Analysis Platform - Creation

Necessary Preparation for Malware and Reverse Engineering Workshop

DFRWS-EU, Oslo, Norway April 24th 2019

Introduction and Caution

In order to get the most out of the workshop and actively participate, you will have to bring your own computer preinstalled with a safe analysis environment.

How to create your analysis platform is described in this presentation.

This is a customized setup for this workshop, using older versions of some software for demonstration purposes.

NB! This workshop will examine and execute a live malware sample.

Quick Guide

1. Install VMware or VirtualBox
2. Download a win7 virtual machine (.ovf) from: https://filesender.uninett.no/?s=download&token=8a9af686-7267-4988-9ef7-b50f6d00f387
3. Download REMnux virtual machine (.ova) from: https://remnux.org/
4. Install and configure win7 virtual machine
    1. Open .ovf in VMware or VirtualBox (only one)
    2. Download and install IDA Freeware Version 5.0 on win7 machine from: https://www.scummvm.org/news/20180331/
    3. Disconnect from Internet
5. Install and configure REMnux virtual machine
    1. Open .ova in VMware or VirtualBox
    2. Run *update-remnux full*
    3. Disconnect from Internet
6. Connect both machines to the same virtual network and check (ping)
7. Take a snapshot (DFRWS_start) on both machines
8. Enjoy the workshop ☺

Detailed instructions on each step is provided next.

In case of any problems, please contact sergii.banin@ntnu.no

1) Install VMware or VirtualBox

We will use VMware (60 day trial license available), but VirtualBox will work as well.

2) Download a win7 virtual machine (.ovf)

3 files (DFRWS2019.mf, .ofv and .vmdk) can be downloaded from:
https://filesender.uninett.no/?s=download&token=8a9af686-7267-4988-9ef7-b50f6d00f387

This is a win7 machine preinstalled with malware and tools for the purpose of the tutorial in this workshop

3) Download REMnux virtual machine (.ova)

remnux-6.0-ova-public.ova can be downloaded from:
https://remnux.org/

This is a freely-available malware reversing and analysis utilities maintained by Lenny Zeltser and Davis Westcott

VMware
4) Install and configure win7 virtual machine

4.1. Open DFRWS2019.ovf in VMware

- Start VMWare
- *File-Open – choose DFRWS2019.ovf*
- Type in DFRWS2019 as a name and change storage path if needed.
- Press Import (may take a some time)
- Optional (if limited storage): Take a base Snapshot: VM- Take Snapshot, type in name DFRWS2019_BASE
- Power on the win7 virtual machine
- Close the Windows activation window.
- Click Restart now, if a windows with restart request pops up.
- Close the Windows activation window if needed.
- Right Click on the machines name (DFRWS2019) or click on VM menu
- Choose Settings-Hardware-Network Adapter.
- Make sure NAT is selected and tick on the “Connected” and “Connected at power on”. Click Ok.
- Now you should be connected to the Internet, needed to download IDA Pro free

VMWare - continued
4) Install and configure win7 virtual machine

4.2. Download and install IDA Freeware version 5.0 on win7 machine

- From inside the win7 machine, go to: https://www.scummvm.org/news/20180331/
- Download IDA Freeware Version 5.0
- When download is finished – install it. (create desktop icon, but don't launch it yet)

4.3 Disconnect from Internet

- Right Click on the machines name (DFRWS2019) or click on VM menu
- Choose Settings-Hardware-Network Adapter.
- Tick **off** the Connected and Connected at power on.
- Click Ok.

Optional! Take a snapshot. Name it DFRWS2019_IDA

VirtualBox (alternative)
4) Install and configure win7 virtual machine

4.1. Open .ovf in VirtualBox

- Open VirtualBox
- File – Import Appliance. Open the Win7 .OVF file provided..
- RightClick on the VM, select Display, Give 128MB of Video memory to this VM. Hit Ok.
- Create Snapshot. Start the VM. Right click on the Desktop. Choose higher resolution (at least 1024x768, the more – the better). Power off the machine. Take another snapshot.

4.2. Download and install IDA Pro free 5.0 on win7 machine

4.3. Disconnect from Internet

- Right click on the VM name – Settings – Network. Uncheck the Enable Network Adapter checkbox.

VMWare
5) Install and configure REMnux virtual machine

5.1. Open .ova in Vmware

- Start VMWare or go out of the win7 machine (DFRSW2019)
- *File-Open – choose remnux-6.0-ova-public.ova*
- Type in REMnux_DFRWS2019 as a name and change storage path if needed.
- Press Import (may take a some time)
- Optional (if limited storage): Take a base Snapshot: VM- Take Snapshot, type in name DFRWS2019_BASE
- Power on the machine

5.2. Run ***update-remnux full*** (may take some time)

- Sudo reboot when finished

5.3. Disconnect from Internet

- Right Click on the machines name (DFRWS2019) or click on VM menu
- Choose Settings-Hardware-Network Adapter.
- Tick **off** the Connected and Connected at power on.
- Click Ok.

Optional! Take a snapshot. Name it DFRWS2019_update

VirtualBox
5) Install and configure REMnux virtual machine

4.1. Open .ova in VirtualBox

- Open VirtualBox
- File – Import Appliance. Open the .OVA file provided..
- RightClick on the VM, select Display, Give 128MB of Video memory to this VM. Hit Ok.

4.2. Run *update-remnux full*

- Type *update-remnux full* in the terminal and hit enter. Update process may take some time.
- Sudo reboot when finished

4.3. Disconnect from Internet

- Right click on the VM name – Settings – Network. Uncheck the Enable Network Adapter checkbox.

Optional! Take a snapshot. Name it DFRWS2019_IDA

VMware
6) Connect both machines to the same virtual network

- **Create Virtual Network**
  - Goto Edit – Virtual Network Editor.
  - Click on Change Settings and click Yes.
  - Click Add Network. Select e.g. VMnet2. Click Ok.
- **Config**:
  Make sure the network is selected (e.g. VMnet2) and choose the following:
  - VMnet information: Select Host-Only.
  - Deselect “Connect a host virtual adapter…”
  - Select: “Use local DHCP services…”,
  - Subnet IP: 192.168.xxx.0 (write this down, xxx can be anything)
  - subnet mask 255.255.255.0.
  - Click Apply and Ok.
- **Connect**: For both Win7 and Remnux machines connect to this network.
  - Go to VM-Settings-Hardware-Network Adapter.
  - Network Connection, select Custom and the Network you created (e.g. VMnet2)
  - Choose Connected and Connected at power on.
  - *Click Ok. **(NB! repeat for both machines**)*

VirtualBox
6) Connect both machines to the same virtual network

- **Create** your own host-based network (File – Host Network Manager). Enable DHCP, use 255.255.255.0 mask for simplicity. Remember the IPv4 address of adapter.
- **Connect** your Windows and Remnux machines to this network.
- Right Click on the VM – Settings – Network. Choose Attached to: select the name of the host-based network you just created.

6) Check (ping)

Check IP address

- Win7:
  - Go to Start menu. Type cmd, hit enter.
  - Type ipconfig and hit enter.
  - IP address should be 192.168.xxx.zzz
  - xxx is same as Subnet IP used in Network editor from previous page
  - zzz can be anything
- REMnux
  - Type i*pconfig (or ifconfig)*
  - *IP address should be 192.168.xxx.yyy*
  - xxx is same as Subnet IP used in Network editor from previous page
  - yyy can be anything but is often is zzz+/- 1.
  - *If incorrect or missing, try to run renew-dhcp* command

Check connection

- Win7: Ping 192.168.xxx.yyy
- REMnux: Ping 192.168.xxx.zzz (ctrl c to stop)

6) Network configuration

On Win7 machine:

- Goto: Control Panel
  - Choose: Network and Internet - Network and Sharing Center – Change Adapter Settings
- Right click on Local Area Connection (should be only one)
- Choose: Properties
- Mark IPv4, choose Properties

- Set the following manually:

  Select: Use the following IP address
  - IP address: 192.168.xxx.zzz (IP address of Win7 machine)
  - Subnet Mask: 255.255.255.0
  - Default gateway: 192.168.xxx.yyy (ip address of REMnux machine)

  Select: Use the following DNS server address
  - Preferred DNS server: 192.168.xxx.yyy (ip address of REMnux machine)

- Ok - close
- Choose Public Network in the pop up menu.

NB! Not optional
7) Take a snapshot (DFRWS_start) on both machines

VMWare

- On win7: Close the cmd terminal unless already done
- Right Click on the machines name (DFRWS2019) or click on VM menu
- Choose Snapshot – Take Snapshot
- Name it DFRWS2019_start
- NB! repeat for both win7 and REMnux

Virtual Box

- Select VM. Click on the down arrow next to a Machine Tools button.
- Choose Snapshots.
- Press Take button.
- Name it DFRWS2019_start

8) Enjoy the Workshop

You should now have a clean image of both win7 and REMnux virtual machines called DFRWS_start as a necessary starting point for the workshop ☺

Welcome!