Cyber FIRE Malware Analysis Host Configuration

V 1.4 (9 February 2016)

This doc describes how to set up an environment that will be used for the Malware Analysis track. It can also serve as a base for your own analysis set up. Questions, comments, corrections, etc. should be sent to tf6e- malware@lanl.gov

Host Laptop Required

- If your host is anything other than a Linux flavor or a Windows version, consider yourself self-supported
- You will need either an 802.11n compatible radio, or an ethernet interface
- The host must be able to host 2 guest OSs in an isolated virtual network segment
- You must have VMWare Workstation (**Essential for snapshotting)**

Operating Systems Required

- Windows 7 32 bit – **Must be 32 bit**
- REMnux, found at https://remnux.org/

There are many options to emulate a network. If you already have a sandnet set up that includes windows 7 32 bit, you are welcome to use it (self-supported)

Building REMnux VM

- Download the .OVA at remnux.org
- In VMWare Workstation go to File → Open → remnux-6.0-ova-public.ova
- Follow the prompts to import the .Ova
- Install VMWare Tools on REMnux – this must be done manually
    1. On the top bar, click VM → Install VMWare Tools
    2. Open a terminal as root
    3. Mount the virtual CD
        - mount /dev/cdrom [space] /mnt/cdrom
    4. Change to a working directory
        - cd /tmp
    5. Note the filename of the VMWare Tools Installer
        - ls /mnt/cdrom
    6. Uncompress the installer
        - tar zxpf /mnt/cdrom/VMWareTools--x.x.x-yyyy.tar.gz
    7. Unmount the virtual cd
        - umount /dev/cdrom
    8. Open the VMWare Tools directory
        - cd vmware-tools-distrib
    9. Run the Installer
        - ./vmware-install.pl
    10. Hit enter a few times to accept defaults
    11. Restart the VM
- Optional: Install Bless hex editor – sudo apt-get install bless
- Snapshot and name “clean with tools” or something that makes sense to you

Building Windows 7 VM

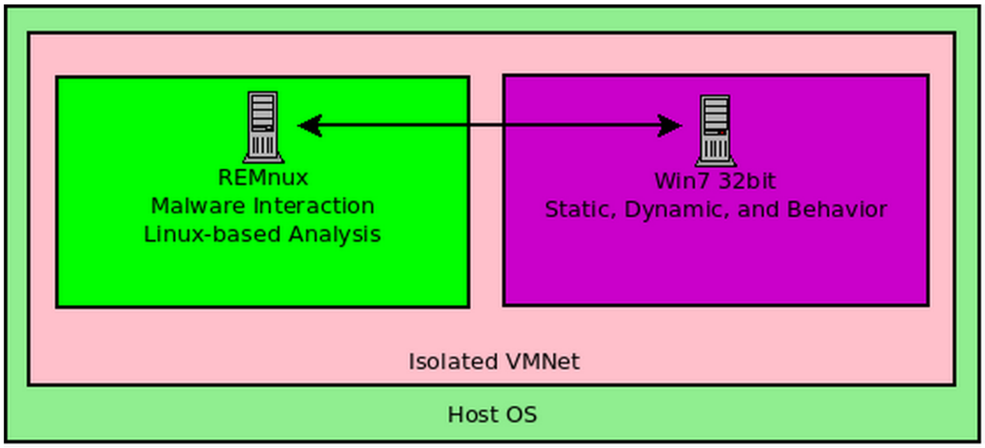
1. Install the OS, nothing else. **No tools, no service packs, no patches**. Take a snapshot and name it something like “Base OS Install” or something meaningful to you.
2. Install VM Tools - VM → Install VMWare Tools. Reboot.
3. Change the power settings so the VM doesn’t sleep (control panel → System and Security → Power Options → Change when the Computer Sleeps
4. Change settings to show hidden folders/files and file extensions – My Computer → Organize → Folder and Search Options → View → check “Show hidden files…” , uncheck “Hide extensions…”
5. Make a folder C:\Reversing. This is where we will put all of our tools (those with and without installers). Make a desktop shortcut to it to save time.
6. Set a different desktop background to remind you that this is a malware VM.
7. Install the following list to the C:\Reversing directory.

    - YARA , Navigate to windows binaries from http://yara.readthedocs.org
    - If not using IDA Pro, IDA Free https://www.hex-rays.com/
    - Visual Studio Express 2008: https://go.microsoft.com/?linkid=7729279
    - PE Insider http://cerbero.io/peinsider/
    - Explorer Suite http://www.ntcore.com/exsuite.php
    - 7zip http://www.7-zip.org/download.html
    - OllyDbg Get version 1.10 http://www.ollydbg.de/
        - Plugins, good to have. Not essential
            - Memory Manage https://tuts4you.com/download.php?view.70
            - OllyDump https://tuts4you.com/download.php?view.88
    - A Hex Editor that can XOR – Most good ones are paid. If you have a license to a good one, bring it over.
        - Alternatively, wait until a later step to download a trial of Hex Workshop or 010 Editor.
    - Sysinternals Suite https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx
    - Regshot http://sourceforge.net/projects/regshot/
    - Notepad++ http://notepad-plus-plus.org/
    - Process Hacker http://processhacker.sourceforge.net/
    - UPX http://upx.sourceforge.net/
    - LordPE LordPE http://www.aldeid.com/wiki/LordPE
    - Firefox and add-on Firebug http://getfirebug.com/
    - PDFStreamDumper https://zeltser.com/pdf-stream-dumper-malicious-file-analysis/
    - OfficeMalScanner http://www.reconstructer.org/code.html
    - McAfee FileInsight http://www.mcafee.com/us/downloads/free-tools/fileinsight.aspx

8. Create desktop shortcuts for the tools. From Sysinternals, you’ll want shortcuts for Process Monitor, Process Explorer, and Autoruns.
9. Take a snapshot and name it “Clean with Tools”, or something that makes sense to you.

Configuring Virtual Networking:

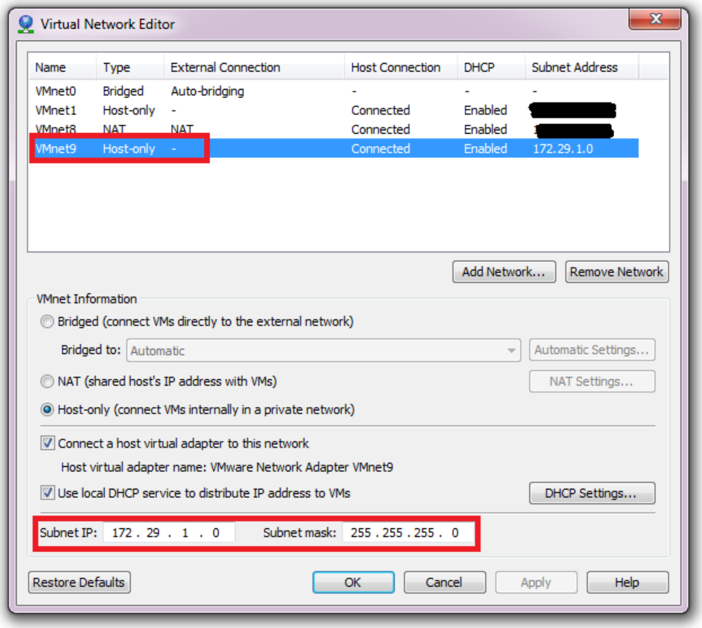
We are now going to link our two VMs together into an isolated VMNet. Neither of the two VMs will be able to access the internet, but they will be able to communicate with each other. There are three parts to this; build a network in VMware, configure REMnux to use the network, and configure Windows to use the network. What we are building will look something like the graphic below:



Building the Network

In VMWare Workstation Home -

1. Edit → Virtual Network Editor
2. Add Network, name it VMNet9. It should default to host only.
3. Select vmnet9 from the upper list
4. Set subnet IP in the lower portion of the window to 172.29.1.0 (click apply)



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	[redacted]
VMnet8	NAT	NAT	Connected	Enabled	[redacted]
VMnet9	Host-only	-	Connected	Enabled	172.29.1.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet9

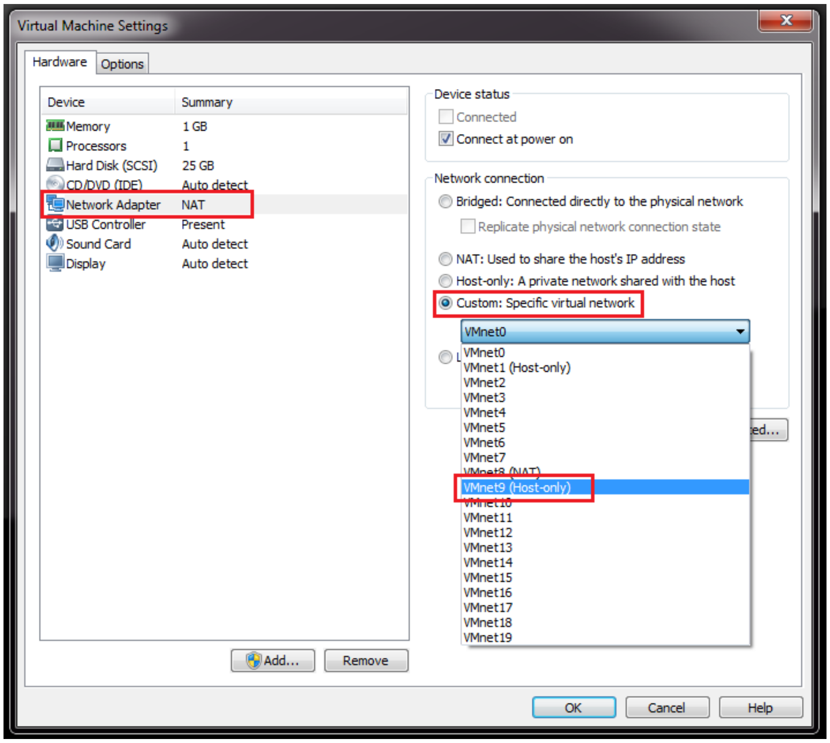
☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 172 . 29 . 1 . 0 Subnet mask: 255 . 255 . 255 . 0

Configuring REMnux Guest Virtual Networking:

In REMnux Tab of VMware Workstation

1. Rt. Click tab → Settings → Network Adapter → Custom → vmnet9 → click ok



Virtual Machine Settings

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	25 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

☐ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

☐ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet0

Within the guest Machine, configure the OS to use ip 172.29.1.10, nm 255.255.255.0

1. `$ sudo vi /etc/network/interfaces` change:

   ```
   # The primary network interface
   auto eth0
   iface eth0 inet dhcp
   ```

   to:

   ```
   # The primary network interface
   auto eth0
   iface eth0 inet static
       address 172.29.1.10
       netmask 255.255.255.0
   ```

2. `$ sudo ifdown eth0`

3. `$ sudo ifup eth0`
4. `$ ifconfig eth0` <- this should confirm you correctly configured the interface.

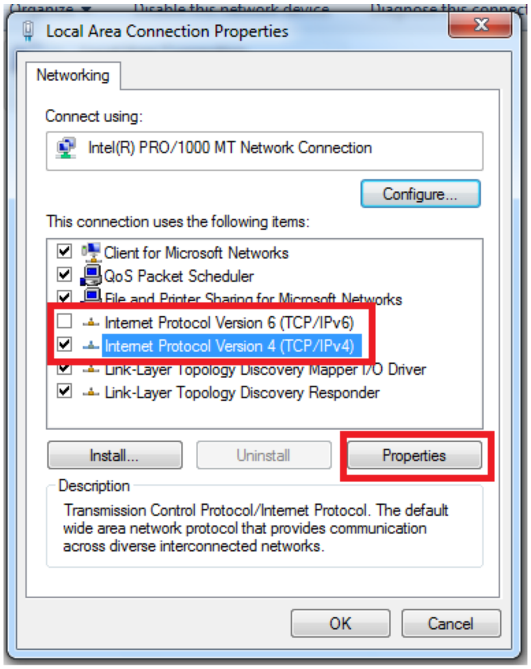
Configuring Windows Guest Virtual Networking:

In Windows Tab of VMware Workstation-

1. Rt. Click tab → Settings → Network Adapter → Custom → vmnet9 → click ok

Within the guest OS

1. Start → Search → "Network and Sharing Center"
2. Left Menu, "Change Adaptor Settings"
3. Right click "Local Area Connection" → Properties
4. Uncheck "TCP/IPv46"
5. Check "TCP/IPv44", click properties
6. Set these Values:
    a. IP Address: 172.29.1.20
    b. Subnet Mask: 255.255.255.0
    c. Default gateway: 172.29.1.10
    d. Preferred DNS Server 172.29.1.10
7. Click OK, close
8. Choose "Home Network" when prompted, click cancel when asked about sharing
9. Run cmd.exe and then ping 172.29.1.10, if this does not receive replies, troubleshoot!



Local Area Connection Properties

Networking

Connect using:

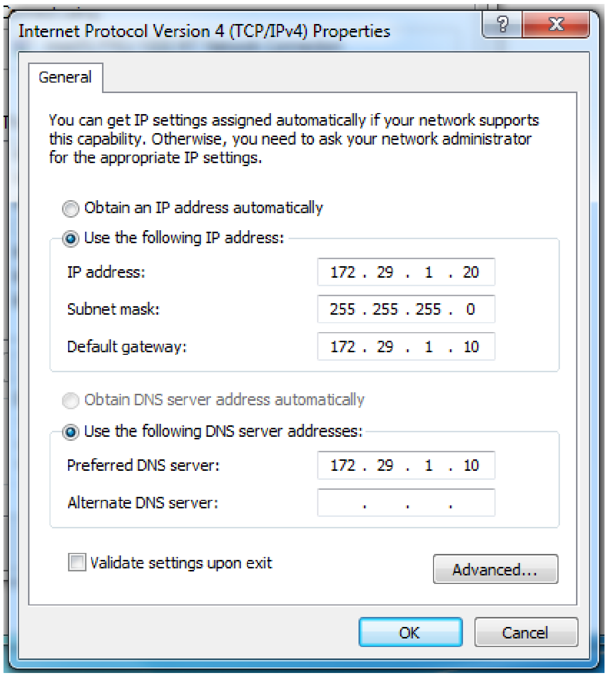
Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☐ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 172 . 29 . 1 . 20
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 29 . 1 . 10

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 172 . 29 . 1 . 10
Alternate DNS server: . . .

☐ Validate settings upon exit

Final Steps

- Snapshot both machines so that you don’t have to setup networking again after each malware infection
- Install any trial version software you want, note that you’ll have to bring it over from you host as you no longer have an internet connection. You will need a hex editor capable or XORing, most are not free. We suggest one of the following trials:
    - 010 Editor (free 30 day trial)
    - Hex Workshop (free 30 day trial)