

# **Installation Manual NIDS & HIDS**

## **Malware lab**

# 1. Preface

This document is a manual for installing a Malware Lab environment. The Malware lab is intended for a research project to compare the detection difference between a NIDS and HIDS. The aim of the research was to advise small and medium-sized enterprises if network detection (NIDS) sufficient is to detect malware infection in a enterprise network or that End-Point detection (HIDS) is necessary. The results of the research can be found [here](#).

The manual is subdivided in to the following parts:

- Installation & Configuration of:
  - VMware Workstation Pro
  - PFSense
  - Windows 10 VM (Victim Machine)
  - HIDS (Ubuntu Server 18 with Wazuh)
  - NIDS (Ubuntu Server 18 with Snort & Suricata)
- Last configuration to combine these VM's

The design of the malware lab:

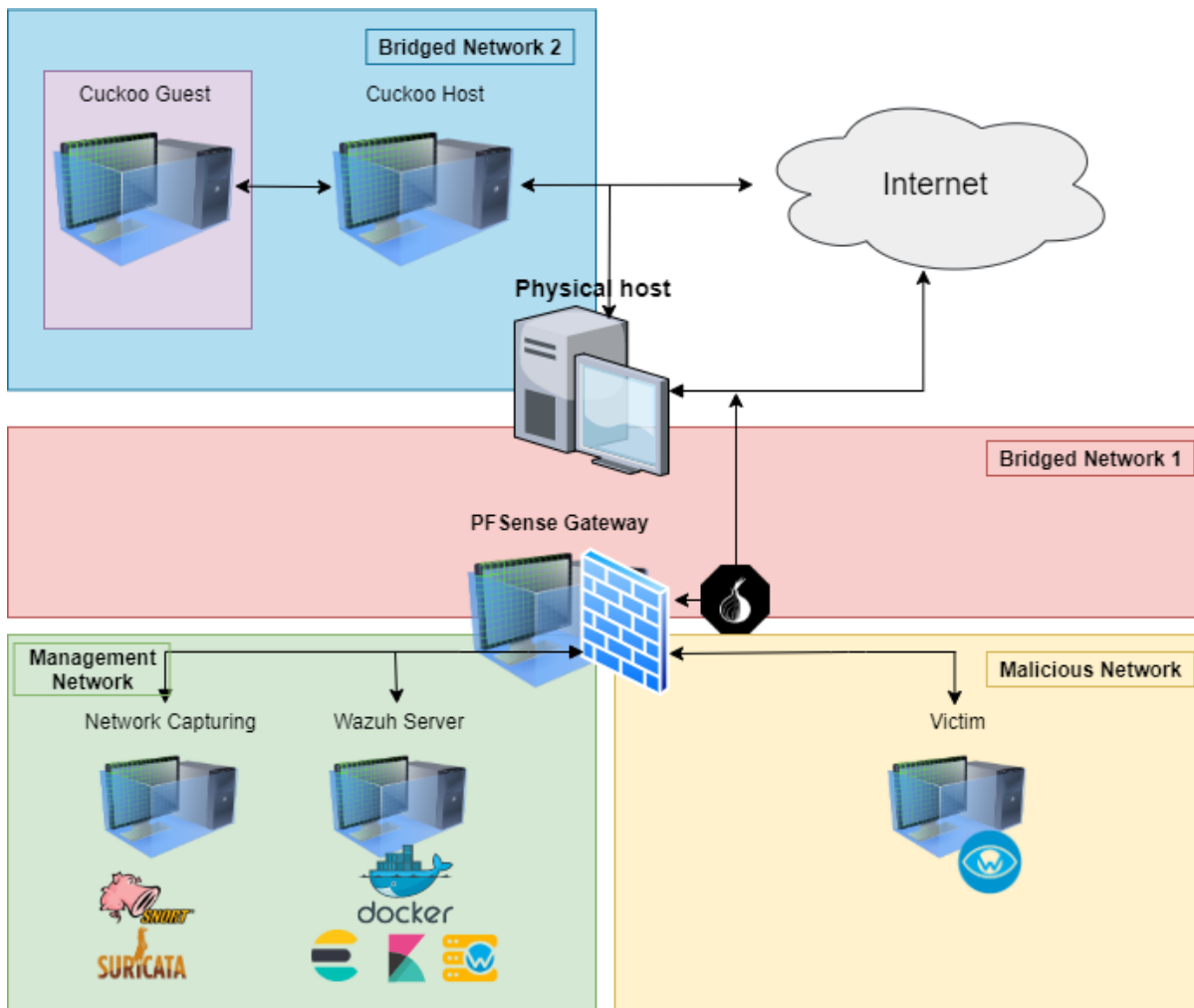


Figure 1. Malware Lab Infrastructure

Wazuh is during the research enriched with [Sigma](#) rules, the converted Wazuh rules can be found in the [sigWah](#) repository.

---

[Click here for the PDF Version of the manual](#)

[Click here for the HTML Version of the manual:](#)

Author: Sander Wiebing

# Table of Contents

1. Preface .....	2
2. Installation & Configuration .....	6
2.1. VMware Workstation Pro .....	6
2.1.1. Installation .....	6
2.1.2. Virtual Networks .....	6
2.2. pfSense .....	8
2.2.1. Installation pfSense .....	8
2.2.2. Adapter Settings host machine .....	9
2.2.3. Setup pfSense .....	10
Network Configuration PfSense .....	11
pfSense Web configurator setup .....	13
2.3. Victim Machine (Windows 10) .....	16
2.3.1. Installation Victim .....	16
2.3.2. VMwareHardenedLoader .....	17
Edit .vmx file .....	17
2.3.3. Install VMloader .....	18
2.3.4. Additional software .....	19
2.3.5. OpenSSH Server .....	20
2.3.6. Wazuh agent .....	20
2.3.7. Disable Windows Defender .....	21
2.4. NIDS .....	22
2.4.1. Installation Ubuntu Server 18 .....	22
2.4.2. Snort 2.9 .....	23
Installation .....	23
Download rules .....	25
Edit Snort configuration file .....	25
Configuring Network Cards .....	28
Run a test .....	30
2.4.3. Suricata 5.0 .....	31
Installation .....	31
Download rules .....	32
Edit Suricata configuration file .....	32
Run a test .....	34
2.5. HIDS .....	36
2.5.1. Installation Ubuntu Server 18 .....	36
2.5.2. Docker.io .....	37
2.5.3. Wazuh Container .....	38
3. Last configuration .....	40

3.1. pfSense Firewall rules .....	40
3.1.1. WAN interface .....	40
3.1.2. LAN interface .....	40
3.1.3. OPT1 interface .....	40
3.2. Register Wazuh agent at Wazuh manager .....	41
3.3. Install Filebeat on NIDS .....	42
3.4. Wazuh .....	43
3.4.1. Configure Wazuh Group configuration .....	43
3.4.2. Sysmon Second Batch .....	50
3.4.3. Sysmon Third Batch .....	51
3.5. Tor / VPN Tunneling .....	52
4. Cuckoo Sandbox .....	52

## 2. Installation & Configuration

### 2.1. VMware Workstation Pro

In this manual we will use VMware Workstation Pro as the virtualization software. The Pro version is not free but a trial of 30 days is available.

#### 2.1.1. Installation

Download the latest version [here](#), we are using version 15.5.2. Run the installer and complete the installation, no additional settings are required during the installation.

#### 2.1.2. Virtual Networks

The Malware Lab uses 4 virtual networks. By default VMware has 3 virtual networks:

1. VMnet0 - Bridged network
2. VMnet1 - Host only network
3. VMnet8 - NAT adapter

Open VMware Workstation Pro and go to *Edit > Virtual Network Editor*, the default networks should be visible.

#### NOTE

Click in Windows on 'Change Settings' to make the VMnet0 network and settings options available.

Follow the steps below to setup the virtual networks:

1. Select VMnet1
  - Uncheck 'Use local DHCP service to distribute IP address to VM'
  - Press 'Add Network' > VMnet2 > Ok
2. Select VMnet2
  - Uncheck connect a host virtual adapter to this network
  - Uncheck 'Use local DHCP service to distribute IP address to VM'
3. Press 'Add Network' > VMnet 3 > Ok
  - Uncheck connect a host virtual adapter to this network
  - Uncheck 'Use local DHCP service to distribute IP address to VM'

After the setup the Virtual Network Editor should look like this:

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	-	192.168.136.0
VMnet2	Custom	-	-	-	192.168.126.0
VMnet3	Custom	-	-	-	192.168.21.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.56.0

Figure 2. Virtual Network Editor

## 2.2. pfSense

pfSense will be used as the Firewall in the malware lab environment. The latest ISO file can be downloaded [here](#), select the AMD64 architecture and select the installer 'CM image (ISO) installer'. In this manual version 2.4.4-p3 will be used.

### 2.2.1. Installation pfSense

After the download is completed unzip the file and follow the steps below:

1. In VMware Workstation Pro click on File > New Virtual Machine
2. Select Typical > Next
3. Browse to the just downloaded pfSense ISO > Next
4. Give the VM a name, enter 'pfSense' > Next
5. Set the maximum disk size to 5 GB
6. Select 'Store virtual disk size as a single file' > next
7. Click 'Customize hardware'
  - a. Set the amount of memory to 512 MB
  - b. Click on 'Network Adapter'
    - Select 'Connect at power on'
    - Select 'Bridged: Connected to the physical network'
  - c. Click 'Add...'
    - Select 'Network Adapter' > Next
    - Select Custom > VMnet1 (Host-only)
    - Check 'Connect at power on'
    - Press finish
  - d. Click 'Add...'
    - Select 'Network Adapter' > Next
    - Select Custom > VMnet2
    - Check 'Connect at power on'
    - Press finish
  - e. Select 'USB controller' > Click 'Remove'
  - f. Select 'Sound Card' > Click 'Remove'

The hardware configuration should look like this:











Device	Summary
 Memory	512 MB
 Processors	1
 Hard Disk (SCSI)	5 GB
 CD/DVD (IDE)	Using file C:\Users\wiebing\...
 Network Adapter	Bridged (Automatic)
 Network Adapter 2	Custom (VMnet1)
 Network Adapter 3	Custom (VMnet2)
 Display	Auto detect

Figure 3. Hardware Configuration pfSense

g. Click 'Close'

8. Click 'Finish'

### 2.2.2. Adapter Settings host machine

On the Windows machine are some Network adapter settings required, follow the steps below:

1. Open Network and Sharing Center (Control Panel\Network and Internet\Network and Sharing Center)
2. Click 'Change adapter Settings'
3. Right click 'VMware Network Adapter VMnet1' > select Properties
4. Disable all options except of:
  - QoS Packet Scheduler
  - Internet Protocol Version 4 (TCP/IPv4)
5. Select 'Internet Protocol Version 4 (TCP/IPv4)' and click 'Properties'
  - a. Fill in the following properties:
    - IP address: **172.16.1.2**
    - Subnet mask: **255.255.255.0**
    - Default gateway: **<empty>**
  - b. The properties should look like this:

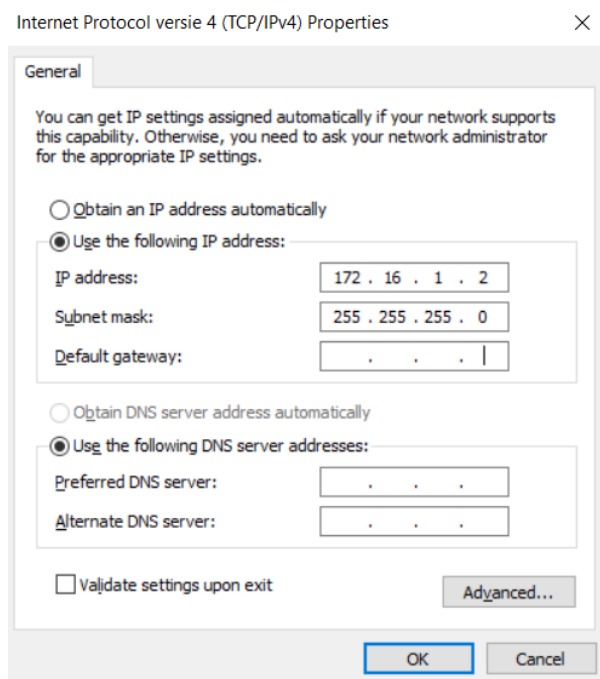


Figure 4. Windows Adapter Settings VMnet1

- c. Click 'Advanced' > select the 'WINS' tab
  - Disable 'NetBIOS over TCP/IP':

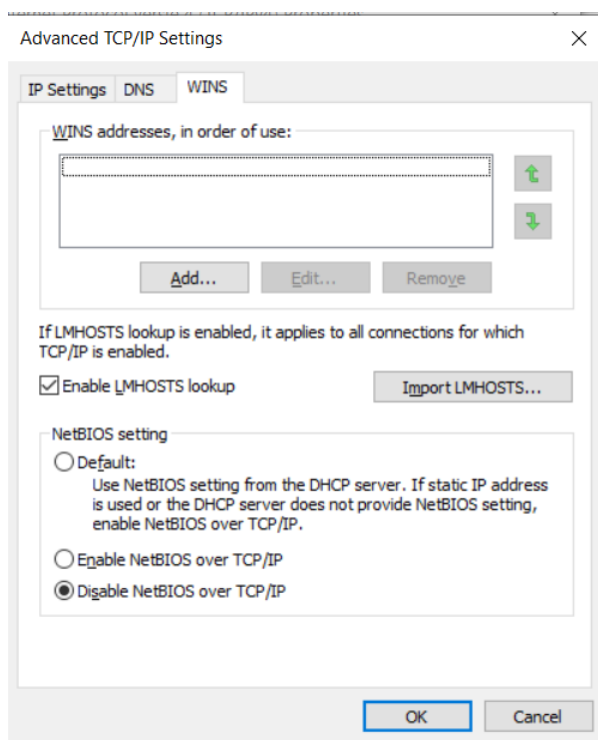


Figure 5. Windows Advanced Adapter Settings VMnet1

6. To finish, click 3 times 'OK'

### 2.2.3. Setup pfSense

After the installation pfSense the pfSense VM is ready to start and to configure. Follow the steps below:

1. Select in VMware Workstation Pro the pfSense vm and press 'Start up this guest operating system'
2. Read the Copyright and distribution notice and select Accept > press enter
3. Select 'Install pfSense ' > press enter
4. Select the right keymap > press enter
5. Select 'Guided disk setup' > press enter
6. After the install is completed, select 'No' for the manual configuration option > press enter
7. Select reboot > press Enter
8. After the reboot, power off the machine
9. Select pfSense VM > right click > 'Settings'
10. Select CD/DVD (IDE) > Click 'Remove'
11. Select Network adapter > Press advanced
  - a. Document the MAC-address
  - b. Repeat this step for Network adapter 2 and 3  
Mac-addresses in our case:
    - Network Adapter (VMnet0): 00:0C:29:2E:BC:73
    - Network Adapter 2 (VMnet1): 00:0C:29:2E:BC:7D
    - Network Adapter 3 (VMnet2): 00:0C:29:2E:BC:87

## **Network Configuration PfSense**

1. Start the pfSense VM
2. Select option 1, 'Assign Interfaces'
  - a. Enter 'n' for the question 'Should VLANs be set up now?'
  - b. Check using the documented MAC-address which adapter is which VMnet
  - c. Assign the WAN interface to the Network Adapter (VMnet0), in our case em0
  - d. Assign the LAN interface to the Network Adapter 2 (VMnet1), in our case em1
  - e. Assign the Optional 1 interface to the Network Adapter 3 (VMnet2), in our case em2
  - f. Enter 'y'
3. Select option 2, 'Set interface(s) IP address'
  - a. Enter 1 (WAN)
  - b. Fill out the following settings:

LAN IP: **172.16.1.1**  
LAN Subnet bit count: **24**  
LAN upstream gateway address: **<empty>**  
LAN IPv6 address: **<empty>**  
Do you want to enable the DHCP server on LAN? **y**  
LAN DHCP start address: **172.16.1.10**  
LAN DHCP end address: **172.16.1.254**  
Do you want to revert to HTTP as the webConfigurator protocol? **n**

4. Select again option 2, 'Set interface(s) IP address'

- a. Enter 2 (LAN)
- b. Fill out the following settings:

LAN IP: **172.16.1.1**  
LAN Subnet bit count: **24**  
LAN upstream gateway address: **<empty>**  
LAN IPv6 address: **<empty>**  
Do you want to enable the DHCP server on LAN? **y**  
LAN DHCP start address: **172.16.1.10**  
LAN DHCP end address: **172.16.1.254**  
Do you want to revert to HTTP as the webConfigurator protocol? **n**

- c. Press enter

5. Select for the last time option 2, 'Set interface(s) IP address'

- a. Enter 3 (OPT1)
- b. Fill out the following settings:

LAN IP: **172.16.2.1**  
LAN Subnet bit count: **24**  
LAN upstream gateway address: **<empty>**  
LAN IPv6 address: **<empty>**  
Do you want to enable the DHCP server on LAN? **y**  
LAN DHCP start address: **172.16.2.10**  
LAN DHCP end address: **172.16.2.254**  
Do you want to revert to HTTP as the webConfigurator protocol? **n**

- c. Press enter

6. The pfSense Menu should look something like this:

```
*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.212/24
                                     v6/DHCP6: fdf7:effa:2821:0:20c:29ff:fe2e:bc73/
64
LAN (lan)      -> em1      -> v4: 172.16.1.1/24
OPT1 (opt1)    -> em2      -> v4: 172.16.2.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Figure 6. pfSense Menu

**NOTE** | Don't forget to take several snapshots in the installation process.

### pfSense Web configurator setup

Open on the host machine a web browser and navigate to <https://172.16.1.1> (the LAN interface). Log in with the default credentials **admin/pfsense** and follow the steps below:

1. In the 'pfSense Setup' click 2 times 'next'
2. Fill out the following settings:
  - a. Primary DNS Server **8.8.8.8**
  - b. Secondary DNS server **8.8.4.4**
3. Click 'next'
4. Uncheck the following options:
  - a. Block private networks from entering via WAN
  - b. Block non-Internet routed networks from entering via WAN
5. Click 'next'
6. Set a admin password
7. Finish the setup
8. On the top bar, go to Firewall > rules
9. Select 'LAN' and click the 'add' button <u>with the arrow facing up</u>
  - a. Fill out the follow settings:

Action: **Pass**  
Disabled: <**unchecked**>  
Interface: **LAN**  
Address Family: **IPv4**  
Protocol: **TCP**  
Source: <**unchecked invert match**> - **Single host or alias - 172.16.1.2**  
Destination: <**unchecked invert match**> - **Single host or alias - 172.16.1.1**  
Destination port range: From **HTTPS(443)** - To **HTTPS(443)**  
Log: <**unchecked**>  
Description: **pfsense strict anti-lockout**

b. Click 'save'

**NOTE**      This rule will prevent the machine from accessing the pfSense Web Interface

10. Select 'OP1' and click the 'add' button <u>with the arrow facing up</u>

a. Fill out the follow settings:

Action: **Pass**  
Disabled: <**unchecked**>  
Interface: **OP1**  
Address Family: **IPv4**  
Protocol: **Any**  
Source: <**unchecked invert match**> - **OPT1 net**  
Destination: <**unchecked invert match**> - **Any**  
Log: <**unchecked**>  
Description: **Default allow OPT1 to any rule**

b. Click 'save'

11. Still in 'OP1', click again the 'add' button <u>with the arrow facing up</u>

a. Fill out the follow settings:

Action: **Pass**  
Disabled: <**unchecked**>  
Interface: **OP1**  
Address Family: **IPv6**  
Protocol: **Any**  
Source: <**unchecked invert match**> - **OPT1 net**  
Destination: <**unchecked invert match**> - **Any**  
Log: <**unchecked**>  
Description: **Default allow OPT1 to any rule**

b. Click 'save'

12. Click 'Apply Changes'

**NOTE** | These two rules will give OPT1 internet access

13. Navigate to Firewall > Aliases

14. Select 'IP' and click on 'Add'

a. Fill out the follow settings in 'Properties':

Name: **RFC1918**  
Description: **An alias for all RFC1918 netowrks**  
Type: **Network(s)**

b. Press 2 times on 'Add network' and set the network settings to:

i. Address: **10.0.0.0/8** Description: **10.x.x.x RFC 1918 networks**

ii. Address: **172.16.0.0/12** Description: **172.16.x.x RFC 1918 networks**

iii. Address: **192.168.0.0/16** Description: **192.168.x.x RFC 1918 networks**

c. Click 'Save'

15. Click 'Apply Changes'

16. Navigate to System > Advanced

a. Enable the option 'Disable webConfigurator anti-lockout rule'

**WARNING** | Without the firewall rule above you will block your self from access the WebConfigurator

## 2.3. Victim Machine (Windows 10)

The victim machine will have Windows 10 as operating system. Free to download virtual machines are available on [this](#) site, they are completely ready but the VMware Tools are installed by default. VMware tools can be easily detect by malware, that is why we will use a Windows 10 ISO. With the Media Creation Tool it is possible to make a ISO file, the tool can be downloaded [here](#).

### 2.3.1. Installation Victim

After the Windows 10 ISO file is ready, follow the steps below:

1. In VMware Workstation Pro click on File > New Virtual Machine
2. Select Typical > Next
3. Browse to the created Windows 10 ISO > Next
4. Give the VM a name, enter 'Victim\_Windows10' > Next
5. Set the maximum disk size to 100 GB
6. Select 'Store virtual disk size as a single file' > next
7. Click 'Customize hardware'
  - a. Set the amount of memory to 2048 MB
  - b. Set number of processors to 2
  - c. Set number of cores per processor to 2
  - d. Set the MAC-address to: "E4-70-B8-23-CF-E0"
  - e. Click on 'Network Adapter'
    - Select 'Connect at power on'
    - Select Custom > VMnet2
  - f. Press Close
8. Press Finish
9. Log in to the pfSense web UI
  - a. Navigate to Services > DHCP server and select 'OPT1'
  - b. Add a Static mapping
    - Mac-adress of the victim machine: E4-70-B8-23-CF-E0
    - IP Address: 172.16.2.2
  - c. Click 'save' > 'Apply changes'
10. Start the Virtual Machine
11. Go through the installation process
  - a. Select 'I don't have a product key'
  - b. Select Windows 10 Home
  - c. Select option 'Custom: Install Windows Only'



- d. Select the unallocated Space > next  
Windows will be installed
- 12. When is asked to sign in, follow these steps:
  - a. Fill in for username: test
  - b. Password: test (or something else)  
You will get a error that the account is locked, now you can use a offline account
- 13. Resume the installation
  - a. Enter the name: 'John Williams'
  - b. Fill in a password and **document it**
  - c. Fill in the security questions
- 14. Disable all features and extra services like 'find my device'  
Windows will be loaded, remember:

**WARNING** | Do not install VMware Tools!

### 2.3.2. VMwareHardenedLoader

With the standard configuration, the virtual environment is easily detected by malware. A example below, a simple PowerShell command reveals the virtualization with the manufacturer and model field.

```
PS C:\Users\John> Get-WmiObject Win32_ComputerSystem

Domain           : WORKGROUP
Manufacturer     : VMware, Inc.
Model            : VMware7,1
Name             : DESKTOP-0T07MVE
PrimaryOwnerName : John
TotalPhysicalMemory : 2146287616
```

Figure 7. PowerShell Win32\_ComputerSystem

VMwareHardenedLoader is an open-source tool on github. It is a detection mitigation loader, it gets vmware guest undetected by VMProtect 3.2, Safengine and Themida (anti-vm feature).

We will follow the steps provided [here](#), the first part is editing the .vmx file.

#### Edit .vmx file

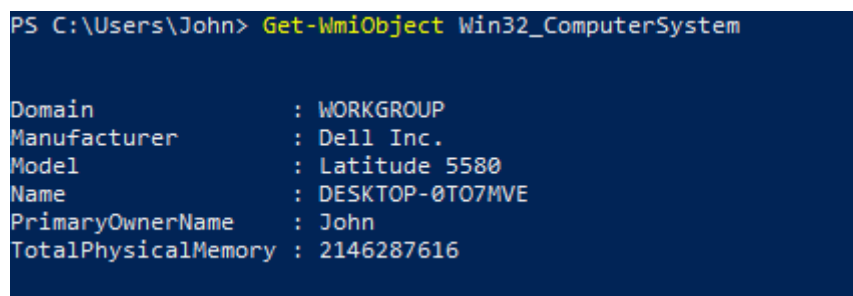
Shut down (Do not pause) the Victim machine, in Workstation, right click on 'Victim\_Windows10' > 'Open VM Directory'. Open the .vmx file (Victim\_Windows10.vmx) in a text editor and add the following settings (at the bottom):

```

hypervisor.cpubid.v0 = "FALSE"
board-id.reflectHost = "TRUE"
hw.model.reflectHost = "TRUE"
serialNumber.reflectHost = "TRUE"
smbios.reflectHost = "TRUE"
SMBIOS.noOEMStrings = "TRUE"
isolation.tools.getPtrLocation.disable = "TRUE"
isolation.tools.setPtrLocation.disable = "TRUE"
isolation.tools.setVersion.disable = "TRUE"
isolation.tools.getVersion.disable = "TRUE"
monitor_control.disable_directexec = "TRUE"
monitor_control.disable_chksimd = "TRUE"
monitor_control.disable_ntreloc = "TRUE"
monitor_control.disable_selfmod = "TRUE"
monitor_control.disable_reloc = "TRUE"
monitor_control.disable_btinout = "TRUE"
monitor_control.disable_btmemspace = "TRUE"
monitor_control.disable_btpriv = "TRUE"
monitor_control.disable_btseg = "TRUE"
monitor_control.restrict_backdoor = "TRUE"
scsi0:0.productID = "Tencent SSD"
scsi0:0.vendorID = "Tencent"
ethernet0.address = "E4-70-B8-23-CF-E0"

```

Save the file and start up the Victim machine. If we run the PowerShell command again it will give as result something like this:



```

PS C:\Users\John> Get-WmiObject Win32_ComputerSystem

Domain           : WORKGROUP
Manufacturer     : Dell Inc.
Model            : Latitude 5580
Name             : DESKTOP-0T07MVE
PrimaryOwnerName : John
TotalPhysicalMemory : 2146287616

```

Figure 8. PowerShell Win32\_ComputerSystem with loader configuration

### 2.3.3. Install VMloader

Step 2 is installing the VmwareHardenedLoader service. Download the 'bin' folder [here](#) and run install.bat as administrator in the victim machine.

```

C:\Users\John Williams\Downloads\VmwareHardenedLoader-master\VmwareHardenedLoader-master\bin>install.bat

C:\Users\John Williams\Downloads\VmwareHardenedLoader-master\VmwareHardenedLoader-master\bin>copy "C:\Users\John Williams\Downloads\VmwareHardenedLoader-master\VmwareHardenedLoader-master\bin\vmloader.sys" "C:\vmloader.sys"
1 file(s) copied.

C:\Users\John Williams\Downloads\VmwareHardenedLoader-master\VmwareHardenedLoader-master\bin>sc create vmloader binPath=
"\\?\c:\vmloader.sys" type= "kernel" start= "system"
[SC] CreateService SUCCESS

C:\Users\John Williams\Downloads\VmwareHardenedLoader-master\VmwareHardenedLoader-master\bin>sc start vmloader

SERVICE_NAME: vmloader
        TYPE               : 1  KERNEL_DRIVER
        STATE                : 4  RUNNING
                           (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
        PID                 : 0
        FLAGS                 :

```

```

C:\Users\John Williams\Downloads\VmwareHardenedLoader-master\VmwareHardenedLoader-master\bin>reg delete "HKLM\HARDWARE\ACPI\DSDT\PTLTD_" /f
The operation completed successfully.

```

Figure 9. VMwareHardenedLoader install

### 2.3.4. Additional software

We will install some extra software for two reasons. First the machine has to look as a normal machine which is being used, second it helps some malware to run as they might have it as a dependency.

The following software has to be installed:

Table 1. Installed software

Name	Version	link
Google Chrome	80.0.3987.132	<a href="https://www.google.com/chrome">https://www.google.com/chrome</a>
Firefox	74.0	<a href="https://www.mozilla.org/firefox/new/">https://www.mozilla.org/firefox/new/</a>
x65 Java runtime	8 Update 241	<a href="https://www.java.com/download">https://www.java.com/download</a>
.NET Core Runtime	v3.1.2	<a href="https://dotnet.microsoft.com/download/dotnet-core">https://dotnet.microsoft.com/download/dotnet-core</a>
Silverlight	5	<a href="https://microsoft.com/silverlight">https://microsoft.com/silverlight</a>
LibreOffice	6.4.1	<a href="https://libreoffice.org/download/download">https://libreoffice.org/download/download</a>
7-Zip	19.00	<a href="https://www.7-zip.org/download.html">https://www.7-zip.org/download.html</a>
Thunderbird	68.6.0	<a href="https://www.thunderbird.net">https://www.thunderbird.net</a>
Python 3	3.8.2	<a href="https://www.python.org/downloads">https://www.python.org/downloads</a>
Python 2	2.7.17	<a href="https://www.python.org/downloads">https://www.python.org/downloads</a>

Name	Version	link
Microsoft Visual C++ Redistributable Package	2015 - 2019 14.25.28508	<a href="https://support.microsoft.com/help/2977003/the-latest-supported-visual-c-downloads">https://support.microsoft.com/help/2977003/the-latest-supported-visual-c-downloads</a>
Nitro Reader	Pro 11	<a href="https://www.gonitro.com/pdf-reader">https://www.gonitro.com/pdf-reader</a>
VLC media-player	3.0.8	<a href="https://videolan.org">https://videolan.org</a>
Microsoft Office Home and Student 2016		<a href="https://officecdn.microsoft.com/db/492350F6-3A01-4F97-B9C0-C7C6DDF67D60/media/en-US/HomeStudentRetail.img">https://officecdn.microsoft.com/db/492350F6-3A01-4F97-B9C0-C7C6DDF67D60/media/en-US/HomeStudentRetail.img</a>

To resemble the victim machine as a normal machine we also create some folders and documents. It does not matter what kind of documents, just fill it up. Some sample documents:

- 'Financial Sample.xlsx' - <https://go.microsoft.com/fwlink/?LinkID=521962>
- Word templates - <https://go.microsoft.com/fwlink/?LinkID=521962>
- Sample pdf - <http://www.africau.edu/images/default/sample.pdf>
- Images - <https://www.google.com/imghp>

### 2.3.5. OpenSSH Server

To transfer the malicious files to the victim we will use the SCP command. For this reason we are going to install the OpenSSH server

1. Open Powershell as Administrator
2. Run these commands:

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
Start-Service sshd
Set-Service -Name sshd -StartupType 'Automatic'
```

### 2.3.6. Wazuh agent

We need to install the Wazuh agent to make monitoring for the HIDS possible.

1. Start the Victim VM
2. Open a browser, go to the wazuh packages

<https://documentation.wazuh.com/3.11/installation-guide/packages-list/#windows>

3. Download the agent for windows (wazuh-agent-3.11.4-1.msi) and execute it
  - a. Read and accept the term > press 'Install'

- b. Check 'Run agent configuration interface' and press 'Finish'
- c. Set the Manager IP to: 172.16.1.3
- d. Click save and exit

We register the agent to the manager when the installation of the HIDS is completed

### 2.3.7. Disable Windows Defender

We need to disable the Windows Defender to run the malware.

1. Start the Victim VM
2. Press Windows Key + r
  - a. Type in 'regedit' and click 'OK'
3. Browse to the following path:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender

4. Right click on Windows defender folder
  - a. Select New > DWORD (32-bit)
  - b. Name it 'DisableAntiSpyware' and press Enter
5. Double-click on the just created 'DisableAntiSpyware' item.
  - a. Set the value data to: 1

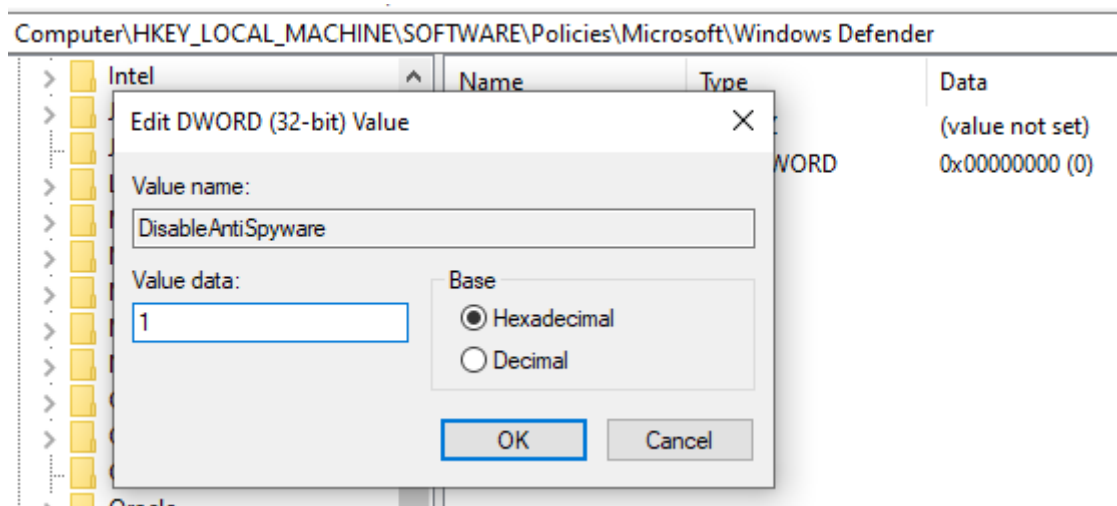


Figure 10. Regex Editor - Disable Defender

- b. Restart the VM

## 2.4. NIDS

We will use Ubuntu Server as operating system for the NIDS and HIDS VM. The ISO can be downloaded [here](#) (18.04.4).

### 2.4.1. Installation Ubuntu Server 18

1. In VMware Workstation Pro click on File > New Virtual Machine
2. Select Typical > Next
3. Browse to the downloaded Ubuntu Server ISO > Next
4. Fill in the fields name, username (we use nids), password
5. Give the VM a name, enter 'NIDS' > Next
6. Set the maximum disk size to 50 GB
7. Select 'Store virtual disk size as a single file' > next
8. Click 'Customize hardware'
  - a. Set the amount of memory to 2048 MB
  - b. Set number of processors to 2
  - c. Set number of cores per processor to 2
  - d. Click on 'Network Adapter'
    - Select 'Connect at power on'
    - Select Custom > VMnet1 (Host-only)
  - e. Click 'Add...'
    - Select 'Network Adapter' > Next
    - Select Custom > VMnet2 (IPS1)
    - **Uncheck** 'Connect at power on'
    - Press finish
  - f. Click 'Add...'
    - Select 'Network Adapter' > Next
    - Select Custom > VMnet3 (IPS2)
    - **Uncheck** 'Connect at power on'
    - Press finish
  - g. Select 'USB controller' > Click 'Remove'
  - h. Select 'Sound Card' > Click 'Remove'
  - i. Select 'Printer' > Click 'Remove'
  - j. Press Close
9. Press Finish

10. Open the VM settings again
  - a. Remove the CD/ DVD with the 'autoinst.iso' inserted
  - b. Remove the Floppy drive with the 'autoinst.flp' inserted
11. Start the Virtual Machine
12. Go through the installation process
  - a. At the software selection phase, make sure to install OpenSSH server'
13. Shut down the VM after the installation is completed
  - a. Remove the last CD/DVD drive
  - b. Document the MAC-address of the network adapter
  - c. Check the *connect at power on* for Network adapter 2 (VMnet2) and Network adapter 3 (VMnet3)
14. Log in to the pfSense web UI
  - a. Navigate to Services > DHCP server and select 'LAN'
  - b. Add a Static mapping
    - Mac-address of the NIDS machine (E4-70-B8-23-CF-E0)
    - IP Address: 172.16.1.4
  - c. Click 'save' > 'Apply changes'
15. Start up the VM
  - a. Log in
  - b. Verify that the IP-address is 172.16.1.4 (with ifconfig)
  - c. Update the vm with:

```
sudo apt-get update; sudo apt-get upgrade;
```

- d. Make sure the server has the correct time and time zone with:

```
sudo dpkg-reconfigure tzdata
```

### 2.4.2. Snort 2.9

The NIDS software we will install is Snort (<http://www.snort.org/>). For the main we follow [this](#) guide. The steps are documented below

#### Installation

1. Log into the NIDS VM

#### TIP

Login from the host machine with SHH to the NIDS VM for easy copy and paste

2. Execute these commands:

a. Make a folder to store the downloaded files

```
mkdir ~/snort_src  
cd ~/snort_src
```

b. Install the Snort prerequisites

```
sudo apt install -y gcc libpcap-dev zlib1g-dev liblua5.1-dev libpcap-dev  
openssl libssl-dev libnet-dev libdumbnet-dev bison flex libnet
```

c. Install daq

```
cd ~/snort_src  
wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz  
tar -xvzf daq-2.0.6.tar.gz  
cd daq-2.0.6  
./configure && make && sudo make install
```

d. Install Snort

```
cd ~/snort_src  
wget https://www.snort.org/downloads/snort/snort-2.9.15.1.tar.gz  
tar -xvzf snort-2.9.15.1.tar.gz  
cd snort-2.9.15.1  
./configure --enable-sourcefire && make && sudo make install
```

e. Update the shared libraries

```
sudo ldconfig
```

f. Create a symbolic link to snort

```
sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

g. Create the folder structure and create the required files



```

sudo mkdir -p /etc/snort/rules
sudo mkdir /etc/snort/preproc_rules
sudo mkdir /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrules

sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules
sudo touch /etc/snort/rules/local.rules

```

h. Copy the configuration files from the download folder

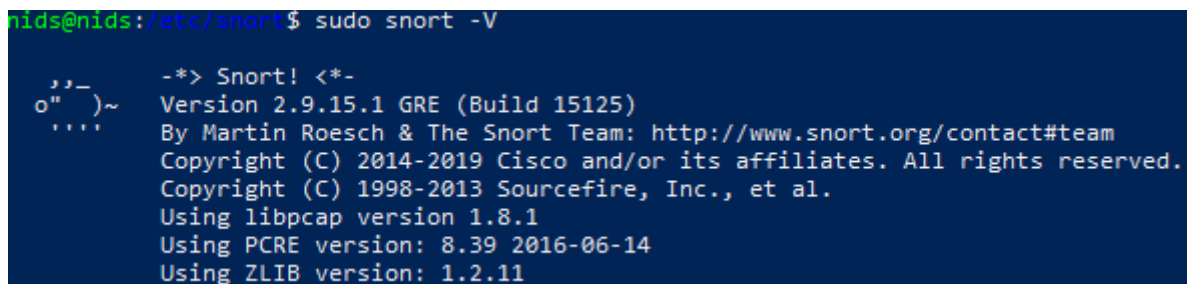
```

sudo cp ~/snort_src/snort-2.9.15.1/etc/*.conf* /etc/snort
sudo cp ~/snort_src/snort-2.9.15.1/etc/*.map /etc/snort
sudo cp ~/snort_src/snort-2.9.15.1/etc/*.dtd /etc/snort

```

3. Verify that Snort can run

```
sudo snort -V
```



```

nids@nids:/etc/snort$ sudo snort -V
_*> Snort! <*-
o" )~ Version 2.9.15.1 GRE (Build 15125)
.... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.8.1
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11

```

Figure 11. Snort installed

## Download rules

For the malware lab we will use PRO rules from [emergingthreats.net](http://emergingthreats.net). If you don't have a pro version, there are also free rules available [here](#) or from the Snort community.

1. Download and setup the rules:

```

cd ~/snort_src/
wget https://rules.emergingthreatspro.com/$oinkcode/snort-
2.9.15.1/etpro.rules.tar.gz
sudo tar -xvf etpro.rules.tar.gz -C /etc/snort

```

## Edit Snort configuration file

We will want to modify our Snort configuration file to enable some extra features and so that we don't have to specify settings at the command line.

1. Open the configuration file

```
sudo nano /etc/snort/snort.conf
```

- a. Find these sections shown below in the configuration file and change the parameters to reflect the examples here.

```
# Setup the network addresses you are protecting
ipvar HOME_NET 172.16.2.0/24
```

```
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
```

```
# Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
```

```
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

- b. Scroll down to section 6 (line 519) and set the output for unified2 to log under filename of snort.log:

```
# unified2
# Recommended for most installs
output unified2: filename snort.log, limit 128
output alert_fast: alert.fast
```

- c. Lastly, scroll down to the bottom of the file to find the list of included rules. Replaces this list with the following (in our case).

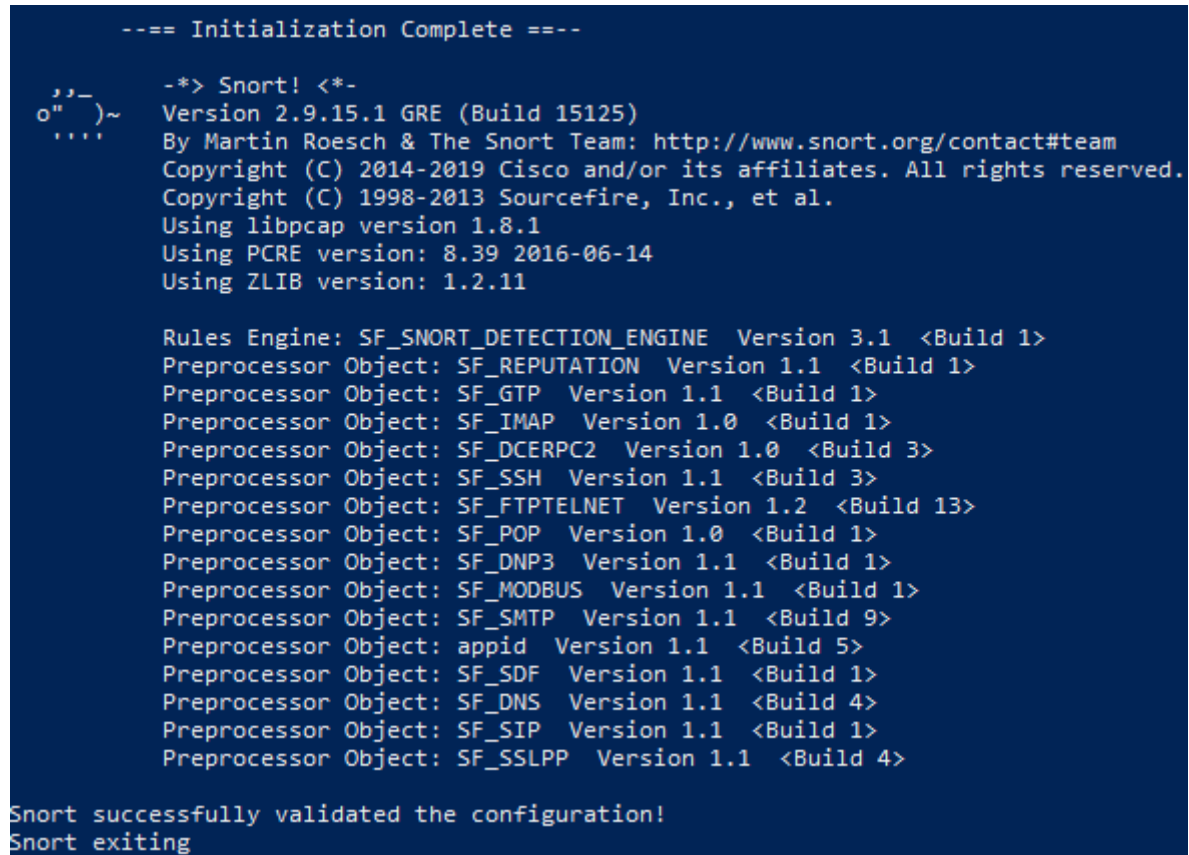
```
include $RULE_PATH/local.rules

include activex.rules
include attack_response.rules
include botcc.portgrouped.rules
include botcc.rules
include chat.rules
include ciarmy.rules
include compromised.rules
include current_events.rules
include deleted.rules
include dns.rules
include dos.rules
include drop.rules
include dshield.rules
include exploit.rules
include ftp.rules
include games.rules
include icmp_info.rules
include icmp.rules
include imap.rules
include inappropriate.rules
include info.rules
include local.rules
include malware.rules
include misc.rules
include mobile_malware.rules
include netbios.rules
include p2p.rules
include policy.rules
include pop3.rules
include rpc.rules
include scada.rules
include scada_special.rules
include scan.rules
include shellcode.rules
include smtp.rules
include snmp.rules
include sql.rules
include telnet.rules
include tftp.rules
include tor.rules
include trojan.rules
include user_agents.rules
include voip.rules
include web_client.rules
include web_server.rules
include web_specific_apps.rules
include worm.rules
```

2. Test if snort loads the configuration file correctly::

```
snort -T -c /etc/snort/snort.conf
```

The result must be **Snort successfully validated the configuration!**

A terminal window with a dark blue background and white text. The output shows the Snort initialization process. It starts with '--- Initialization Complete ---'. Then, it displays the Snort version (2.9.15.1 GRE) and build information (Build 15125). It lists the copyright for Martin Roesch & The Snort Team (2014-2019) and Sourcefire, Inc. (1998-2013). It also shows the versions of dependencies: libpcap 1.8.1, PCRE 8.39 (2016-06-14), and ZLIB 1.2.11. A list of preprocessor objects follows, including SF\_SNORT\_DETECTION\_ENGINE, SF\_REPUTATION, SF\_GTP, SF\_IMAP, SF\_DCERPC2, SF\_SSH, SF\_FTPTELNET, SF\_POP, SF\_DNP3, SF\_MODBUS, SF\_SMTP, appid, SF\_SDF, SF\_DNS, SF\_SIP, and SF\_SSLPP, each with its version and build number. The final line of the output is 'Snort successfully validated the configuration!' followed by 'Snort exiting' on the next line.

```
--- Initialization Complete ---

--> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>

Snort successfully validated the configuration!
Snort exiting
```

Figure 12. Snort with configuration

**TIP** Make a snapshot!

## Configuring Network Cards

Snort has sometimes problems with network card where GRO or / and LRO is enabled, in this section we will disable these features of the network card.

1. First, check which MAC-address correspondent with which Ethernet Adapter, run:

```
ifconfig -a
```

```
nids@nids:~$ ifconfig -a
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.1.4 netmask 255.255.255.0 broadcast 172.16.1.255
    inet6 fe80::20c:29ff:fe67:786e prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:67:78:6e txqueuelen 1000 (Ethernet)
    RX packets 24899 bytes 36637916 (36.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6981 bytes 631612 (631.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens33: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:67:78:78 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens34: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:67:78:82 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 13. NIDS ifconfig

In our case ens33 is the IPS1 (Vmnet2) and ens34 the IPS2 (VMnet3) network, we will now use IPS1 for the capture.

2. For a NIDS we want to disable offloading (GRO and LRO) on the network card. To check if it is enabled:

```
sudo ethtool -k ens33 | grep receive-offload
```

```
nids@nids:~$ sudo ethtool -k ens33 | grep receive-offload
generic-receive-offload: on
large-receive-offload: off [fixed]
```

Figure 14. NIDS Offload status

3. As you can see the GRO is enabled, we could disable it with the ethtool, but the setting would not persist after a system reboot. The solution is to create a systemd script to set this every boot.

Create the sytemD script

```
sudo nano /lib/systemd/system/ethtool.service
```

Enter the following lines:

```
[Unit]
Description=Ethtool Configuration for Network Interface

[Service]
Requires=network.target
Type=oneshot
ExecStart=/sbin/ethtool -K ens33 gro off
ExecStart=/sbin/ethtool -K ens33 lro off

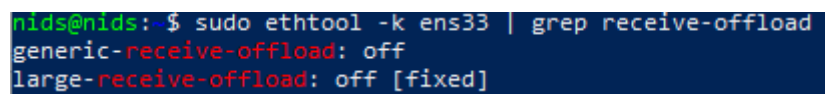
[Install]
WantedBy=multi-user.target
```

Once the file is created, enable the service:

```
sudo systemctl enable ethtool
sudo service ethtool start
```

#### 4. Check if both are disabled

```
sudo ethtool -k ens33 | grep receive-offload
```



```
nids@nids:~$ sudo ethtool -k ens33 | grep receive-offload
generic-receive-offload: off
large-receive-offload: off [fixed]
```

Figure 15. NIDS Offload status off

Both are disabled now.

### Run a test

To test if Snort is processing as intended the traffic made by the Victim machine, we add a custom detection rule alert on incoming ICMP connections.

#### 1. Open local.rules

```
sudo nano /etc/snort/rules/local.rules
```

Add the following line:

```
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
```

#### 2. Start snort with:

```
sudo snort -A console -i ens33 -c /etc/snort/snort.conf
```

### 3. Start the Victim machine

- a. Open PowerShell and run the command:

```
ping www.google.com
```

### 4. On the NIDS side you should see these alerts:

```
Commencing packet processing (pid=38645)
03/19-16:26:27.005029  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 172.217.168.206 -> 172.16.2.2
03/19-16:26:28.020038  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 172.217.168.206 -> 172.16.2.2
03/19-16:26:29.034596  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 172.217.168.206 -> 172.16.2.2
03/19-16:26:30.052290  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 172.217.168.206 -> 172.16.2.2
```

Figure 16. Snort IMCP alert

It is working!

**TIP** | Make a snapshot!

## 2.4.3. Suricata 5.0

The second NIDS software we will install is Suricata (<https://suricata-ids.org/>). For the main we follow [this](#) guide. The steps are documented below

### Installation

#### 1. Log into the NIDS VM

**TIP** | Login from the host machine with SSH to the NIDS VM for easy copy and paste

#### 2. Execute these commands:

- a. Make a folder to store the downloaded files

```
mkdir ~/suricata_src
cd ~/suricata_src
```

- b. Install Suricata (5.0.2)

```
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install suricata
```

#### 3. Verify that Suricata can run

```
sudo suricata -V
```

```
nids@nids:~/suricata_src/suricata-5.0.2$ sudo suricata -V
This is Suricata version 5.0.2 RELEASE
```

Figure 17. Suricata installed

**TIP** Make a snapshot!

## Download rules

For the malware lab we will use PRO rules from [emergingthreats.net](https://rules.emergingthreatspro.com/). If you don't have a pro version, there are also free rules available [here](#).

1. Download and setup the rules:

```
cd ~/suricata_src/
wget https://rules.emergingthreatspro.com/$oinkcode/suricata-5.0/etpro.rules.tar.gz
sudo rm -r /etc/suricata/rules
sudo tar -xvf etpro.rules.tar.gz -C /etc/suricata
```

## Edit Suricata configuration file

We have to modify the configuration files to enable the rules and some other things.

1. Open the configuration file

```
cd /etc/suricata
sudo nano suricata.yaml
```

- a. Find these sections shown below in the configuration file and change the parameters to reflect the examples here.

```
HOME_NET: "[172.16.2.0/24]"
```

```
- eve.log:
  [...]
- stats:
  totals: no
  threads: no
  deltas: no
```

```
default-rule-path: /etc/suricata/rules
```

```
rule-files:
- local.rules
- activex.rules
- adware_pup.rules
```

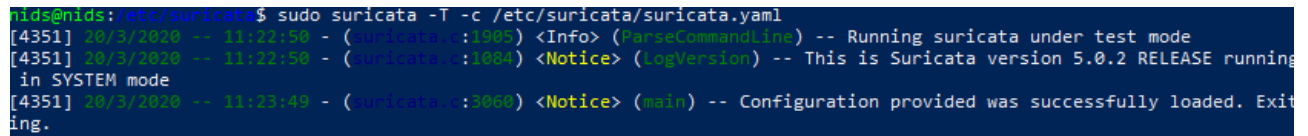


- attack\_response.rules
- botcc.portgrouped.rules
- botcc.rules
- chat.rules
- ciarmy.rules
- coinminer.rules
- compromised.rules
- current\_events.rules
- deleted.rules
- dns.rules
- dos.rules
- drop.rules
- dshield.rules
- exploit\_kit.rules
- exploit.rules
- ftp.rules
- games.rules
- hunting.rules
- icmp\_info.rules
- icmp.rules
- imap.rules
- inappropriate.rules
- info.rules
- ja3.rules
- malware.rules
- misc.rules
- mobile\_malware.rules
- netbios.rules
- p2p.rules
- phishing.rules
- policy.rules
- pop3.rules
- rpc.rules
- scada.rules
- scada\_special.rules
- scan.rules
- shellcode.rules
- smtp.rules
- snmp.rules
- sql.rules
- telnet.rules
- tftp.rules
- tor.rules
- user\_agents.rules
- voip.rules
- web\_client.rules
- web\_server.rules
- web\_specific\_apps.rules
- worm.rules

2. Test if Suricata loads the configuration file correctly:

```
sudo suricata -T -c /etc/suricata/suricata.yaml
```

The output should look like this:



```
nids@nids:/etc/suricata$ sudo suricata -T -c /etc/suricata/suricata.yaml
[4351] 20/3/2020 -- 11:22:50 - (suricata.:1905) <Info> (ParseCommandLine) -- Running suricata under test mode
[4351] 20/3/2020 -- 11:22:50 - (suricata.:1084) <Notice> (LogVersion) -- This is Suricata version 5.0.2 RELEASE running
in SYSTEM mode
[4351] 20/3/2020 -- 11:23:49 - (suricata.:3060) <Notice> (main) -- Configuration provided was successfully loaded. Exiting.
```

Figure 18. Suricata configuration loaded

## Run a test

To test if Suricata is processing as intended the traffic made by the Victim machine, we add a custom detection rule alert on incoming ICMP connections.

1. Open local.rules

```
sudo nano /etc/suricata/rules/local.rules
```

Add the following line:

```
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
```

2. Start Suricata with:

```
sudo suricata -i ens33 -c /etc/suricata/suricata.yaml
```

3. Open a new windows and run this command in the NIDS:

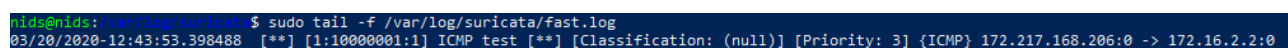
```
sudo tail -f /var/log/suricata/fast.log
```

4. Start the Victim machine

- a. Open PowerShll and run the command:

```
ping www.google.com
```

5. On the NIDS side you should see these alert:



```
nids@nids:/var/log/suricata$ sudo tail -f /var/log/suricata/fast.log
03/20/2020-12:43:53.398488  [**] [1:10000001:1] ICMP test [**] [Classification: (null)] [Priority: 3] {ICMP} 172.217.168.206:0 -> 172.16.2.2:0
```

Figure 19. Suricata ICMP alert

It is working!

**TIP** | Make a snapshot!

## 2.5. HIDS

We will use Ubuntu Server as operating system for the NIDS and HIDS VM. The ISO can be downloaded [here](#) (18.04.4).

### 2.5.1. Installation Ubuntu Server 18

This installation is quite similar tot the NIDS installation.

1. In VMware Workstation Pro click on File > New Virtual Machine
2. Select Typical > Next
3. Browse to the downloaded Ubuntu Server ISO > Next
4. Fill in the fields name, username (we use hids), password
5. Give the VM a name, enter 'NIDS' > Next
6. Set the maximum disk size to 80 GB
7. Select 'Store virtual disk size as a single file' > next
8. Click 'Customize hardware'
  - a. Set the amount of memory to 4096 MB
  - b. Set number of processors to 2
  - c. Set number of cores per processor to 2
  - d. Click on 'Network Adapter'
    - Select 'Connect at power on'
    - Select Custom > VMnet1 (Host-only)
  - e. Select 'USB controller' > Click 'Remove'
  - f. Select 'Sound Card' > Click 'Remove'
  - g. Select 'Printer' > Click 'Remove'
  - h. Press Close
9. Press Finish
10. Open the VM settings again
  - a. Remove the CD/ DVD with the 'autoinst.iso' inserted
  - b. Remove the Floppy drive with the 'autoinst.flp' inserted
11. Start the Virtual Machine
12. Go through the installation process
  - a. At the software selection phase, make sure to install OpenSSH server'
13. Shut down the VM after the installation is completed
  - a. Remove the last CD/DVD drive
  - b. Document the MAC-address of the network adapter

14. Log in to the pfSense web UI
  - a. Navigate to Services > DHCP server and select 'LAN'
  - b. Add a Static mapping
    - Mac-address of the NIDS machine (00:0C:29:87:0A:4C)
    - IP Address: 172.16.1.3
  - c. Click 'save' > 'Apply changes'
15. Start up the VM
  - a. Log in
  - b. Verify that the IP-address is 172.16.1.3 (with ifconfig)
  - c. Update the vm with:

```
sudo apt-get update; sudo apt-get upgrade;
```

## 2.5.2. Docker.io

We will use Docker to run the Wazuh server and ELK stack. We have to install docker first.

1. Log into the HIDS VM
2. Install docker

```
curl -sSL https://get.docker.com/ | sh
```

3. Start and automate Docker

```
sudo systemctl enable docker  
sudo systemctl start docker
```

4. Check if docker is installed correctly

```
docker --version
```

```
Docker version 19.03.8, build afacb8b7f0
```

5. Install docker-compose

```
sudo curl -L "https://github.com/docker/compose/releases/download/1.25.4/docker-  
compose-Linux-x86_64" -o /usr/local/bin/docker-compose  
chmod +x /usr/local/bin/docker-compose
```

6. Check if docker-compose is installed correctly

```
docker-compose --version
```

```
docker-compose version 1.25.4, build 8d51620a
```

### 2.5.3. Wazuh Container

We will follow [this](#) guide to deploy the Wazuh container, steps are documented below.

1. Increase max\_map\_count:

```
sudo nano /etc/sysctl.conf
```

At the bottom add this line:

```
vm.max_map_count=262144
```

2. Get the docker-compose.yml

```
curl -so docker-compose.yml https://raw.githubusercontent.com/wazuh/wazuh-docker/v3.11.4_7.6.1/docker-compose.yml
```

3. Get the Wazuh repository

```
git clone https://github.com/wazuh/wazuh-docker.git -b v3.11.4_7.6.1 --single-branch
```

4. Start the stack

```
sudo docker-compose up
```

The installation will take some time. When the installation is done go to <https://172.16.1.3/> in your browser (host machine), default password is 'foo' and 'bar'. You should have access now to the Kibana interface.

5. We want the docker container to start automatically at system start up. Follow the steps below.

- a. Stop the stack (Ctrl-c)
- b. Open docker-compose-app.service (New file)

```
sudo nano /etc/systemd/system/docker-compose-app.service
```

And add the following content:

```
[Unit]
Description=Docker Compose Application Service
Requires=docker.service
After=docker.service

[Service]
Type=oneshot
RemainAfterExit=yes
WorkingDirectory=/home/hids/
ExecStart=/usr/local/bin/docker-compose up -d
ExecStop=/usr/local/bin/docker-compose down
TimeoutStartSec=0

[Install]
WantedBy=multi-user.target
```

c. Enable and start the service

```
sudo systemctl enable docker-compose-app
sudo systemctl start docker-compose-app
```

## 3. Last configuration

### 3.1. pfSense Firewall rules

We will add some extra firewall rules to prevent the Victim accessing other machines in the network (except of de Wazuh server).

#### 3.1.1. WAN interface

We don't need any extra rules for the WAN interface.

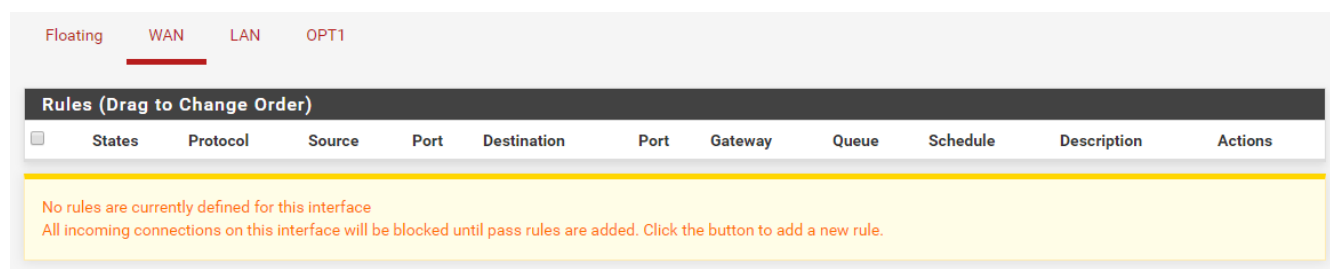


Figure 20. pfSense WAN rules

#### 3.1.2. LAN interface

We want to block all traffic to local networks (the RFC1918 alias we created). However the host machine (172.16.1.2) needs SSH access tot the victim and the HIDS will use the Wazuh Ports 1514 and 1515 to communicate with the victim and retrieve the alerts.

If we keep this in mind the configuration should look like this:

The screenshot shows the pfSense firewall rules configuration for the LAN interface. The 'Rules (Drag to Change Order)' table contains 7 rules. The interface tabs are Floating, WAN, LAN, and OPT1.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/30 KiB	IPv4 UDP	172.16.1.0/24	*	172.16.1.1	53 (DNS)	*	none		Allow DNS traffic to gateway	
0/0 B	IPv4 UDP	172.16.1.0/24	*	172.16.1.1	123 (NTP)	*	none		Allow NTP traffic to gateway	
0/7.35 MiB	IPv4 TCP	172.16.1.2	*	172.16.2.2	22 (SSH)	*	none		Allow SSH acces from host to victim	
2/7.89 MiB	IPv4 TCP	172.16.1.2	*	172.16.1.1	443 (HTTPS)	*	none		pfSense strict anti-lockout	
0/1.39 MiB	IPv4+6 *	*	*	RFC1918	*	*	none		Deny acces to any other RFC1918 networks	
0/25.11 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Figure 21. pfSense LAN rules

#### 3.1.3. OPT1 interface

As with the LAN interface we want to block all traffic to local networks (the RFC1918 alias we created), except for the communication to the HIDS Wazuh server. The Victim machine is allowed to have access to the outside world.

The configuration should look like this:



Floating

WAN

LAN

OPT1

Rules (Drag to Change Order)





























	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 30 KiB	IPv4 UDP	172.16.1.0/24	*	172.16.1.1	53 (DNS)	*	none		Allow DNS traffic to gateway	   
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 UDP	172.16.1.0/24	*	172.16.1.1	123 (NTP)	*	none		Allow NTP traffic to gateway	   
<input type="checkbox"/>	✓ 0 / 7.35 MiB	IPv4 TCP	172.16.1.2	*	172.16.2.2	22 (SSH)	*	none		Allow SSH acces from host to victim	   
<input type="checkbox"/>	✓ 2 / 7.89 MiB	IPv4 TCP	172.16.1.2	*	172.16.1.1	443 (HTTPS)	*	none		pfsense strict anti-lockout	   
<input type="checkbox"/>	✗ 0 / 1.39 MiB	IPv4+6 *	*	*	RFC1918	*	*	none		Deny acces to any other RFC1918 networks	   
<input type="checkbox"/>	✓ 0 / 25.11 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	   
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	   

Figure 22. pfSense OPT1 rules

## 3.2. Register Wazuh agent at Wazuh manager

The installation of both the Victim VM and the HIDS VM is completed, it is time to register the Wazuh agent at the Wazuh Manger.

1. Start the HIDS and run the command:

```
docker-compose exec wazuh /bin/bash
```

- a. Add add the agent with manage\_agents:

```
/var/ossec/bin/manage_agents -a any -n windows-10
```

- b. List the agents

```
/var/ossec/bin/manage_agents -l
```

Available agents:

ID: 004, Name: windows-10, IP: any

- c. Use the ID from the previous command to extract the agents key using:

```
/var/ossec/bin/manage_agents -e 004
```

Agent key information for '004' is:

```
MDA0IHdpbmRvd3MtMTAgYW55IDA3YzI3OTNjYjA3NDJiODAwYjE4ZWUwY2F1ZTk1NGU2MGIwODNiOTFm
MjcycjMGFhMWVjZDg5ZGMwMGU5NDIxMWQ=
```

2. Open a shell at the Victim machine

- a. Import the previous key with manage\_agents

```
'C:\Program Files (x86)\ossec-agent\manage_agents' -i  
MDA0IHdpbmRvd3MtMTAgYW55IDA3YzI3OTNjYjA3NDJiODAwYjE4ZWwY2F1ZTk1NGU2MGUwODNiOTFm  
MjcyMGFhMWVjZDg5ZGMwMGU5NDIxMWQ=
```

```
Agent information:  
ID:004  
Name:windows-10  
IP Address:any  
  
Confirm adding it?(y/n): y  
Added.
```

Figure 23. Wazuh Agent key imported

- b. Restart wazuh-manager (Victim machine)

```
Restart-Service -Name wazuh
```

At the HIDS Kibana interface, the agent should be visible now:

+ Add new agent							
ID	Name	IP	Status	Group	OS name	OS version	Version
004	windows-10	172.16.2.2	Active	default	Microsoft Windows 10 Home	10.0.18363	Wazuh v3.11.4

Figure 24. Wazuh Agent registered Kibana

### 3.3. Install Filebeat on NIDS

Wazuh uses an Elasticsearch database with Kibana to display the alerts. It is possible to send the NIDS alerts to the same Elasticsearch database to centralize the alerts.

1. Open a shell at the NIDS
2. Install Filebeat

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-  
amd64.deb  
sudo dpkg -i filebeat-7.6.1-amd64.deb  
rm filebeat-7.6.1-amd64.deb
```

3. Open the configuration file

```
sudo nano /etc/filebeat/filebeat.yml
```

Find the input section and fill in:

```
- type: log
  enabled: true
  paths:
    - /var/log/snort/alert.fast
    - /var/log/suricata/fast.log
```

Find the output section and fill in:

```
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["172.16.1.2:9200"]

  #api_key: "id:api_key"
  username: "foo"
  password: "bar"
```

#### 4. Enable the Suricata module

```
sudo filebeat modules enable suricata
filebeat setup -e
```

#### 5. Enable and start filebeat

```
sudo systemctl enable filebeat
sudo systemctl start filebeat
```

## 3.4. Wazuh

### 3.4.1. Configure Wazuh Group configuration

We will edit some Wazuh Monitor configuration. All time intervals must be less than 5 minutes because each malware test will last no longer than 10 minutes.

1. Open the Kibana web interface and navigate to the Wazuh App > Management> Groups
2. Press the + to create a new group
  - a. Set the group name to 'Windows10-Machines'
3. Click 'Edit configuration'

Paste the following lines:

```
<!-- Log analysis -->
<localfile>
  <location>Application</location>
```

```

    <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
  <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
    EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660
and
    EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907
and
    EventID != 5152 and EventID != 5157]</query>
</localfile>

<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>active-response\active-responses.log</location>
  <log_format>syslog</log_format>
</localfile>

<!-- Sysmon tool -->
<localfile>
<location>Microsoft-Windows-Sysmon/Operational</location>
<log_format>eventchannel</log_format>
</localfile>

<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <base_directory>C:</base_directory>
  <scanall>yes</scanall>
  <skip_nfs>no</skip_nfs>
  <frequency>60</frequency>
  <check_dev>yes</check_dev>
  <check_files>no</check_files>
  <check_if>yes</check_if>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_sys>yes</check_sys>
  <check_trojans>no</check_trojans>
  <check_winaudit>no</check_winaudit>
  <check_winmalware>yes</check_winmalware>
  <check_winapps>yes</check_winapps>
  <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
  <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

```

```

<!-- Security Configuration Assessment -->
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>4m</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>60</frequency>

  <!-- Default files to be monitored. -->
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\regedit.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\system.ini</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\win.ini</directories>

  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\at.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\attrib.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\cacls.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\cmd.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\drivers\etc</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\eventcreate.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\ftp.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\lsass.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\net.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\net1.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\netsh.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\reg.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\regedt32.exe</directories>
  <directories check_all="yes" realtime="yes"

```

```

whodata="yes">%WINDIR%\SysNative\regsvr32.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\runas.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\sc.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\schtasks.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\sethc.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\subst.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\wbem\WMIC.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\WindowsPowerShell\v1.0\powershell.exe</directories>
>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\SysNative\winrm.vbs</directories>

  <!-- 32-bit programs. -->
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\at.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\attrib.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\cacls.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\cmd.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\drivers\etc</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\eventcreate.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\ftp.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\net.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\net1.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\netsh.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\reg.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\regedit.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\regedt32.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\regsvr32.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\runas.exe</directories>
  <directories check_all="yes" realtime="yes"

```

```

whodata="yes">%WINDIR%\System32\sc.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\schtasks.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\sethc.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\subst.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\wbem\WMIC.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\WindowsPowerShell\v1.0\powershell.exe</directories>
  <directories check_all="yes" realtime="yes"
whodata="yes">%WINDIR%\System32\winrm.vbs</directories>
  <directories check_all="yes" realtime="yes" whodata="yes"
report_changes="yes">%PROGRAMDATA%\Microsoft\Windows\Start
Menu\Programs\Startup</directories>
  <directories check_all="yes" realtime="yes" report_changes="yes"
whodata="yes">C:\Users\John Williams\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup</directories>
  <ignore>%PROGRAMDATA%\Microsoft\Windows\Start
Menu\Programs\Startup\desktop.ini</ignore>
  <ignore>C:\Users\John Williams\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\desktop.ini</ignore>
  <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

  <!-- Windows registry entries to monitor. -->

<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</windows_registry>

<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</windows_registry>

<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\comfile</windows_registry>

<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\exefile</windows_registry>

<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\piffile</windows_registry>

<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\AllFileSystemObjects</windows_registry>

<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Directory</windows_registry>
  <windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\Folder</windows_registry>
  <windows_registry
arch="both">HKEY_LOCAL_MACHINE\Software\Classes\Protocols</windows_registry>
  <windows_registry
arch="both">HKEY_LOCAL_MACHINE\Software\Policies</windows_registry>
  <windows_registry>HKEY_LOCAL_MACHINE\Security</windows_registry>
  <windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer</windows_registry>

```

```

<windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services</windows_registry>
  <windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
  Manager\KnownDLLs</windows_registry>

<windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg</windows_registry>

  <windows_registry
  arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</windows_registry>
  <windows_registry
  arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</windows_registry>

<windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</windows_registry>
  <windows_registry
  arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\URL</windows_registry>
  <windows_registry
  arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies</windows_registry>
  <windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</windows_registry>
  <windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon</windows_registry>

  <windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components</windows_registry>

  <!-- added manually -->
  <windows_registry arch="both">HKEY_USERS\S-1-5-21-438079597-2123118846-2669748851-1001\Software\Microsoft\Windows\CurrentVersion\Run</windows_registry>
  <windows_registry arch="both">HKEY_USERS\S-1-5-21-438079597-2123118846-2669748851-1001\Software\Microsoft\Windows\CurrentVersion\RunOnce</windows_registry>

  <!-- Windows registry entries to ignore. -->
  <registry_ignore>HKEY_LOCAL_MACHINE\Security\Policy\Secrets</registry_ignore>

<registry_ignore>HKEY_LOCAL_MACHINE\Security\SAM\Domains\Account\Users</registry_ignore>
  <registry_ignore type="sregex">\Enum$</registry_ignore>

<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\AppCs</registry_ignore>

<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\DHCP</registry_ignore>

```



```

<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\IPTLSIn</registry_ignore>

<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\IPTLSOut</registry_ignore>

<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\RPC-EPMAP</registry_ignore>

<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\Teredo</registry_ignore>

<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PolicyAgent\Parameters\Cache</registry_ignore>

<registry_ignore>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</registry_ignore>

<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ADOVMPPackage\Final</registry_ignore>

    <!-- Frequency for ACL checking (seconds) -->
    <windows_audit_interval>240</windows_audit_interval>
</syscheck>

<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>4m</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="yes">yes</ports>
  <processes>yes</processes>
</wodle>

<!-- Active response -->
<active-response>
  <disabled>no</disabled>
  <ca_store>wpk_root.pem</ca_store>
  <ca_verification>yes</ca_verification>
</active-response>

```

Summary changes made from default configuration:

- Sysmon tool:

```
<!-- Sysmon tool -->
<localfile>
<location>Microsoft-Windows-Sysmon/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
```

- Rootcheck:
  - a. Frequency: 60
- Security Configuration Assessment (SCA):
  - a. interval: 4m
- Syscheck:
  - a. Frequency: 60 seconds
  - b. For all directories: realtime="yes" whodata="yes"
  - c. For `%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>`:  
report\_changes="yes"
  - d. Added `directory` to `monitor`: `C:\Users\John Williams\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
  - e. Added 2 Windows registry entries to monitor:

```
<!-- added manually -->
<windows_registry arch="both">HKEY_USERS\S-1-5-21-438079597-2123118846-
2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\Run</windows_registry>
<windows_registry arch="both">HKEY_USERS\S-1-5-21-438079597-2123118846-
2669748851-
1001\Software\Microsoft\Windows\CurrentVersion\RunOnce</windows_registry>
```

- System inventory (wodle name="syscollector")
  - a. Interval: 4m
  - b. Ports all: yes

### 3.4.2. Sysmon Second Batch

In the first batch of the malware research (10 samples) Wazuh did not detect any malware but only some indicators. That is why we will install a ruleset using Sysmon to enhance the detection capabilities. We will use the ruleset from [Hetstat](#).

1. Start the victim machine
2. Download the System tool and unzip it:  
<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>
3. Download the following configuration (the .xml file) and move it to the unzipped System tool folder

<https://github.com/SwiftOnSecurity/sysmon-config>

4. Open PowerShell as administrator and navigate to the unzipped folder
  - a. Install Sysmon with the following command:

```
.\Sysmon64.exe -accepteula -i sysmonconfig-export.xml
```

5. Make sure the following lines are added to the Wazuh Group Configuration:

```
<localfile>  
<location>Microsoft-Windows-Sysmon/Operational</location>  
<log_format>eventchannel</log_format>  
</localfile>
```

6. Open the kibana web interface
  - a. Navigate to Wazuh > Management > Ruleset
  - b. Click 'Manage rules files' and open 'local\_rules.xml'
  - c. Add the following line at the bottom:

```
<!-- https://raw.githubusercontent.com/Hestat/ossec-  
sysmon/master/local_rules.xml -->
```

- d. Paste content from [https://raw.githubusercontent.com/Hestat/ossec-sysmon/master/local\\_rules.xml](https://raw.githubusercontent.com/Hestat/ossec-sysmon/master/local_rules.xml) underneath
  - e. Click Save and restart now

### 3.4.3. Sysmon Third Batch

Contrary to expectations, the results of batch 2 were (almost) no better than batch 1. But we analyzed the Sysmon events generated after the execution and the corresponding rules. We founded several critical bugs why no alerts were generated. The first option was to correct these rules and test them again. But we decided we need a more elaborate version of Sysmon rules, so we started writing a script to generate OSSEC / Wazuh rules from Sigma rules (<https://github.com/Neo23x0/sigma>). The result is that we have written all Windows Sigma rules to the OSSEC format, both the rules and the script are available [here](#).

1. Start the victim machine
2. Download the sysmonconfig.xml from [sigWah](#):
  - a. Install the configuration with the following command:

```
.\Sysmon64.exe -i sysmonconfig.xml
```

3. Make sure the following lines are added to the Wazuh Group Configuration:

```
<localfile>
<location>Microsoft-Windows-Sysmon/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
```

#### 4. Open the kibana web interface

- a. Navigate to Wazuh > Management > Ruleset
- b. Click 'Manage rules files' and open 'local\_rules.xml'
- c. Remove the old Sysmon rules and add the following line at the bottom:

```
<!-- https://github.com/SanWieb/sigWah -->
```

- d. Paste content from [https://github.com/SanWieb/sigWah/master/local\\_rules.xml](https://github.com/SanWieb/sigWah/master/local_rules.xml) underneath
- e. Click Save and restart now

## 3.5. Tor / VPN Tunneling

To prevent to give away your own IP-address to the malware developers it is possible to configure a Tor Network at the pfSense VM or a VPN. [Here](#) are the steps described to install a Tor-network and [here](#) to configure a Free VPN (ProtonVPN) . Alternatively you could use a Mobile phone / Raspberry Pi to setup a network with 3/4G.

We will use the last option because we have a unlimited data abonnement available.

## 4. Cuckoo Sandbox

Follow [this guide](#) to setup the Cuckoo Sandbox environment.