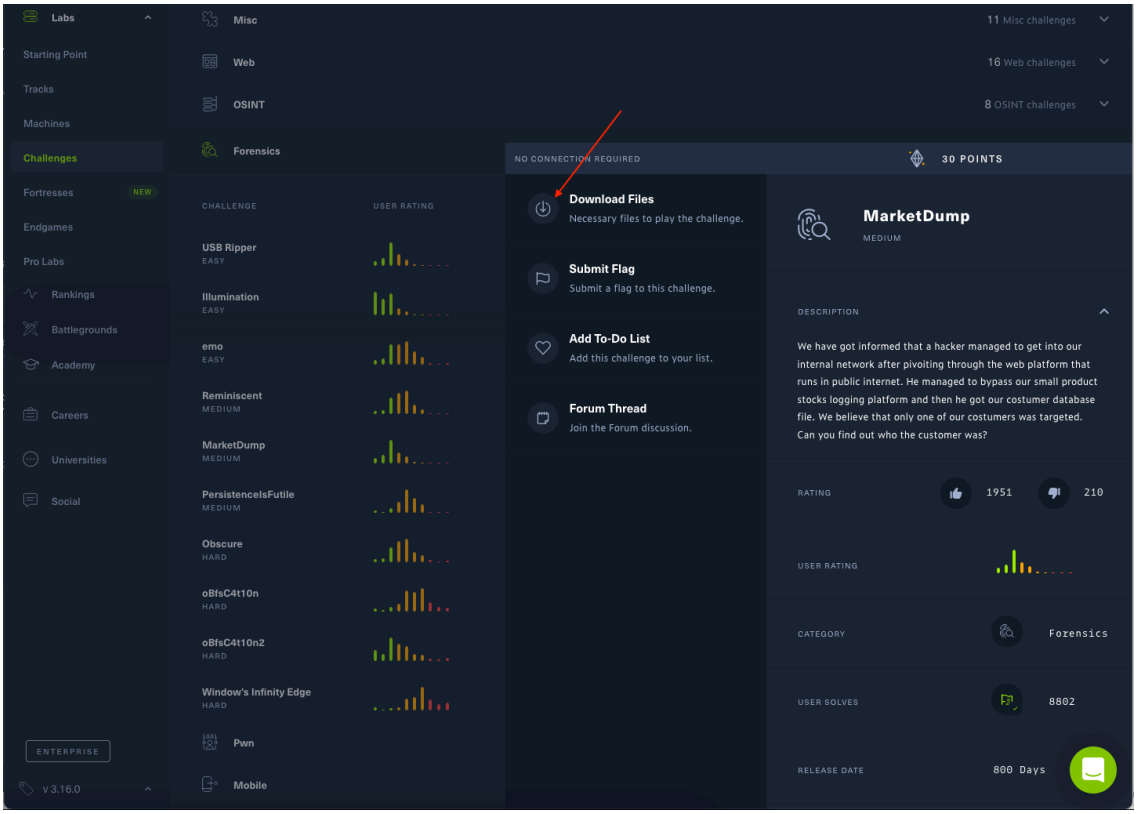

Figure 2: MarketDump challenge description and file download

Tasks

1. Can you explain how the attacker has identified a vulnerability in the target machine?
2. Can you identify the services running on the target machine? Try a display filter that shows server's `TCP SYN + ACK` response. Check out Building Display Filters for more advanced filters.
3. List all the TCP and UDP communications between the attacker and the server (Menu bar → Statistics → Conversations). Observe each TCP stream and identify interesting connections (from bytes exchanged).
4. Identify the protocol used by attacker to gain access to the server (identify the TCP Stream).
5. What program and command the attacker uses for persistent access to the server?
6. List all the commands the attacker has used after establishing a persistent connection.
7. Identify the flag of the challenge. To decode the flag go to https://gchq.github.io/CyberChef and select Magic from operations and paste the flag as Input and click on Bake.

Appendix A - Setup VM

Download and Install VirtualBox

- Download the *VirtualBox* from https://www.virtualbox.org. It is available for all three major platforms: Windows, macOS, and Linux.
- Follow the installation instructions for your operating system.

- Download the *VirtualBox Oracle VM VirtualBox Extension Pack* from the same web page (the file is read by VirtualBox and is the same for all platforms).
- Install the Extension Pack after you have successfully installed the VirtualBox. To install simply double-click it and it should open in VirtualBox dialogue and prompt for approval.

As VirtualBox installs various system drivers it will ask for administrative privileges.

Download and Import Prepared Virtual Machine

The VM contains required software used in lab exercises and or assignments. One such tool is the Core Network Emulator which allows to mimic complex network scenarios without the need for accessing physical equipment. In exercises related to operating system we can safely perform tasks which are contained in the VM without accidentally changing the state of the operating system that runs our physical machine. It also allows us to provide universal instructions and exercises that would work the same way for all students as they will be run within the VM.

- Download the VM file: lu16d-coremu-v1.3.ova
  - **https://cloudstor.aarnet.edu.au/plus/s/vhxKjdq5Jmk8Fis**
- The file is about 2.6 GB so it may take some time to download.
- There are two ways to import the file into VirtualBox:
  - Simply double click on the file and a dialogue box from VirtualBox should open up that will guide you through the importing process.
  - Open VirtualBox and then from the Menu Bar: **File** → **Import Appliance** → **Browse (find the file using the OS file browser)** → **Continue** → **Import**.

Set up a Shared Folder between VM and the Host

In this step you will configure a folder on your host machine (OS running on your physical device) to be shared with the VM (guest which runs a flavour/distribution of Linux). We can use the shared folder to transfer files between the host and guest.

1. Open VBox and select the imported VM (in Section-)
2. Right click on the VM and select **Settings** as shown in Figure-3

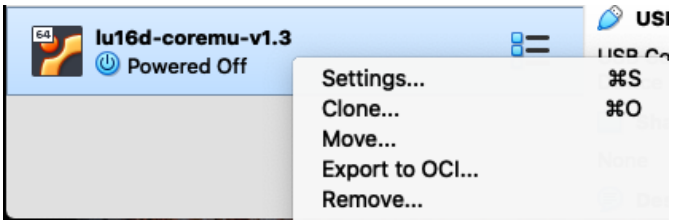

Figure 3: VM Settings - Method 1

An alternative approach is to select the VM and then click on the settings icon in the tools panel (Figure-4).

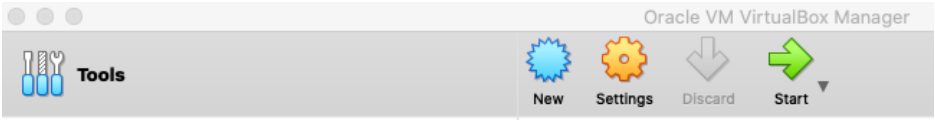

Figure 4: VM Settings - Method 2

3. Click on the **Shared Folder** icon in the settings window, then click on the folder icon with a green plus on the right side of the window to add a new shared folder (Figure-5)

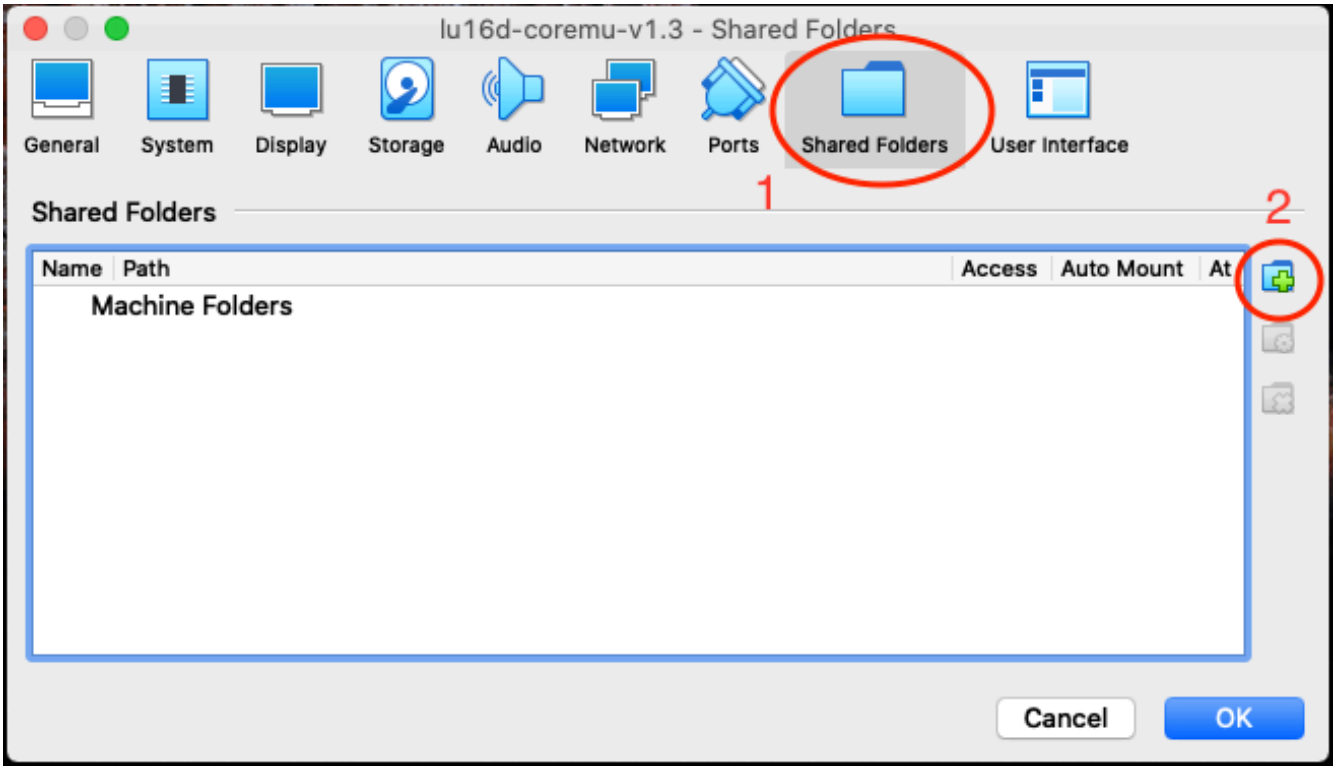

Figure 5: Adding a new shared folder

4. From the Folder Path in the opened window click on the drop down icon and select Other which will open the OS file browser to select a folder on your host machine to be shared with the VM. After selecting the folder check the Auto-mount option to make sure it will be mounted every time the VM is booted (the shared folder is presented as a network attached storage to the VM). Figure-6 shows my chosen Folder Path and Folder Name as well as the Auto-mount option.

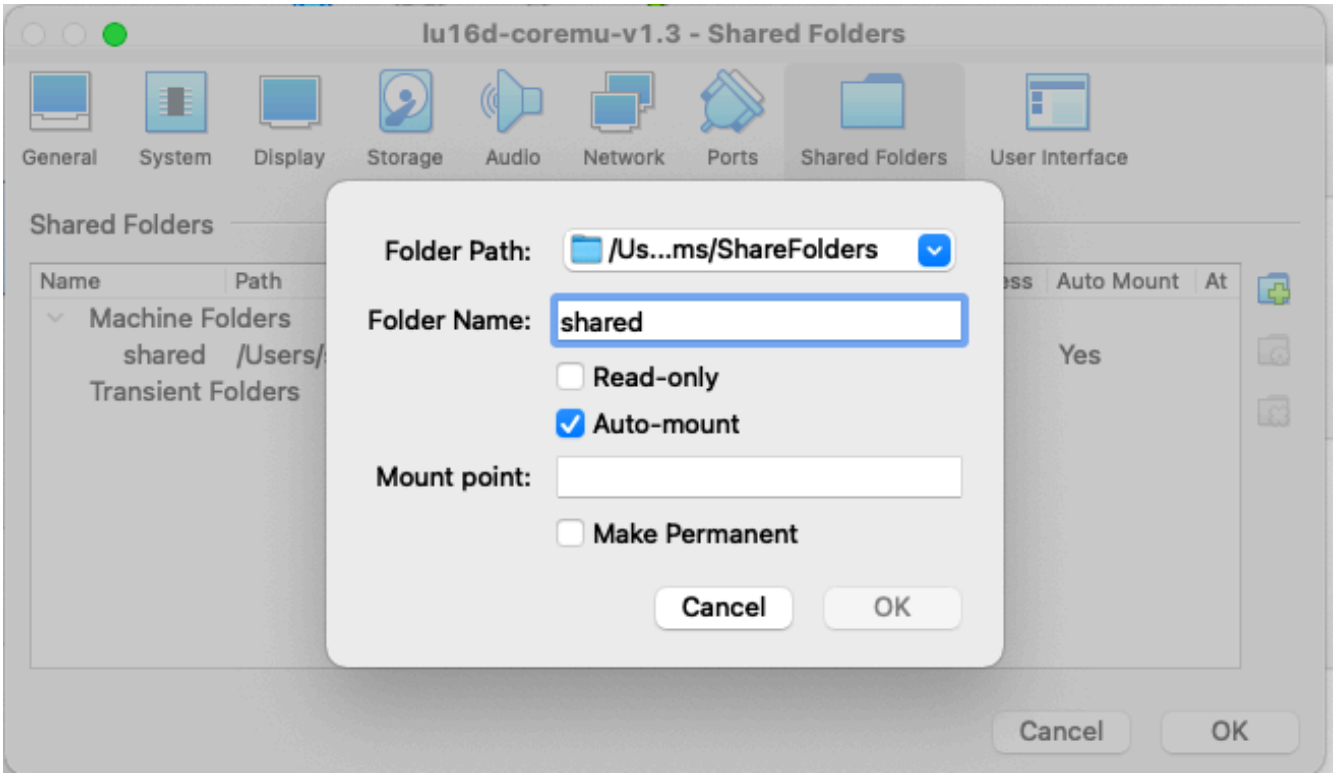

Figure 6: Selecting the shared folder and checking the Auto-mount option