Building a Custom Malware Analysis Lab Environment

labs.sentinelone.com/building-a-custom-malware-analysis-lab-environment/

Marco Figueroa

Introduction

Building the right malware analysis environment is the first step for every malware researcher. When all system configurations and software installations are complete, you're able to analyze and investigate malware properly. In this post, I wanted to share my own experiences and scripts to help ease the workload of setting up a malware environment to explore malicious software.

In this post, you will learn how to:

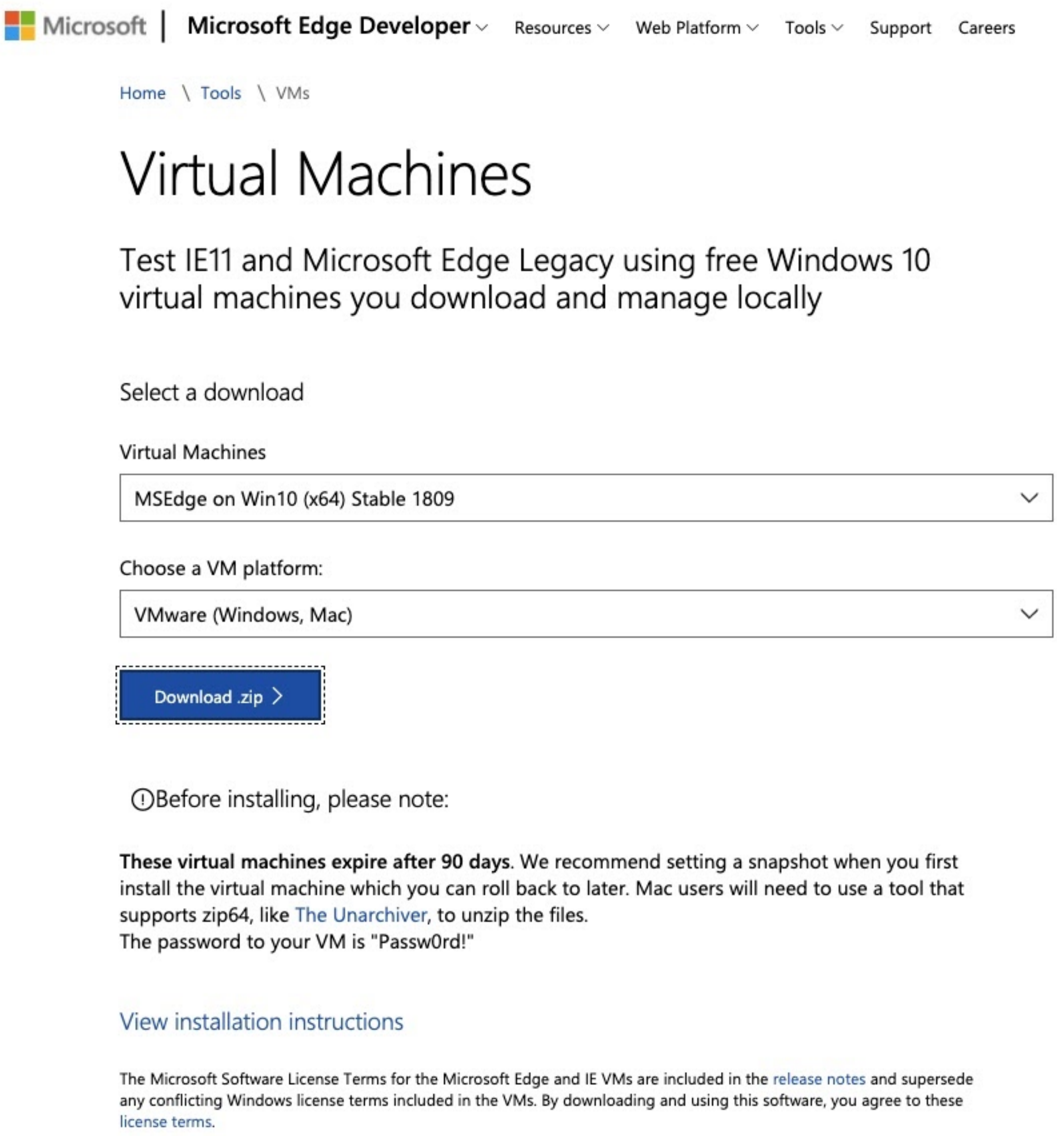
1. download, install and configure a free Windows 10 and a free REMnux Linux virtual machine
2. set up a virtual private network for communication between virtual machines
3. build a custom Windows malware environment with SentinelLabs RevCore Tools
4. learn how to capture network traffic from a Windows 10 virtual machine

Installing Virtual Machines

When running multiple virtual machines, the host operating system will begin slowing down, so it is critical to set each virtual machine's best requirements to optimize its performance. To set up the virtual machines in this post, I recommend that the Windows 10 virtual machine be set with the minimum requirements of two processor cores with 4GB of RAM and the Linux virtual machine with two processor cores with 2GB of RAM.

Downloading a Free Windows 10 Installation

Microsoft provides a free virtual machine which is intended for testing IE and Edge web browsers. To download the Microsoft virtual machine go to https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ and download the MSEdge on Windows 10 zip file and select your preferred VM platform, currently I'm using VM Fusion.



Virtual Machines

Test IE11 and Microsoft Edge Legacy using free Windows 10 virtual machines you download and manage locally

Select a download

Virtual Machines: MSEdge on Win10 (x64) Stable 1809

Choose a VM platform: VMware (Windows, Mac)

ⓘBefore installing, please note:

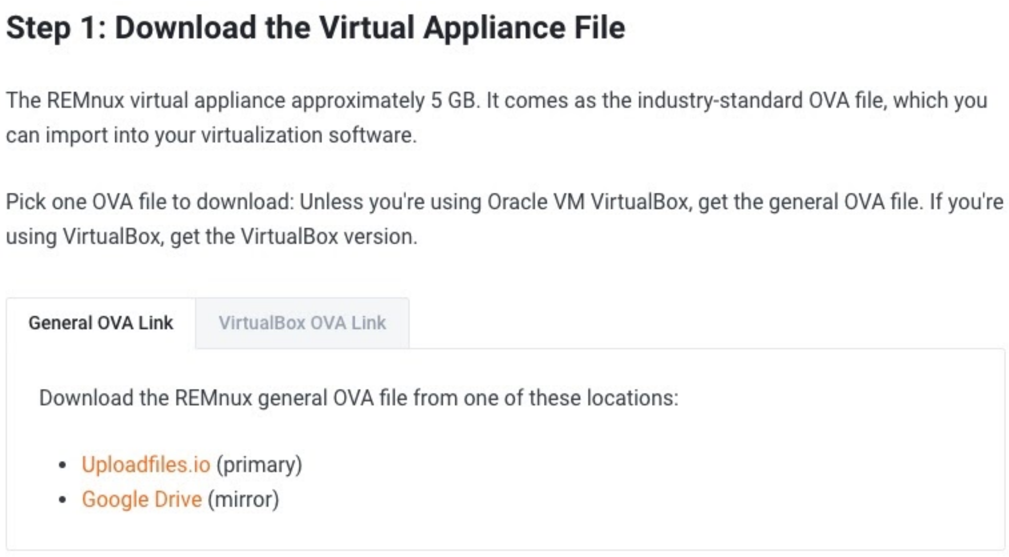
These virtual machines expire after 90 days. We recommend setting a snapshot when you first install the virtual machine which you can roll back to later. Mac users will need to use a tool that supports zip64, like The Unarchiver, to unzip the files.
The password to your VM is "Passw0rd!"

View installation instructions

The Microsoft Software License Terms for the Microsoft Edge and IE VMs are included in the release notes and supersede any conflicting Windows license terms included in the VMs. By downloading and using this software, you agree to these license terms.

Downloading REMnux Linux

The next virtual machine we want to download is REMnux Linux. The REMnux distro is a Linux distribution based on Ubuntu. It has excellent tools for exploring network interactions for behavioral analysis and investigating system-level interactions of malware. To download REMnux go to https://docs.remnux.org/install-distro/get-virtual-appliance and download the Virtual Machine platform of your choice.



Step 1: Download the Virtual Appliance File

The REMnux virtual appliance approximately 5 GB. It comes as the industry-standard OVA file, which you can import into your virtualization software.

Pick one OVA file to download: Unless you're using Oracle VM VirtualBox, get the general OVA file. If you're using VirtualBox, get the VirtualBox version.

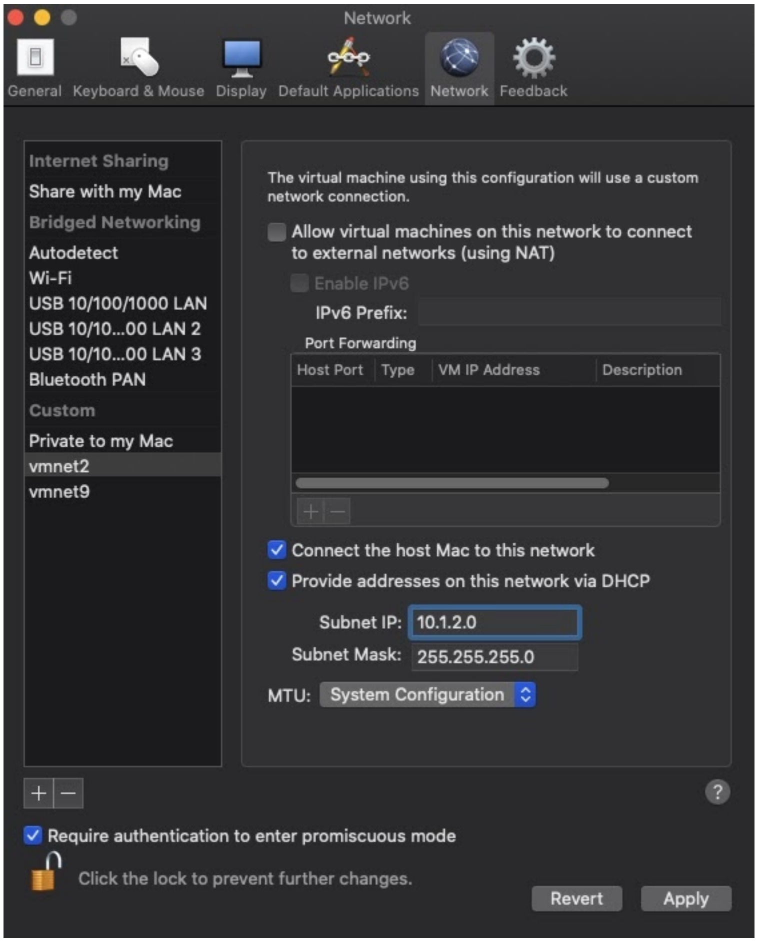
Download the REMnux general OVA file from one of these locations:

- Uploadfiles.io (primary)
- Google Drive (mirror)

Installing and Configuring a Private Isolated Custom Network

Creating an isolated, controlled network environment when analyzing malware is extremely important due to the level of interaction it gives you with malware. VMware Fusion gives you the capabilities to change key networking settings and add a virtual private network configuration to use for analysis between hosts. We will only add two virtual machines to this lab environment, but you can add many virtual machines to this network. The procedures to create this network is as follows:

- Select the tab **VMware Fusion->Preferences->Network**; click the lock icon to make changes
- Select the “**+**” button which creates a `vmnet#` under the **Custom** section.
- Do ***not*** select the *“Allow Virtual machines on this network to connect to external networks (using NAT)”* option.
- Add a *Subnet IP*: I’ve entered `10.1.2.0`
- Click **Apply**



The virtual machine using this configuration will use a custom network connection.

□ Allow virtual machines on this network to connect to external networks (using NAT)

□ Enable IPv6

IPv6 Prefix:

☑ Connect the host Mac to this network

☑ Provide addresses on this network via DHCP

Subnet IP: 10.1.2.0

Subnet Mask: 255.255.255.0

MTU: System Configuration

☑ Require authentication to enter promiscuous mode

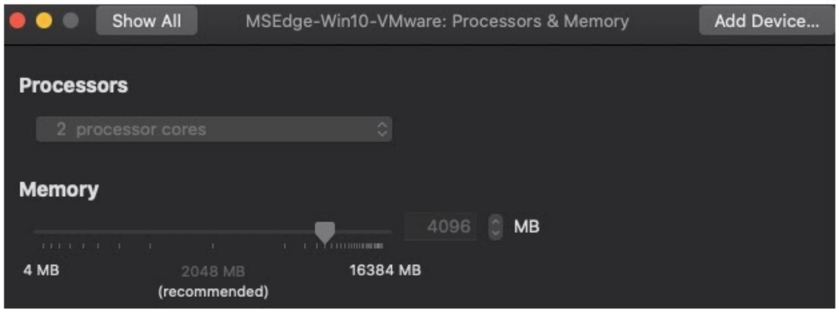
Click the lock to prevent further changes.

Windows 10 Setup

Once you've created a custom network and both virtual machines have been downloaded, begin by unzipping the MSEdge Windows 10. Since I'm using VMware Fusion, I will go through how to import the virtual image; the process for importing the virtual machine with other platforms is similar.

Open up VMware Fusion and follow these steps:

1. After the zip has been unpacked enter the MSEdge-Win10-VMware folder.
2. Select in VMware Fusion **File->Import MSEdge_Win10_VMware**, hit **Continue** and save the Virtual Machine; it will take a few minutes to import the image.
3. Click on **Customize Settings** after the image has been imported.
4. Click into the **Processors & Memory** tab and confirm that the settings has two processor cores and the memory is 4096MB.
5. Before powering on the MSEdge Win10 virtual machine, take a snapshot and name it something like "VM Clean Import".
6. When starting the virtual machine, if prompted to upgrade the virtual machine to greater feature compatibility support, choose **Upgrade**.
7. The password to the virtual machine is `Passw0rd!`
8. Open the command prompt to activate the virtual machine, type `slmgr.vbs /ato`.
9. When prompted, install VMware's "Virtual Tools" and reboot.
10. Once the virtual machine has rebooted, complete login and immediately take a snapshot. Give it a descriptive name, such as "Activation and VM Tools Install" snapshot.

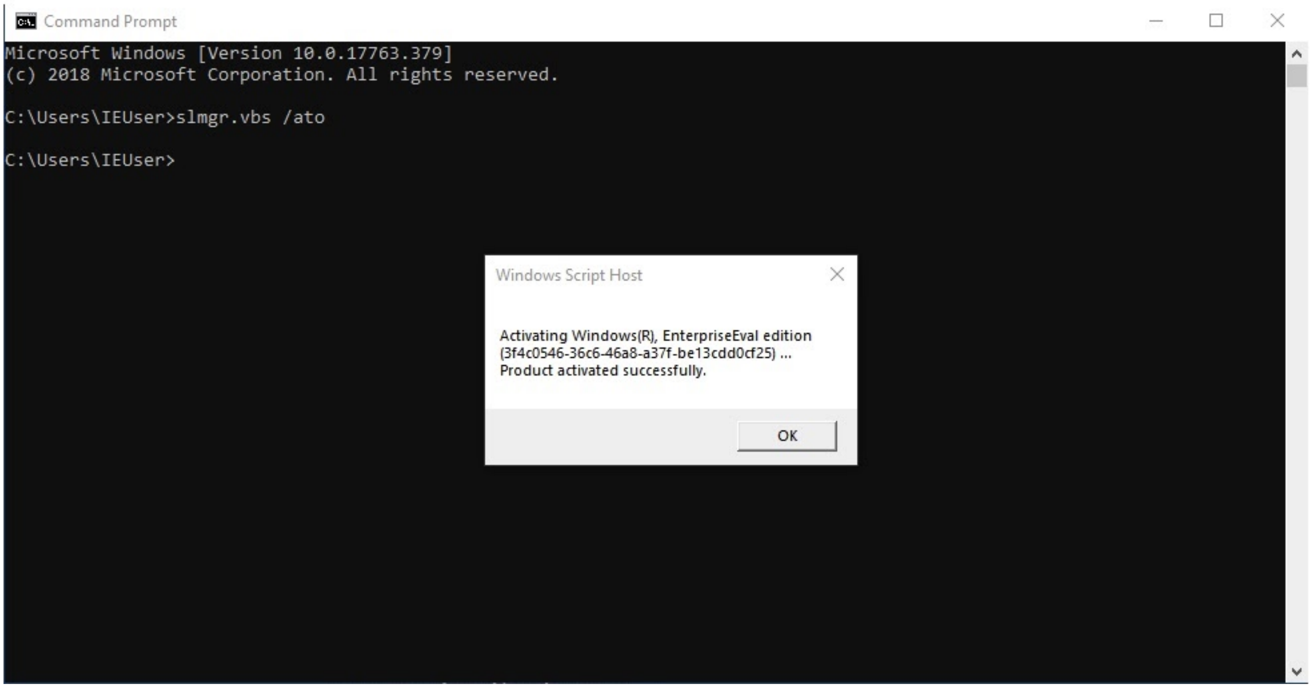


Processors

2 processor cores

Memory

4096 MB



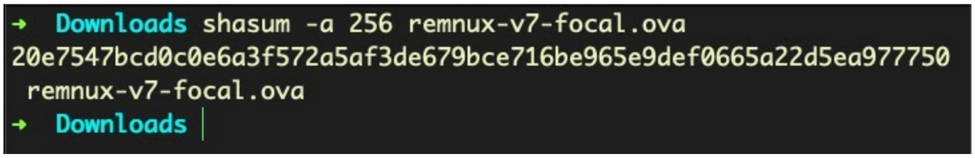
```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>slmgr.vbs /ato

C:\Users\IEUser>
```

Windows Script Host

Activating Windows(R), EnterpriseEval edition (3f4c0546-36c6-46a8-a37f-be13cdd0cf25) ...
Product activated successfully.

REMnux Setup

The REMnux virtual machine downloads as an `.ova` file. I recommend you browse to docs.REMnux.org to confirm the hash of the downloaded OVA file.



```
→  Downloads shasum -a 256 remnux-v7-focal.ova
20e7547bcd0c0e6a3f572a5af3de679bce716be965e9def0665a22d5ea977750
 remnux-v7-focal.ova
→  Downloads
```

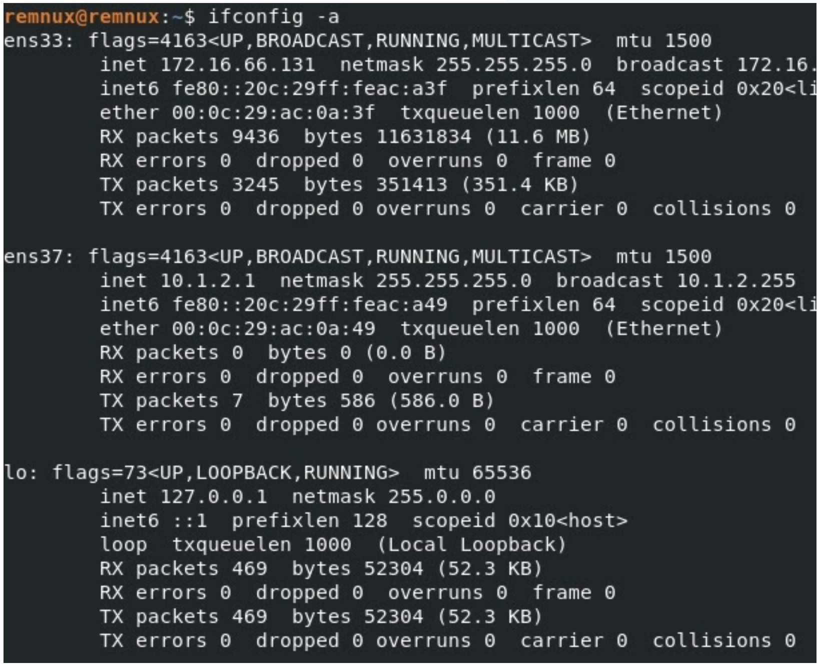
If you are using VirtualBox, you can just import REMnux, but if you are using VMware Fusion or VMware Workstation, follow these instructions to import the REMnux:

1. Select **File->Import->Choose File…** and select *remnux-v7*, hit **Continue** and then **Save**.
2. When the import is complete, click on **Customize Settings**.
3. Click into the **Processors & Memory** pane under *System Settings* and leave the settings with two processor cores; reduce the memory from 4096MB to 2048MB.
4. For the REMnux network configuration, the setup is slightly different. We want to add an additional network adapter.*Note*: There are multiple reasons why I configure this virtual machine this way. If I need to update or download other software having the network adapter configured saves me time; the second is if I want to allow malware callouts.Once the import is complete and you're in the "Settings" menu, select **Network Adapter**. The next step is to click **Add Device…** and select **Network Adapter** and **Add…**. Make sure the *Share with my Mac* radio button is set. Return to the main "Settings" panel and select **Network Adapter 2**. Click the *vmnet2* radio button, then choose **Show All** to go back to Settings.
5. When starting the REMnux virtual machine, if prompted to upgrade the virtual machine to greater feature compatibility support, choose **Upgrade**.
6. Once REMnux boots, the credentials are: Username: `remnux` Password: `malware` .

7. I always change the password on my virtual machines:

    1.
       ```
       $passwd
       UNIX password: malware
       Enter new UNIX password: (your choice)
       ```

8. The next step is to configure the network settings. If you type `ifconfig -a` you should see two network adapters:
    1. Select NAT for the first network adapter. The virtual machine will get an address on that network from the VMware virtual DHCP server. You can ping google to see if you have connectivity or open the Firefox browser and connect to any website to confirm that you have internet access. If you do not, then type this command in terminal: `$ sudo dhclient -r` This should allow you to fetch an IP.
    2. For the second adapter, ens37, type in this command: `$ sudo ifconfig ens37 10.1.2.1 netmask 255.255.255.0`



```
remnux@remnux:~$ ifconfig -a
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.66.131  netmask 255.255.255.0  broadcast 172.16.
        inet6 fe80::20c:29ff:feac:a3f  prefixlen 64  scopeid 0x20<li
        ether 00:0c:29:ac:0a:3f  txqueuelen 1000  (Ethernet)
        RX packets 9436  bytes 11631834 (11.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3245  bytes 351413 (351.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.2.1  netmask 255.255.255.0  broadcast 10.1.2.255
        inet6 fe80::20c:29ff:feac:a49  prefixlen 64  scopeid 0x20<li
        ether 00:0c:29:ac:0a:49  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 586 (586.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 469  bytes 52304 (52.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 469  bytes 52304 (52.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

9. Hit the “Snapshot” button and name it something like “Clean Snapshot”.
10. Update and upgrade REMnux: `$ sudo apt-get update; sudo apt-get upgrade`

Installing SentinelLabs RevCore Tools

One of the reasons I wanted to create a SentinelLabs VM Bare Bones malware analysis toolkit was that when installing FlareVM, I find it contains many tools that I do not use, and it takes a minimum of 40 minutes to install. I wanted to create a script of the core tools and system configurations that I need to be able to analyze malware.

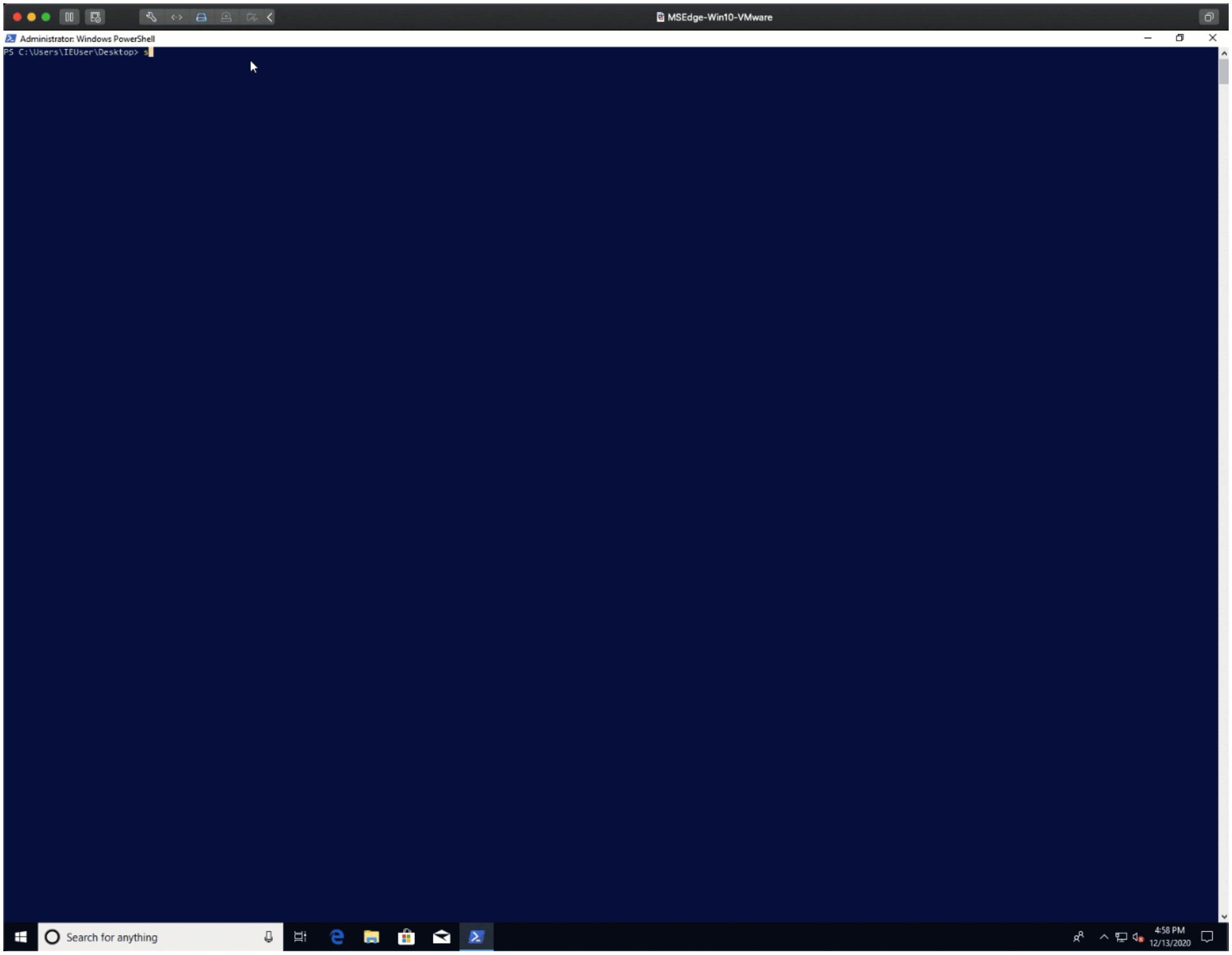
Follow this procedure to instal SentinelLabs RevCore Tools on MSEdge WIndows 10:

1. Browse to the SentinelLabs RevCore Tools github page and download the zip.
2. Unzip it and drag the `SentinelLabs_RevCore_Tools_codeSnippet.ps1` script onto your desktop.
3. If you are using the free downloaded Windows 10 virtual machine that I’ve mentioned above go to Step 4; if you are using your own Windows virtual machine continue with these substeps:
    1. Instead of dragging just the `SentinelLabs_RevCore_Tools_codeSnippet.ps1`, drag the entire folder onto your virtual machine desktop.
    2. Open the `SentinelLabs_RevCore_Tools_codeSnpippet.ps1` file and modify line 4 after `-PackageName.` You will modify the url and change it to the directory location on your desktop. E.g., `'https://raw.githubusercontent.com/SentineLabs/SentinelLabs_RevCore_Tools/master/SentinelLabs_RevCore_Tools.ps` to `'c:UsersyourUsernameDesktopSentinelLabs_RevCore_Tools-mainSentinelLabRevCoreTools.ps1' ;`
    3. The final thing to do is to modify the `SentinelLabsRevCoreTools.ps1.` On lines 105-117, replace `IEUser` with the User profiles name you are using. Save all files and run the script. E.g.,

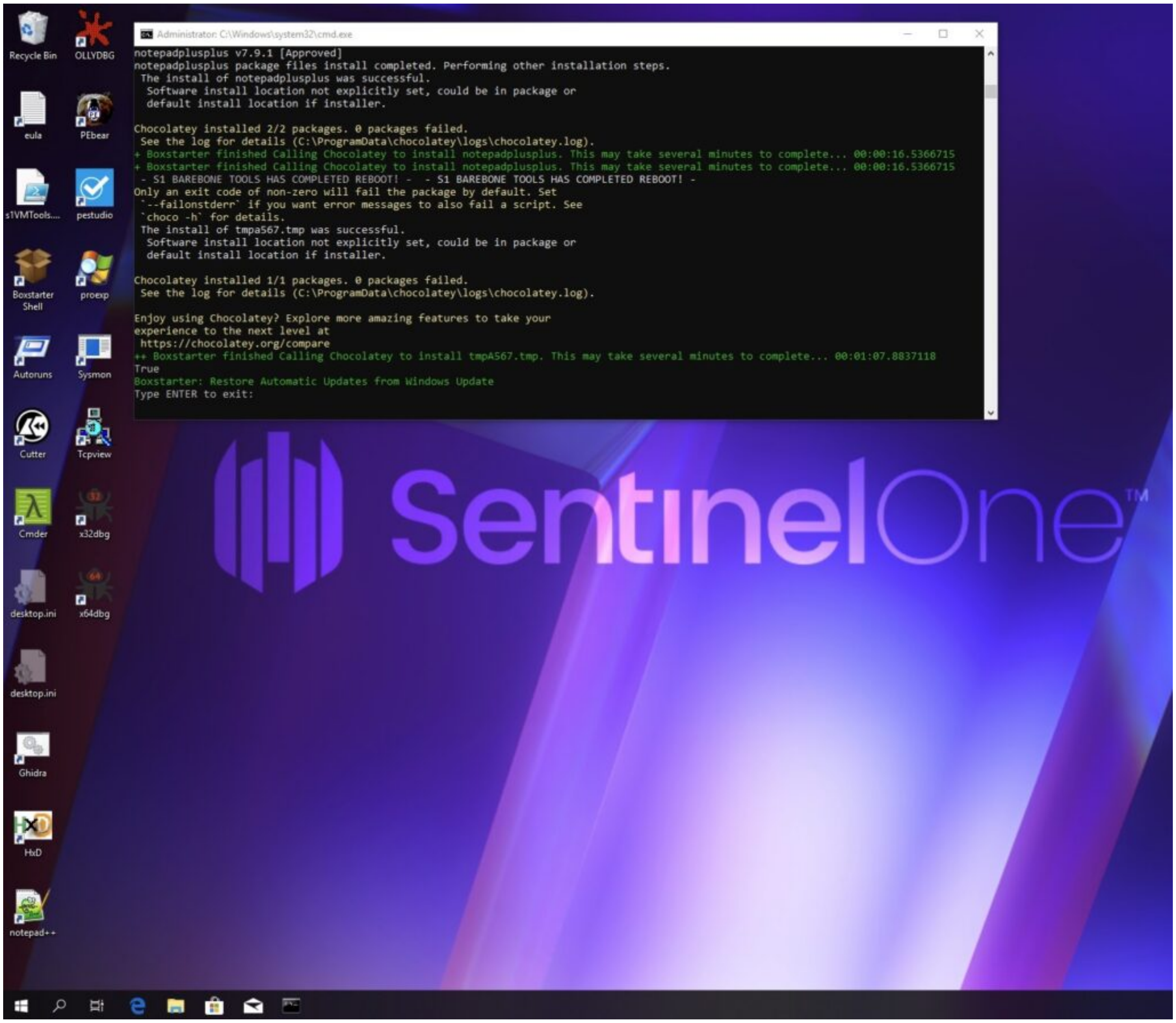
       ```
       Install-ChocolateyShortcut -ShortcutFilePath "C:\Users\IEUser\Desktop\HxD.lnk" -TargetPath "C:\Program Files\HxD\HxD.exe"

       Install-ChocolateyShortcut -ShortcutFilePath "C:\Users\YourUser Profile\Desktop\HxD.lnk" -TargetPath "C:\Program
       Files\HxD\HxD.exe"
       ```

    4. Go to Step 5.
4. In the Windows 10 search bar, type `powershell`, right click and run as administrator. Browse to the location of the `SentinelLabs_RevCore_Tools_codeSnippet.ps1` powershell script, then run the script: `.SentinelLabs_RevCore_Tools_codeSnippet.ps1` .

5. The script will cause two automatic reboots, and you’ll need to log in again with your user password after each. The first reboot will continue disabling various system services that could otherwise hinder your malware analysis and continue to install the core tools. After the second reboot, the script will finalize and confirm all of the configurations and installations.The installed tools and modified system configurations are listed below. Don’t forget to take a snapshot when it’s finished and you’ve reached the “Type ENTER to exit” point.
    1. **Tools:**
       Checksum, 7zip, Process Explorer, Autoruns, TCPview, Sysmon, HxD, PEbear, PEStudio, PEsieve, Cmder, NXlog, X64dbg, X32dbg, Ollydbg, IDA-Free, Cutter, Ghidra, Openjdk11, Python3, PIP, PIP pefile, PIP YaraA tool that I frequently use is Hiew, Chocolatey does not have Hiew in its collection. My recommendation is to download and try out the free version, once you see the power of Hiew you should definitely purchase lifetime access because it is worth every penny.
    2. **System Configuration:**
       Disabling – Bing Search, Game Bar Tips, Computer Restore, UAC, Update, Firewall, Windows Defender, Action Center
       Set Window Theme, Set Wallpaper, Create Shortcuts For Tools



```
PS C:\Users\IEUser\Desktop> s
```



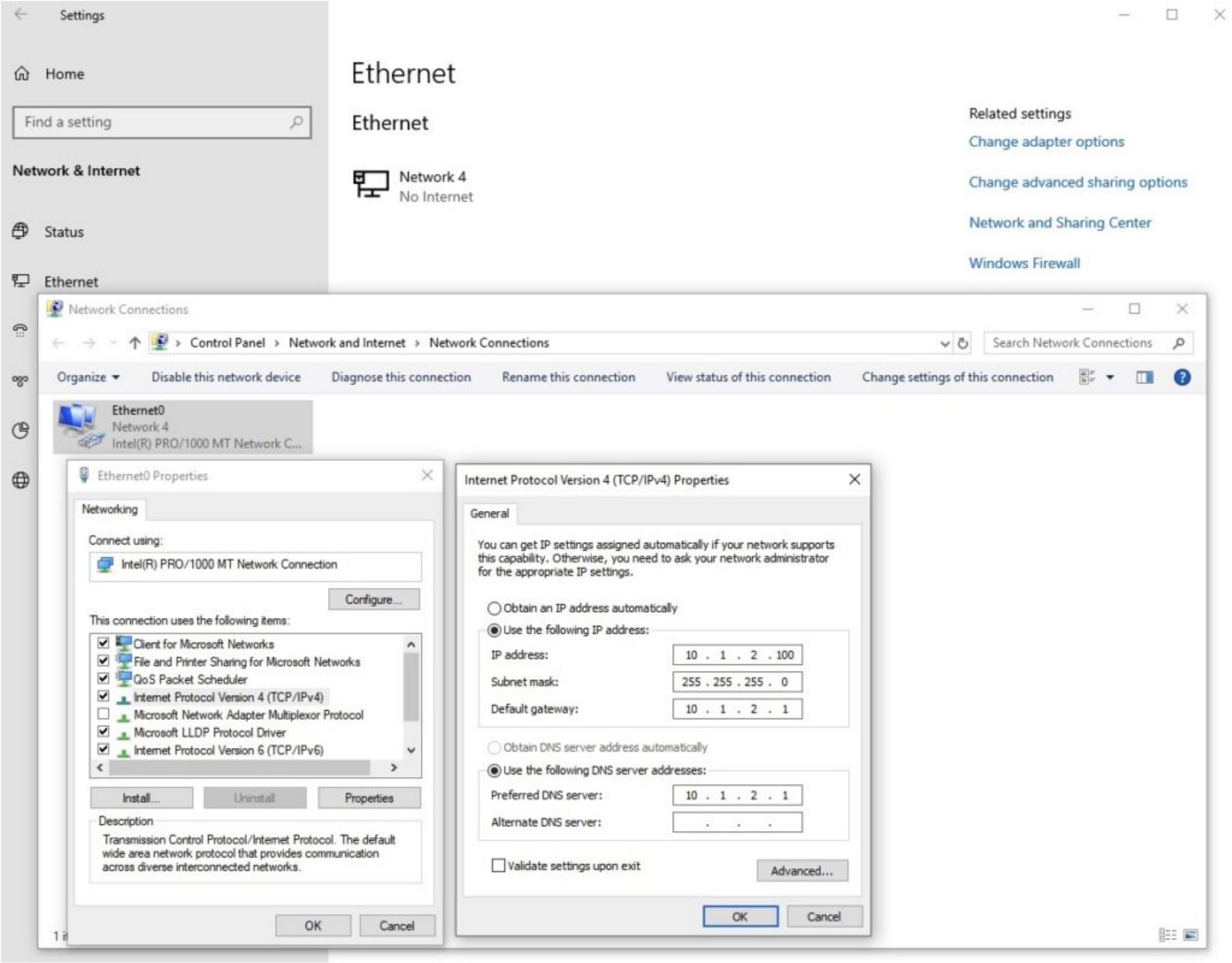
```
notepadplusplus v7.9.1 [Approved]
notepadplusplus package files install completed. Performing other installation steps.
 The install of notepadplusplus was successful.
  Software install location not explicitly set, could be in package or
  default install location if installer.

Chocolatey installed 2/2 packages. 0 packages failed.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
+ Boxstarter finished Calling Chocolatey to install notepadplusplus. This may take several minutes to complete... 00:00:16.5366715
+ Boxstarter finished Calling Chocolatey to install notepadplusplus. This may take several minutes to complete... 00:00:16.5366715
 - S1 BAREBONE TOOLS HAS COMPLETED REBOOT! -  - S1 BAREBONE TOOLS HAS COMPLETED REBOOT! -
Only an exit code of non-zero will fail the package by default. Set
 `--failonstderr` if you want error messages to also fail a script. See
 `choco -h` for details.
 The install of tmpa567.tmp was successful.
  Software install location not explicitly set, could be in package or
  default install location if installer.

Chocolatey installed 1/1 packages. 0 packages failed.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Enjoy using Chocolatey? Explore more amazing features to take your
experience to the next level at
 https://chocolatey.org/compare
++ Boxstarter finished Calling Chocolatey to install tmpA567.tmp. This may take several minutes to complete... 00:01:07.8837118
True
Boxstarter: Restore Automatic Updates from Windows Update
Type ENTER to exit:
```

Network Traffic Collection

When analyzing malware, often the malware operation and the C2s are still active, so an excellent way to stay under the radar is to run malware in a controlled environment. Analyzing network traffic is a trivial process in detecting malicious software callouts in real time network traffic. This section will help you configure your virtual machines to capture the detonated malicious software's network traffic or statically step through debugged code, which allows your investigation to understand the potential threat at hand.

The first thing that must be configured is the virtual private network communication between the MSEdge Windows 10 and REMnux:

1. On the Windows 10 virtual machine, select the custom `vmnet2` network (**Virtual Machine->Network Adapter->Custom (vmnet2)**).
2. On the Windows 10 VM, right click on the network adapter in the taskbar and choose *Open Network & Internet settings*.
3. Select *Ethernet* and click on **Change adapter options**.
4. Right click on *Ethernet0* and select **Properties**.
5. Double click on *Internet Protocol Version 4 (TCP/IPv4)*.
6. Click the radio button to select "*Use the following IP address:*", then add the IP address, Subnet mask, Default gateway, and Preferred DNS server as follows:
    1. IP Address: 10.1.2.100
    2. Subnet mask: 255.255.255.0
    3. Default Gateway: 10.1.2.1
    4. Click the radio button to select *"Use the following DNS server address:"* and add:
       Preferred DNS Server: 10.1.2.1
    5. Click **OK** to complete configuration of the network settings.



Ethernet0 Properties

Connect using:
Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

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

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: 10 . 1 . 2 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 1 . 2 . 1

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

Preferred DNS server: 10 . 1 . 2 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

The REMnux adapter for the virtual private network has already been configured from the previous section.

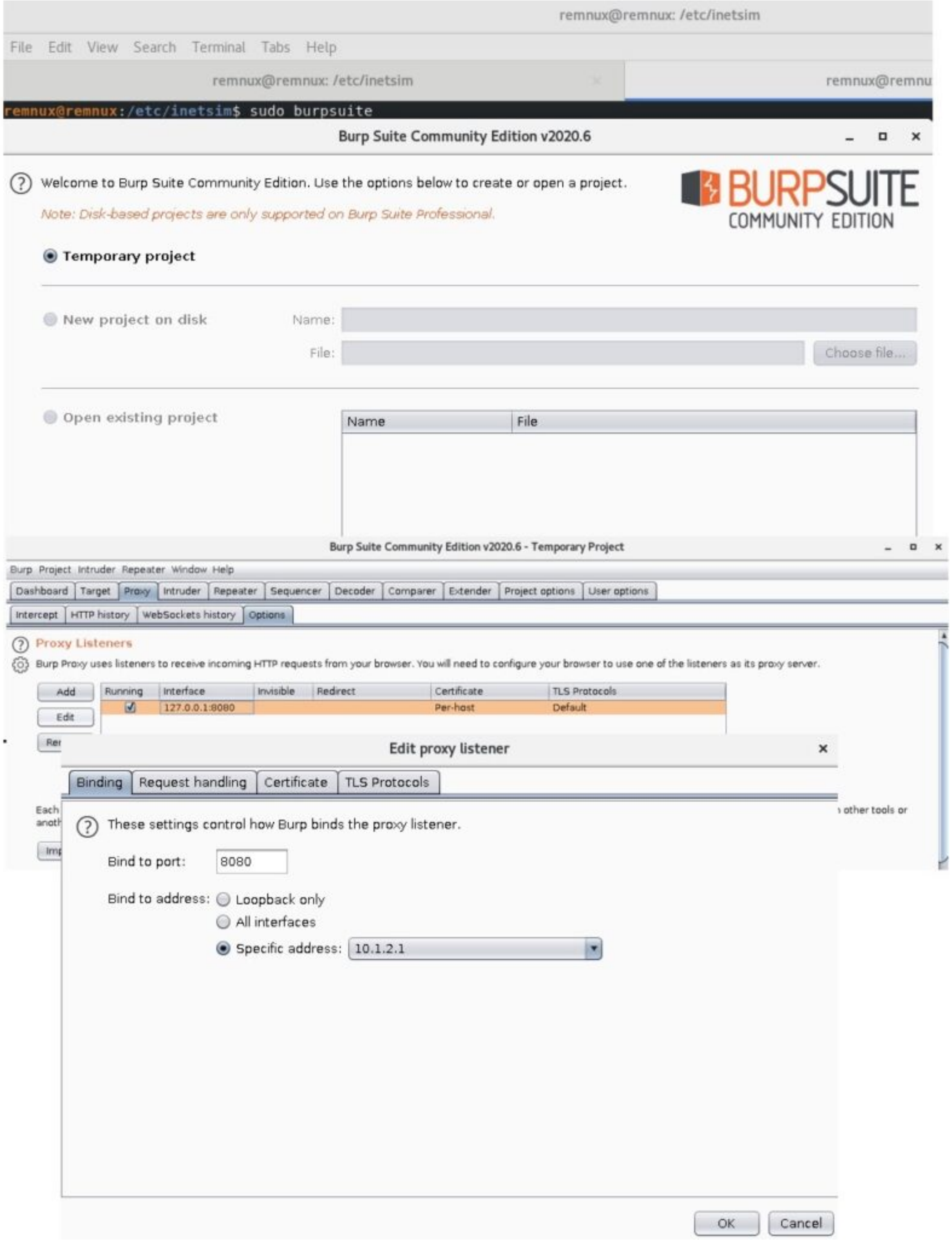
Now that the virtual machines are networked and can communicate with each other, it is time to configure a few tools on the REMnux virtual machine to capture traffic.

Installed on REMnux are various tools you can use to capture network traffic. We will configure Burp Suite and INetSim. Burp Suite is typically used to test web application firewalls, but in our case we want to configure it so that when Windows 10 detonates malware, it will try to establish a connection to a domain or C2. The traffic will potentially use HTTPS and pass through Burp Suite, which will be bound to INetSim. INetSim is a software suite that simulates common services for lab environments to analyze malware’s network behavior.

Burp Suite Configuration

The Burp Suite setup is straightforward, but there are a couple of steps that we must configure before we can begin using it.

- Open a command prompt and type: `$ sudo Burp Suite`.
- select *Temporary project*, then hit **Next** and then **Start Burp**.
- Select the **Proxy** tab and then “Options”. Under *Proxy Listeners*, select the default interface and click the **Edit** button.
- Under the **Binding** tab, set *Bind to address* to *Specific address: 10.1.2.1* and click **OK**.


remnux@remnux: /etc/inetsim
File Edit View Search Terminal Tabs Help
remnux@remnux: /etc/inetsim
remnux@remnu
Burp Suite Community Edition v2020.6
BURPSUITE
COMMUNITY EDITION
Burp Suite Community Edition v2020.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Add
Edit
Edit proxy listener
Binding Request handling Certificate TLS Protocols
OK
Cancel

```
remnux@remnux:/etc/inetsim$ sudo burpsuite
```

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project

○ New project on disk — Name: — File: — Choose file...

○ Open existing project

Name	File

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

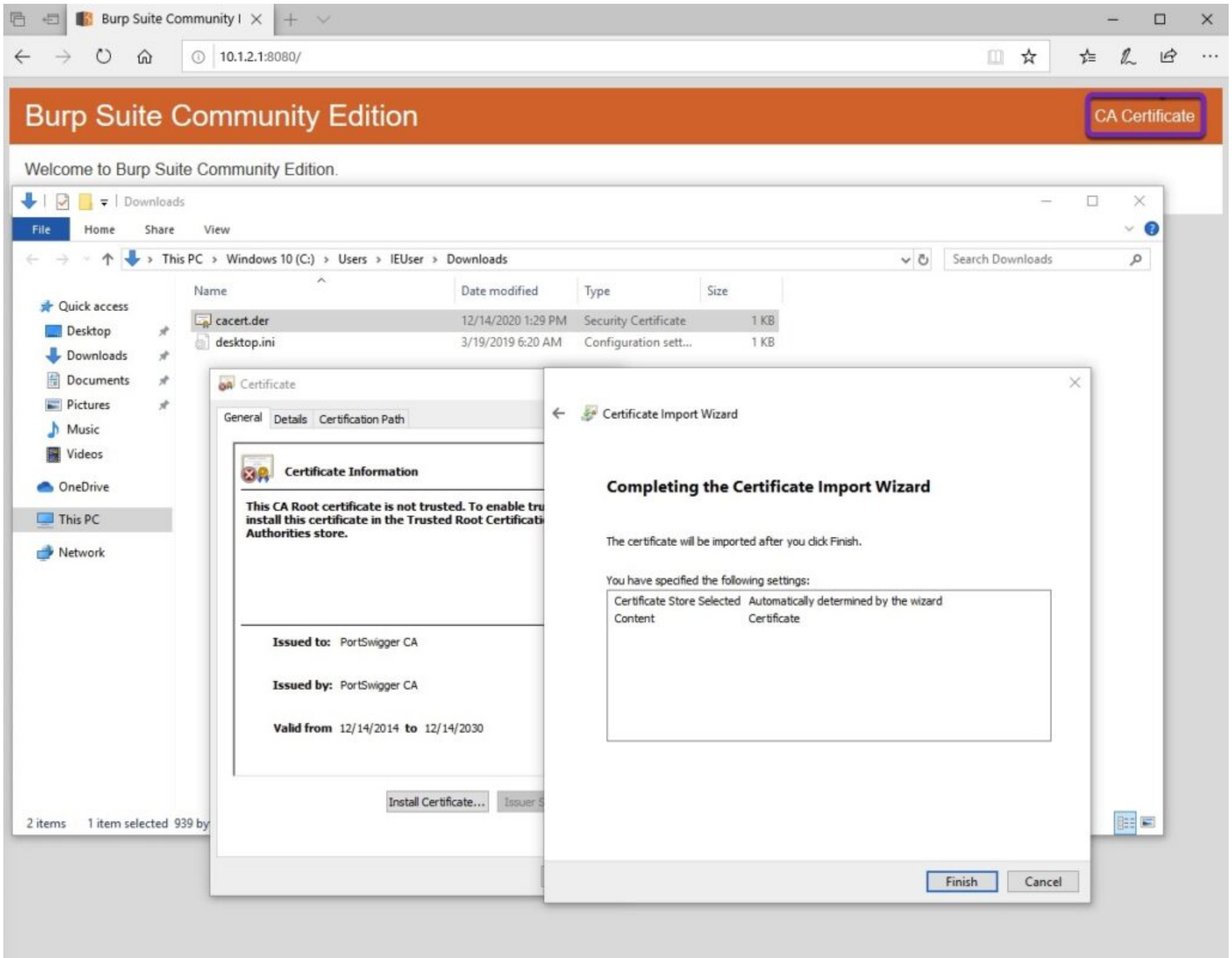
These settings control how Burp binds the proxy listener.

Bind to port: 8080

Bind to address: ○ Loopback only
○ All interfaces
● Specific address: 10.1.2.1

IMPORTANT STEP:

- Go back to you MSEDGE Windows 10 virtual machine and open up the Edge browser.
- Type in the address bar: `http://10.1.2.1:8080`. You should see “Burp Suite Community Edition”.
- Download the CA Certificate on the top right side of the page.
- Open the location of the file and double click on the certificate file.
- Select `Install Certificate...` .
- Select `Current User` as the Store Location and click `Next` .
- Select `Automatically select the certificate store based on the type of certificate` . Click `Next` and then click `Finish` .
- Go into the settings of the EDGE Browser and disable all security functionalities; this will help with testing the connection to INetSim in the next section.
- Make sure you take a snapshot.



Burp Suite Community Edition

Welcome to Burp Suite Community Edition.

Name	Date modified	Type	Size
cacert.der	12/14/2020 1:29 PM	Security Certificate	1 KB
desktop.ini	3/19/2019 6:20 AM	Configuration sett...	1 KB

2 items 1 item selected 939 by

Certificate Information

This CA Root certificate is not trusted. To enable tru install this certificate in the Trusted Root Certificati Authorities store.

Issued to: PortSwigger CA

Issued by: PortSwigger CA

Valid from 12/14/2014 to 12/14/2030

Completing the Certificate Import Wizard

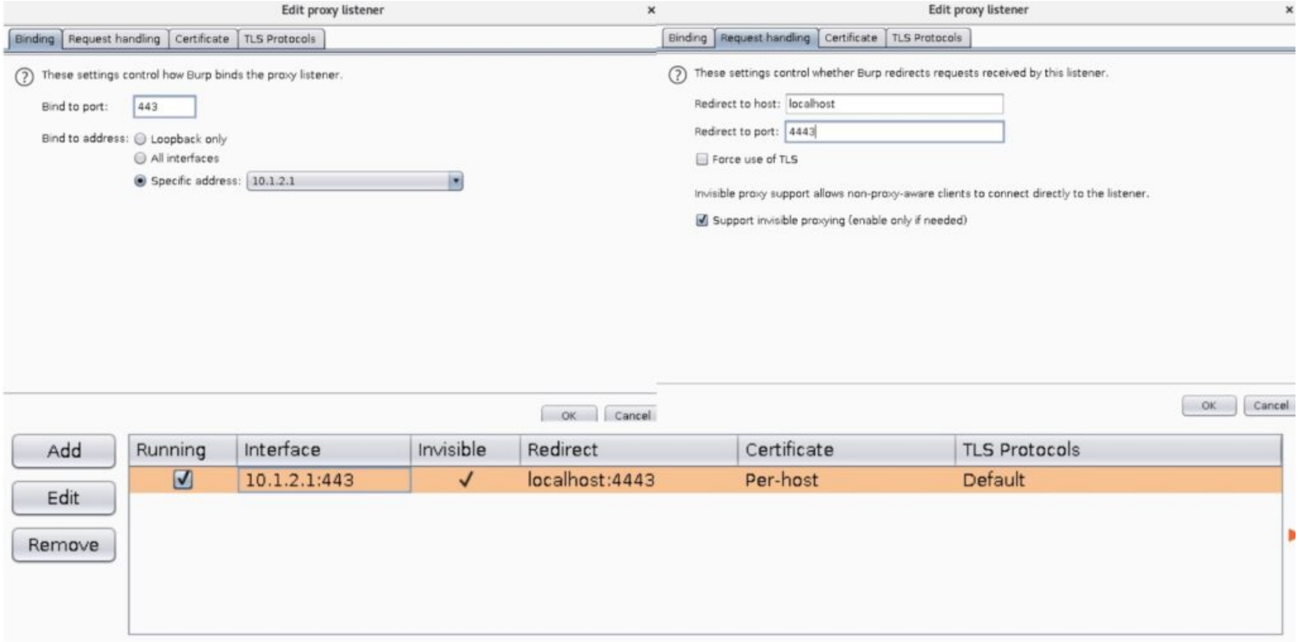
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

Go back to the REMnux virtual machine. You should still be in Burp Suite Proxy tab, *Edit proxy listener* options.

- Under the **Request handling** tab, set *Redirect to host* to `localhost` and *Redirect to port* to `4443` . Select *support for invisible proxying*.
- Now go to the **Intercept** tab and make sure *intercept* is **off**.
- Under **Proxy Listeners**, select the default and click `Edit`
- Under the Binding tab, `Bind to address: Specific address: 10.1.2.1` should still be kept, but change the *Bind* to port `443`
- Click on the **Request handling** tab and set the *Redirect to host* option to `localhost` and `Redirect to port` to `4443.`
- Select the *Support invisible proxying (enable only if needed.)* and click **OK**.



Edit proxy listener

Binding | Request handling | Certificate | TLS Protocols

These settings control how Burp binds the proxy listener.

Bind to port: 443

Bind to address: ○ Loopback only
○ All interfaces
● Specific address: 10.1.2.1

Edit proxy listener

Binding | Request handling | Certificate | TLS Protocols

These settings control whether Burp redirects requests received by this listener.

Redirect to host: localhost

Redirect to port: 4443

□ Force use of TLS

Invisible proxy support allows non-proxy-aware clients to connect directly to the listener.

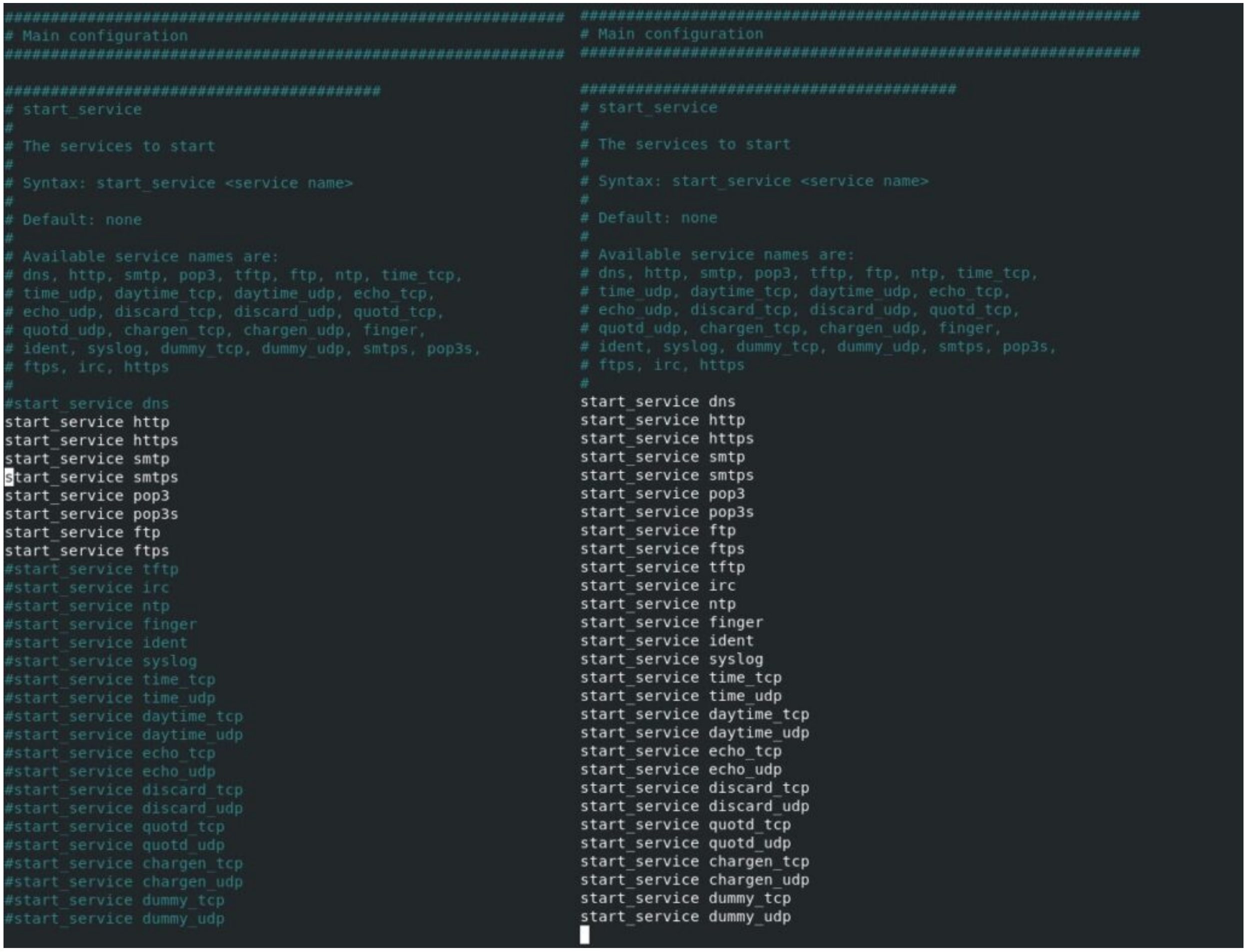
☑ Support invisible proxying (enable only if needed)

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	10.1.2.1:443	✓	localhost:4443	Per-host	Default

INetSim Configuration Setup

REMnux has INetSim preinstalled. Use your favorite text editor and open up the `inetsim.conf` file located in `/etc/inetsim/` . Follow the steps to configure INetSim:

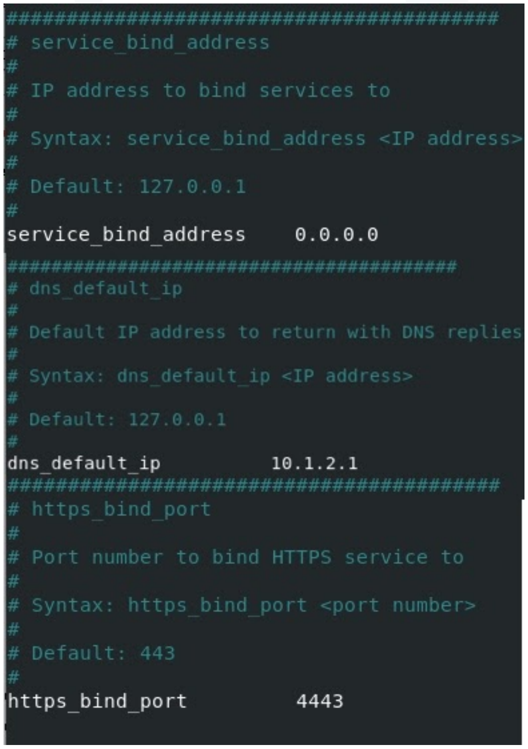
1. `$ sudo vi /etc/inetsim/inetsim.conf` and enable all the services by uncommenting out the services by deleting the `#` character.*Pro Tip:* Be aware that malware could potentially detect it is running in a virtual environment by checking whether everything in this file is uncommented. I have yet to come across this, but it is good to be aware of the possibility. You could take a more conservative approach and only uncomment services you intend to use.



```
#############################################################
# Main configuration
#############################################################

#########################################
# start_service
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
#start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
#start_service echo_tcp
#start_service echo_udp
#start_service discard_tcp
#start_service discard_udp
#start_service quotd_tcp
#start_service quotd_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp
```

```
#############################################################
# Main configuration
#############################################################

#########################################
# start_service
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
start_service tftp
start_service irc
start_service ntp
start_service finger
start_service ident
start_service syslog
start_service time_tcp
start_service time_udp
start_service daytime_tcp
start_service daytime_udp
start_service echo_tcp
start_service echo_udp
start_service discard_tcp
start_service discard_udp
start_service quotd_tcp
start_service quotd_udp
start_service chargen_tcp
start_service chargen_udp
start_service dummy_tcp
start_service dummy_udp
```

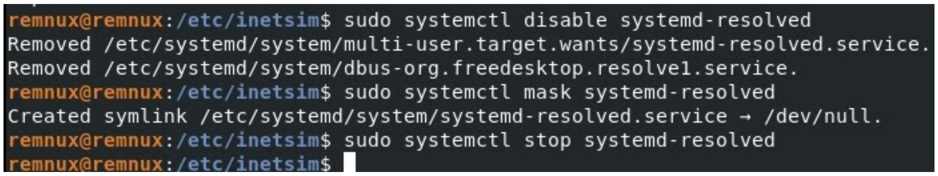
2. The next step is to bind the REMnux network adapter IP in the `inetsim.conf` file. The next section after the services menu is the `service_bind_address` . Uncomment the `#` and change the default IP address from 10.10.10.1 to `0.0.0.0` .
3. Scroll down to the `dns_default_ip` section, uncomment the `#` and change the IP address from 10.10.10.1 to `10.1.2.1` .
4. The last thing to do is to bind the HTTPS port so Burp Suite can route the traffic to the port 4443. Scroll down to the `https_bind_port` section, uncomment the `#` character and replace 443 with `4443` .



```
#########################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address    0.0.0.0
#########################################
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip          10.1.2.1
#########################################
# https_bind_port
#
# Port number to bind HTTPS service to
#
# Syntax: https_bind_port <port number>
#
# Default: 443
#
https_bind_port         4443
```

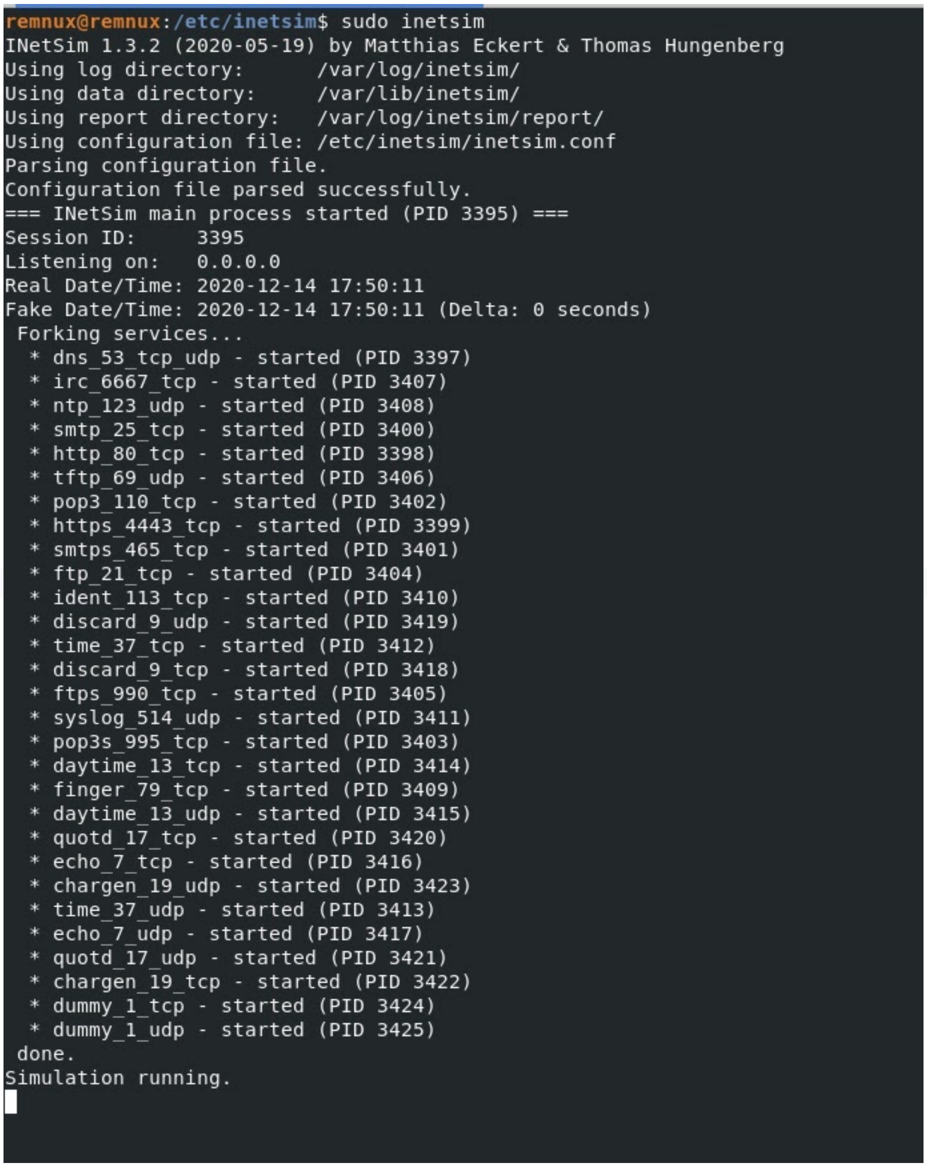
5. Save the changes and exit the editor.
6. The next step is to run the following commands which are VERY IMPORTANT to execute or INetSim will not work correctly. Ubuntu has a system-resolved system service which provides network name resolution to local applications. This conflicts with INetSim so we need to disable the service.We have to disable `system-resolve` and also mask it so that it doesn't auto start on reboot. Finally, we will stop the service.

```
$ sudo systemctl disable systemd-resolved
$ sudo systemctl mask systemd-resolved
$ sudo systemctl stop systemd-resolved
```



```
remnux@remnux:/etc/inetsim$ sudo systemctl disable systemd-resolved
Removed /etc/systemd/system/multi-user.target.wants/systemd-resolved.service.
Removed /etc/systemd/system/dbus-org.freedesktop.resolve1.service.
remnux@remnux:/etc/inetsim$ sudo systemctl mask systemd-resolved
Created symlink /etc/systemd/system/systemd-resolved.service → /dev/null.
remnux@remnux:/etc/inetsim$ sudo systemctl stop systemd-resolved
remnux@remnux:/etc/inetsim$
```

7. The final step is to run INetSim:

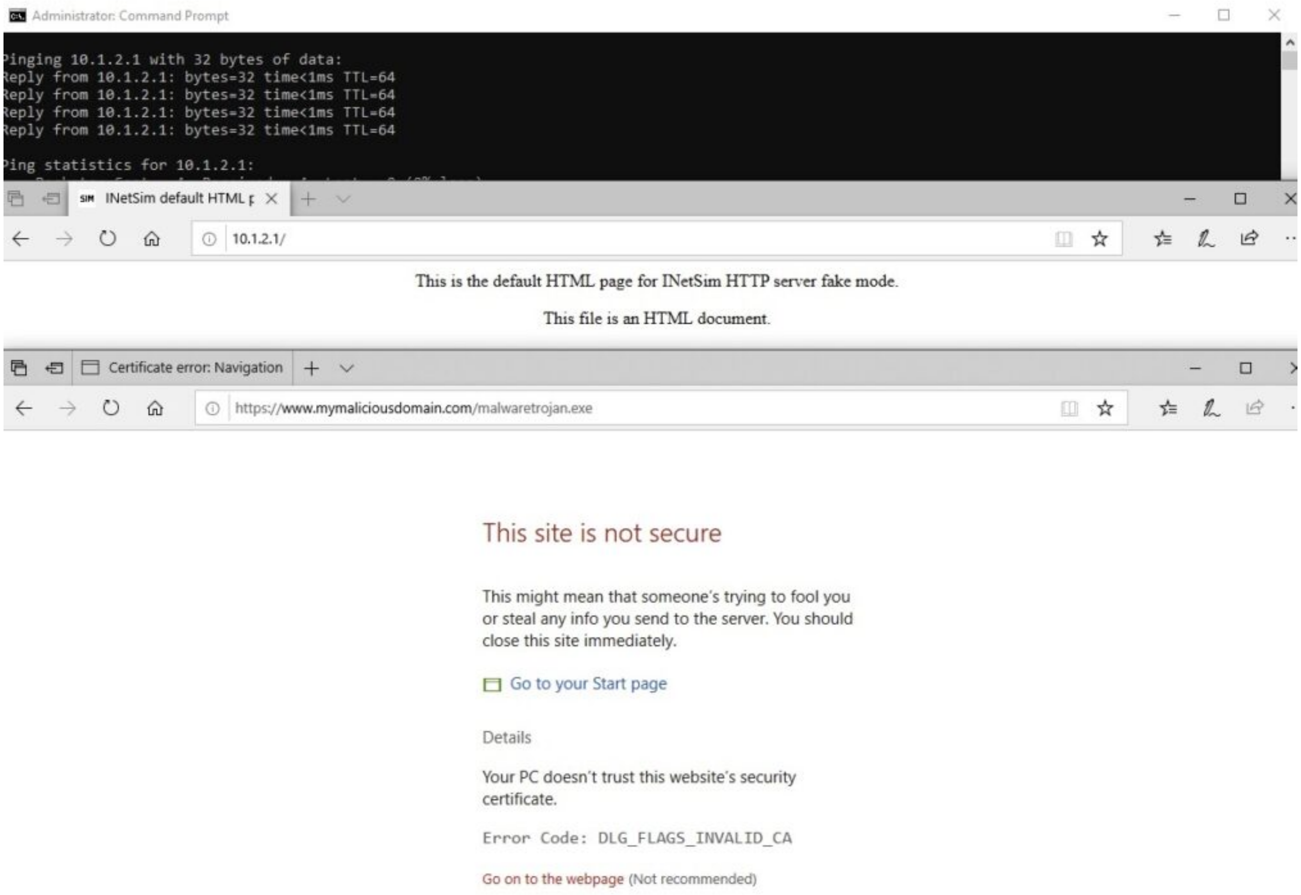


```
remnux@remnux:/etc/inetsim$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 3395) ===
Session ID:     3395
Listening on:   0.0.0.0
Real Date/Time: 2020-12-14 17:50:11
Fake Date/Time: 2020-12-14 17:50:11 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 3397)
  * irc_6667_tcp - started (PID 3407)
  * ntp_123_udp - started (PID 3408)
  * smtp_25_tcp - started (PID 3400)
  * http_80_tcp - started (PID 3398)
  * tftp_69_udp - started (PID 3406)
  * pop3_110_tcp - started (PID 3402)
  * https_4443_tcp - started (PID 3399)
  * smtps_465_tcp - started (PID 3401)
  * ftp_21_tcp - started (PID 3404)
  * ident_113_tcp - started (PID 3410)
  * discard_9_udp - started (PID 3419)
  * time_37_tcp - started (PID 3412)
  * discard_9_tcp - started (PID 3418)
  * ftps_990_tcp - started (PID 3405)
  * syslog_514_udp - started (PID 3411)
  * pop3s_995_tcp - started (PID 3403)
  * daytime_13_tcp - started (PID 3414)
  * finger_79_tcp - started (PID 3409)
  * daytime_13_udp - started (PID 3415)
  * quotd_17_tcp - started (PID 3420)
  * echo_7_tcp - started (PID 3416)
  * chargen_19_udp - started (PID 3423)
  * time_37_udp - started (PID 3413)
  * echo_7_udp - started (PID 3417)
  * quotd_17_udp - started (PID 3421)
  * chargen_19_tcp - started (PID 3422)
  * dummy_1_tcp - started (PID 3424)
  * dummy_1_udp - started (PID 3425)
 done.
Simulation running.
```

```
$ sudo inetsim
```

To test network connectivity from your Windows 10 virtual machine, open a command prompt and ping 10.1.2.1, then open Edge browser and type 10.1.2.1. You should see the following message “*This is the default HTML page for INetSim HTTP server fake mode.*”

The final test is to make sure the DNS is working correctly and serving up requests. For this example, I type in the search bar `https://www.mymaliciousdomain.com/malwaretrojan.exe`. If everything is working, you should see a web page warning that the requested site is not secure.


Administrator: Command Prompt
INetSim default HTML p
10.1.2.1/
Certificate error: Navigation
https://www.mymaliciousdomain.com/malwaretrojan.exe

```
Pinging 10.1.2.1 with 32 bytes of data:
Reply from 10.1.2.1: bytes=32 time<1ms TTL=64
Reply from 10.1.2.1: bytes=32 time<1ms TTL=64
Reply from 10.1.2.1: bytes=32 time<1ms TTL=64
Reply from 10.1.2.1: bytes=32 time<1ms TTL=64

Ping statistics for 10.1.2.1:
```

This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

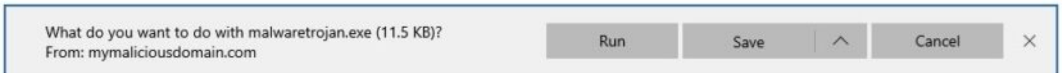
Go to your Start page

Details

Your PC doesn't trust this website's security certificate.

Error Code: DLG_FLAGS_INVALID_CA

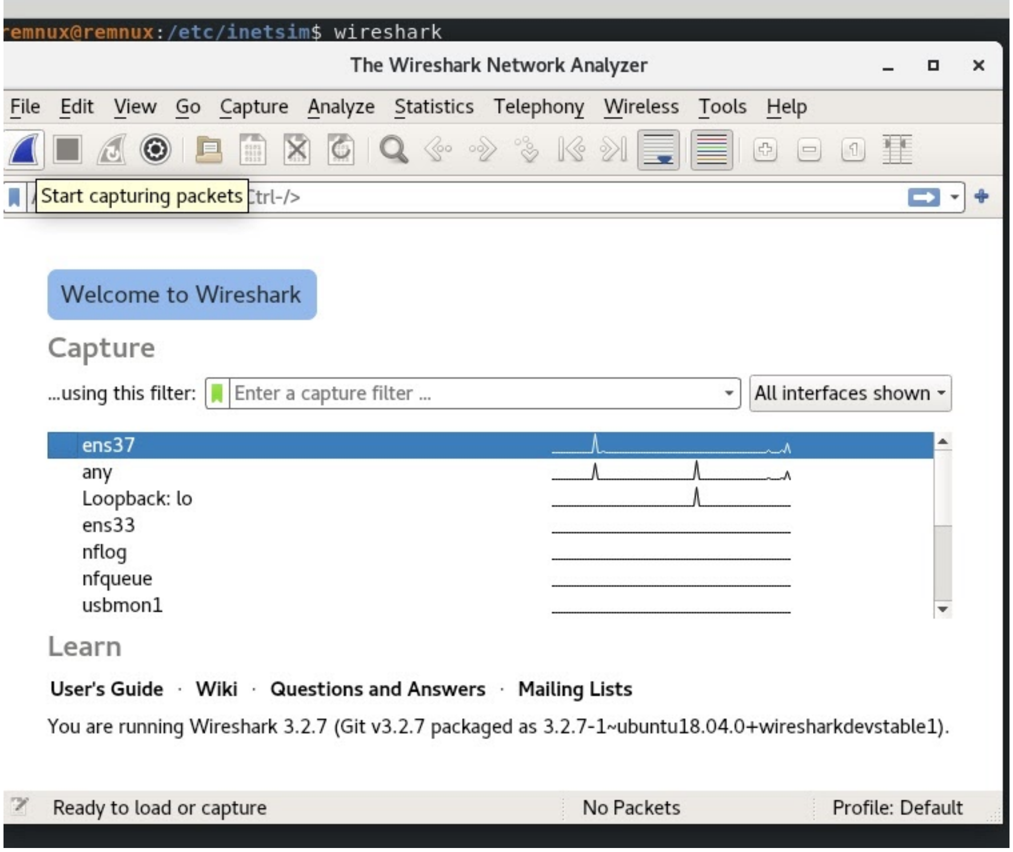
Go on to the webpage (Not recommended)


What do you want to do with malwaretrojan.exe (11.5 KB)?
From: mymaliciousdomain.com

I also like using Wireshark to capture packets to analyze the pcaps when investigating malware.

Open a new tab in your terminal in REMnux and type `$ wireshark`.

Once the application has opened, click on the shark fin icon on the far left of the toolbar to begin capturing packets.



```
remnux@remnux:/etc/inetsim$ wireshark
```

You are running Wireshark 3.2.7 (Git v3.2.7 packaged as 3.2.7-1~ubuntu18.04.0+wiresharkdevstable1).

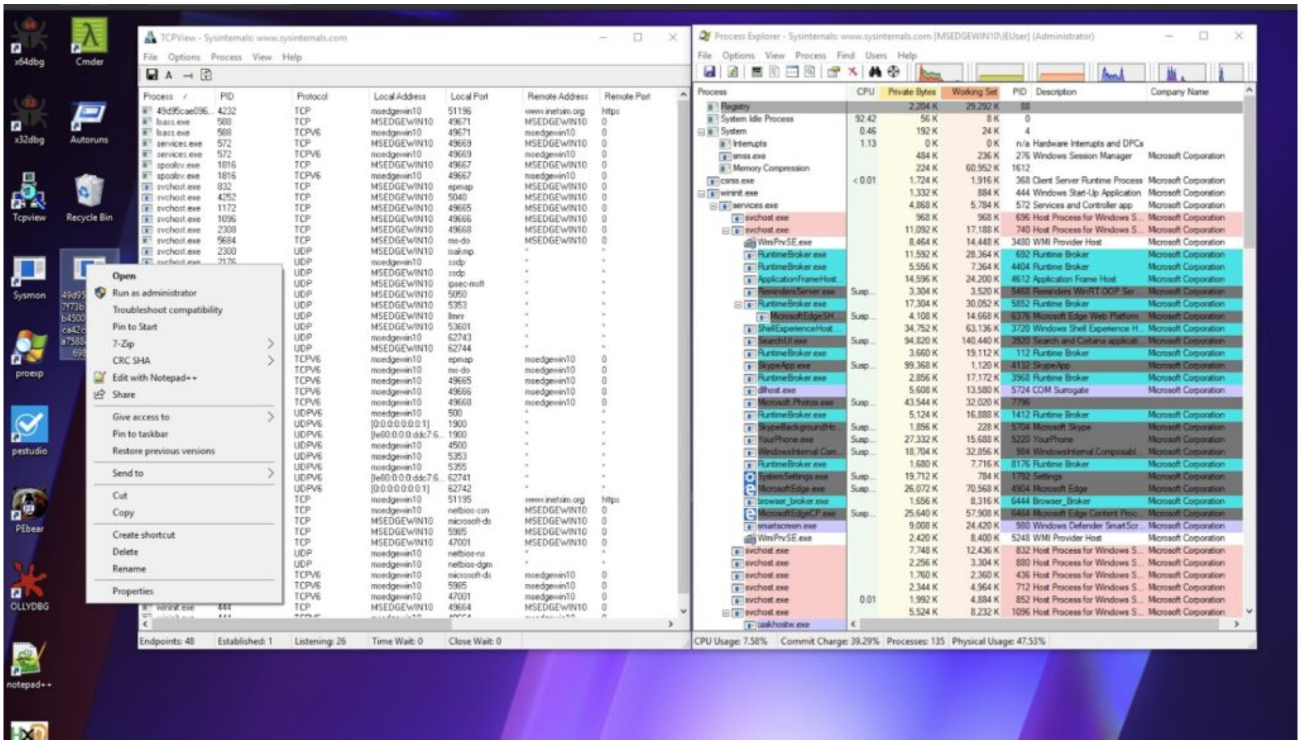
Ready to load or capture | No Packets | Profile: Default

Detonating Malware

When malware is executed, it usually makes some request to a domain or IP address. INetSim helps with this by spoofing the responses to the malware that is waiting for a response. An example would be if malware was executed and reached out to a domain and will not proceed without a response unless the conditions were met, which is the response. If the malware doesn't receive the response, it would terminate and not continue its malicious actions. This is where the live environment assists us with responding to callouts and capturing network traffic.

For the final step of the lab environment setup, we will detonate a notorious binary trojan (or any malware you choose) to test the configuration is working correctly.

I'm testing with a Trickbot binary (**SHA256:** `49d95cae096f7f73b3539568b450076227b4ca42c0240044a7588ddc1f1b6985`). I've opened Process Explorer and TCPView to monitor the execution of this variant of Trickbot.

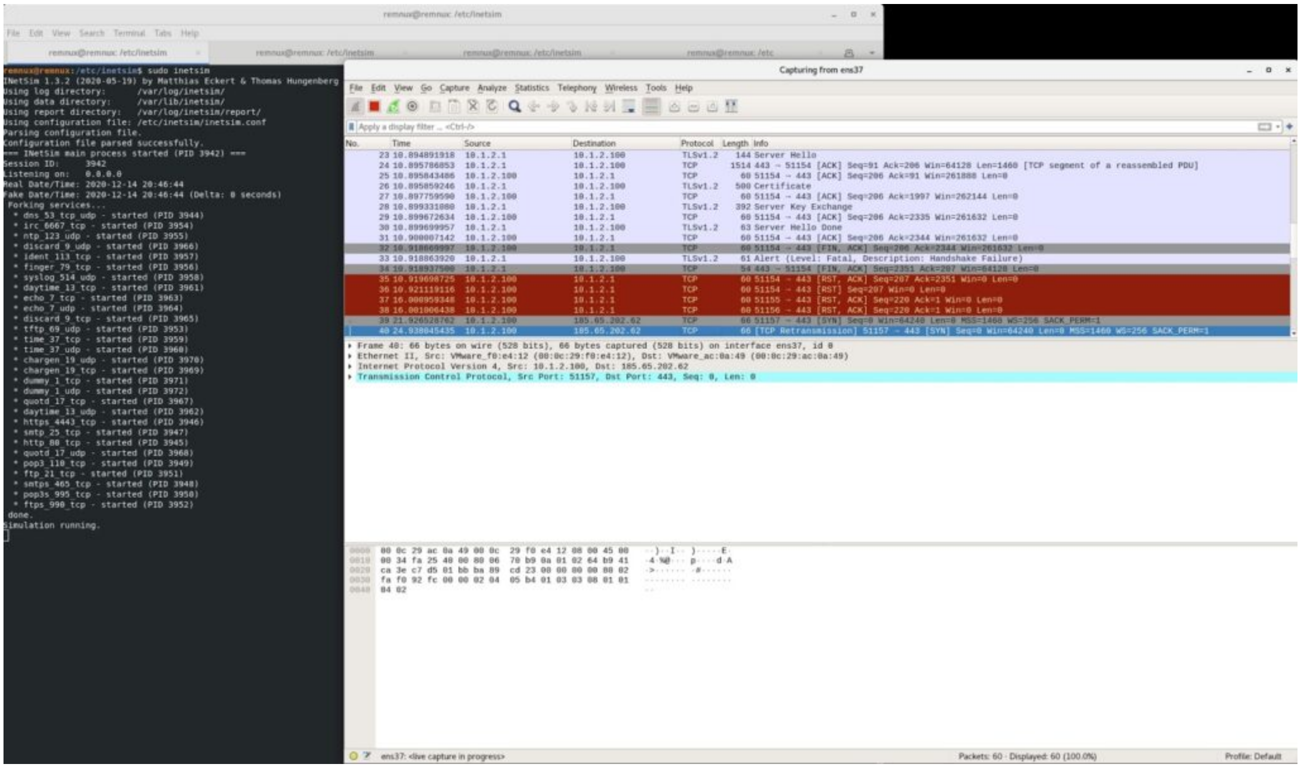

x64dbg
Cmder
x32dbg
Autoruns
Tcpview
Recycle Bin
Sysmon
proexp
pestudio
PEbear
OLLYDBG
notepad++
TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Open
Run as administrator
Troubleshoot compatibility
Pin to Start
7-Zip
CRC SHA
Edit with Notepad++
Share
Give access to
Pin to taskbar
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser] (Administrator)
File Options View Process Find Users Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
49d95cae096...	4232	TCP	msedgewin10	51196	www.inetsim.org	https
lsass.exe	588	TCP	MSEDGEWIN10	49671	MSEDGEWIN10	0
lsass.exe	588	TCPV6	msedgewin10	49671	msedgewin10	0
services.exe	572	TCP	MSEDGEWIN10	49669	MSEDGEWIN10	0
services.exe	572	TCPV6	msedgewin10	49669	msedgewin10	0
spoolsv.exe	1816	TCP	MSEDGEWIN10	49667	MSEDGEWIN10	0
spoolsv.exe	1816	TCPV6	msedgewin10	49667	msedgewin10	0
svchost.exe	832	TCP	MSEDGEWIN10	epmap	MSEDGEWIN10	0
svchost.exe	4252	TCP	MSEDGEWIN10	5040	MSEDGEWIN10	0
svchost.exe	1172	TCP	MSEDGEWIN10	49665	MSEDGEWIN10	0
svchost.exe	1096	TCP	MSEDGEWIN10	49666	MSEDGEWIN10	0
svchost.exe	2308	TCP	MSEDGEWIN10	49668	MSEDGEWIN10	0
svchost.exe	5684	TCP	MSEDGEWIN10	ms-do	MSEDGEWIN10	0
svchost.exe	2300	UDP	MSEDGEWIN10	isakmp	*	*
svchost.exe	2176	UDP	msedgewin10	ssdp	*	*
		UDP	MSEDGEWIN10	ssdp	*	*
		UDP	MSEDGEWIN10	ipsec-msft	*	*
		UDP	MSEDGEWIN10	5050	*	*
		UDP	MSEDGEWIN10	5353	*	*
		UDP	MSEDGEWIN10	llmnr	*	*
		UDP	MSEDGEWIN10	53601	*	*
		UDP	msedgewin10	62743	*	*
		UDP	MSEDGEWIN10	62744	*	*
		TCPV6	msedgewin10	epmap	msedgewin10	0
		TCPV6	msedgewin10	ms-do	msedgewin10	0
		TCPV6	msedgewin10	49665	msedgewin10	0
		TCPV6	msedgewin10	49666	msedgewin10	0
		TCPV6	msedgewin10	49668	msedgewin10	0
		UDPV6	msedgewin10	500	*	*
		UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*
		UDPV6	[fe80:0:0:0:ddc7:6...	1900	*	*
		UDPV6	msedgewin10	4500	*	*
		UDPV6	msedgewin10	5353	*	*
		UDPV6	msedgewin10	5355	*	*
		UDPV6	[fe80:0:0:0:ddc7:6...	62741	*	*
		UDPV6	[0:0:0:0:0:0:0:1]	62742	*	*
		TCP	msedgewin10	51195	www.inetsim.org	https
		TCP	msedgewin10	netbios-ssn	MSEDGEWIN10	0
		TCP	MSEDGEWIN10	microsoft-ds	MSEDGEWIN10	0
		TCP	MSEDGEWIN10	5985	MSEDGEWIN10	0
		TCP	MSEDGEWIN10	47001	MSEDGEWIN10	0
		UDP	msedgewin10	netbios-ns	*	*
		UDP	msedgewin10	netbios-dgm	*	*
		TCPV6	msedgewin10	microsoft-ds	msedgewin10	0
		TCPV6	msedgewin10	5985	msedgewin10	0
		TCPV6	msedgewin10	47001	msedgewin10	0
wininit.exe	444	TCP	MSEDGEWIN10	49664	MSEDGEWIN10	0

Endpoints: 48 | Established: 1 | Listening: 26 | Time Wait: 0 | Close Wait: 0

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		2,204 K	29,292 K	88		
System Idle Process	92.42	56 K	8 K	0		
System	0.46	192 K	24 K	4		
Interrupts	1.13	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		484 K	236 K	276	Windows Session Manager	Microsoft Corporation
Memory Compression		224 K	60,952 K	1612		
csrss.exe	< 0.01	1,724 K	1,916 K	368	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,332 K	884 K	444	Windows Start-Up Application	Microsoft Corporation
services.exe		4,868 K	5,784 K	572	Services and Controller app	Microsoft Corporation
svchost.exe		968 K	968 K	696	Host Process for Windows S...	Microsoft Corporation
svchost.exe		11,092 K	17,188 K	740	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		8,464 K	14,448 K	3480	WMI Provider Host	Microsoft Corporation
RuntimeBroker.exe		11,592 K	28,364 K	692	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		5,556 K	7,364 K	4404	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...		14,596 K	24,200 K	4612	Application Frame Host	Microsoft Corporation
RemindersServer.exe	Susp...	3,304 K	3,520 K	5468	Reminders WinRT OOP Ser	Microsoft Corporation
RuntimeBroker.exe		17,304 K	30,052 K	5852	Runtime Broker	Microsoft Corporation
MicrosoftEdgeSH...	Susp...	4,108 K	14,668 K	6376	Microsoft Edge Web Platform	Microsoft Corporation
ShellExperienceHost...		34,752 K	63,136 K	3720	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	94,820 K	140,440 K	3920	Search and Cortana applicat...	Microsoft Corporation
RuntimeBroker.exe		3,660 K	19,112 K	112	Runtime Broker	Microsoft Corporation
SkypeApp.exe	Susp...	99,368 K	1,120 K	4132	SkypeApp	Microsoft Corporation
RuntimeBroker.exe		2,856 K	17,172 K	3968	Runtime Broker	Microsoft Corporation
dllhost.exe		5,608 K	13,580 K	5724	COM Surrogate	Microsoft Corporation
Microsoft.Photos.exe	Susp...	43,544 K	32,020 K	7796		
RuntimeBroker.exe		5,124 K	16,888 K	1412	Runtime Broker	Microsoft Corporation
SkypeBackgroundHo...	Susp...	1,856 K	228 K	5704	Microsoft Skype	Microsoft Corporation
YourPhone.exe	Susp...	27,332 K	15,688 K	5220	YourPhone	Microsoft Corporation
WindowsInternal.Com...	Susp...	18,704 K	32,856 K	584	WindowsInternal.Composabl...	Microsoft Corporation
RuntimeBroker.exe		1,680 K	7,716 K	8176	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	19,712 K	784 K	1792	Settings	Microsoft Corporation
MicrosoftEdge.exe	Susp...	26,072 K	70,568 K	4904	Microsoft Edge	Microsoft Corporation
browser_broker.exe		1,656 K	8,316 K	6444	Browser_Broker	Microsoft Corporation
MicrosoftEdgeCP.exe	Susp...	25,640 K	57,908 K	6464	Microsoft Edge Content Proc...	Microsoft Corporation
smartscreen.exe		9,008 K	24,420 K	980	Windows Defender SmartScr...	Microsoft Corporation
WmiPrvSE.exe		2,420 K	8,400 K	5248	WMI Provider Host	Microsoft Corporation
svchost.exe		7,748 K	12,436 K	832	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,256 K	3,304 K	880	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,760 K	2,360 K	436	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,344 K	4,964 K	712	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	1,992 K	4,884 K	852	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,524 K	8,232 K	1096	Host Process for Windows S...	Microsoft Corporation
taskhostw.exe						

CPU Usage: 7.58% | Commit Charge: 39.29% | Processes: 135 | Physical Usage: 47.53%


remnux@remnux: /etc/inetsim
File Edit View Search Terminal Tabs Help
remnux@remnux: /etc/inetsim
remnux@remnux: /etc/inetsim
remnux@remnux: /etc/inetsim
remnux@remnux: /etc
Capturing from ens37
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
ens37: <live capture in progress>
Packets: 60 · Displayed: 60 (100.0%)
Profile: Default

```
remnux@remnux:/etc/inetsim$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 3942) ===
Session ID:     3942
Listening on:   0.0.0.0
Real Date/Time: 2020-12-14 20:46:44
Fake Date/Time: 2020-12-14 20:46:44 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 3944)
  * irc_6667_tcp - started (PID 3954)
  * ntp_123_udp - started (PID 3955)
  * discard_9_udp - started (PID 3966)
  * ident_113_tcp - started (PID 3957)
  * finger_79_tcp - started (PID 3956)
  * syslog_514_udp - started (PID 3958)
  * daytime_13_tcp - started (PID 3961)
  * echo_7_tcp - started (PID 3963)
  * echo_7_udp - started (PID 3964)
  * discard_9_tcp - started (PID 3965)
  * tftp_69_udp - started (PID 3953)
  * time_37_tcp - started (PID 3959)
  * time_37_udp - started (PID 3960)
  * chargen_19_udp - started (PID 3970)
  * chargen_19_tcp - started (PID 3969)
  * dummy_1_tcp - started (PID 3971)
  * dummy_1_udp - started (PID 3972)
  * quotd_17_tcp - started (PID 3967)
  * daytime_13_udp - started (PID 3962)
  * https_4443_tcp - started (PID 3946)
  * smtp_25_tcp - started (PID 3947)
  * http_80_tcp - started (PID 3945)
  * quotd_17_udp - started (PID 3968)
  * pop3_110_tcp - started (PID 3949)
  * ftp_21_tcp - started (PID 3951)
  * smtps_465_tcp - started (PID 3948)
  * pop3s_995_tcp - started (PID 3950)
  * ftps_990_tcp - started (PID 3952)
 done.
Simulation running.
```

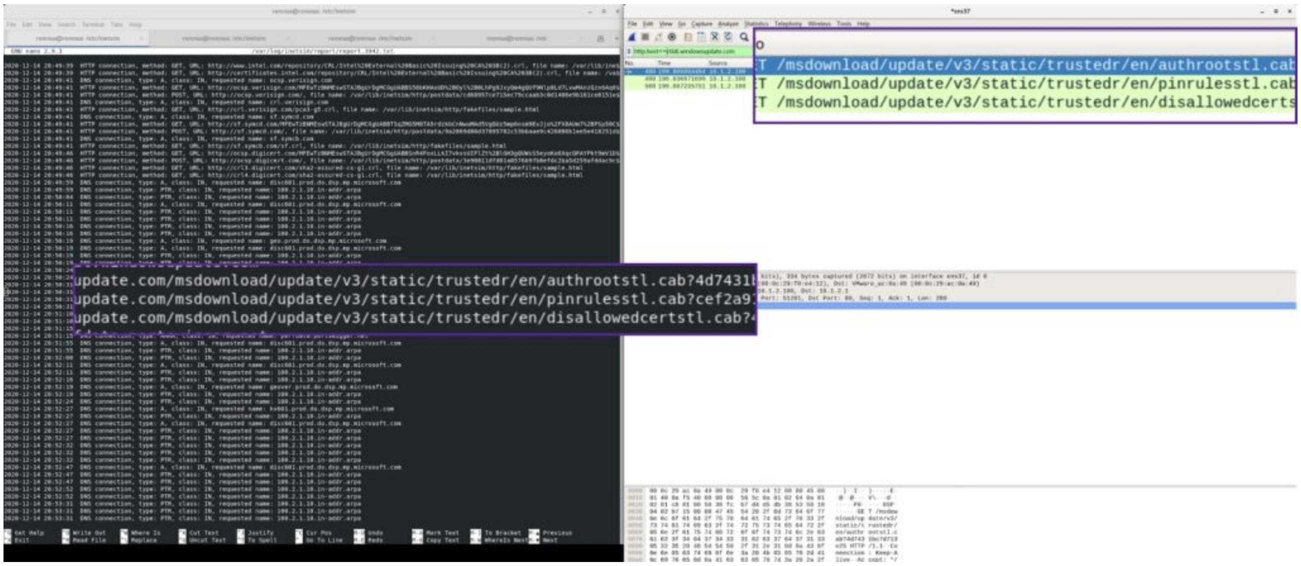
```
No.  Time           Source       Destination   Protocol Length Info
  23 10.894891918   10.1.2.1     10.1.2.100    TLSv1.2   144 Server Hello
  24 10.895786853   10.1.2.1     10.1.2.100    TCP      1514 443 → 51154 [ACK] Seq=91 Ack=206 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
  25 10.895843486   10.1.2.100   10.1.2.1      TCP        60 51154 → 443 [ACK] Seq=206 Ack=91 Win=261888 Len=0
  26 10.895859246   10.1.2.1     10.1.2.100    TLSv1.2   500 Certificate
  27 10.897759590   10.1.2.100   10.1.2.1      TCP        60 51154 → 443 [ACK] Seq=206 Ack=1997 Win=262144 Len=0
  28 10.899331080   10.1.2.1     10.1.2.100    TLSv1.2   392 Server Key Exchange
  29 10.899672634   10.1.2.100   10.1.2.1      TCP        60 51154 → 443 [ACK] Seq=206 Ack=2335 Win=261632 Len=0
  30 10.899699957   10.1.2.1     10.1.2.100    TLSv1.2    63 Server Hello Done
  31 10.900007142   10.1.2.100   10.1.2.1      TCP        60 51154 → 443 [ACK] Seq=206 Ack=2344 Win=261632 Len=0
  32 10.918869997   10.1.2.100   10.1.2.1      TCP        60 51154 → 443 [FIN, ACK] Seq=206 Ack=2344 Win=261632 Len=0
  33 10.918863920   10.1.2.1     10.1.2.100    TLSv1.2    61 Alert (Level: Fatal, Description: Handshake Failure)
  34 10.918937500   10.1.2.1     10.1.2.100    TCP        54 443 → 51154 [FIN, ACK] Seq=2351 Ack=207 Win=64128 Len=0
  35 10.919698725   10.1.2.100   10.1.2.1      TCP        60 51154 → 443 [RST, ACK] Seq=207 Ack=2351 Win=0 Len=0
  36 10.921119116   10.1.2.100   10.1.2.1      TCP        60 51154 → 443 [RST] Seq=207 Win=0 Len=0
  37 16.000959348   10.1.2.100   10.1.2.1      TCP        60 51155 → 443 [RST, ACK] Seq=220 Ack=1 Win=0 Len=0
  38 16.001006438   10.1.2.100   10.1.2.1      TCP        60 51156 → 443 [RST, ACK] Seq=220 Ack=1 Win=0 Len=0
  39 21.926528762   10.1.2.100   185.65.202.62 TCP        66 51157 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  40 24.938045435   10.1.2.100   185.65.202.62 TCP        66 [TCP Retransmission] 51157 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
▸ Frame 40: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface ens37, id 0
▸ Ethernet II, Src: VMware_f0:e4:12 (00:0c:29:f0:e4:12), Dst: VMware_ac:0a:49 (00:0c:29:ac:0a:49)
▸ Internet Protocol Version 4, Src: 10.1.2.100, Dst: 185.65.202.62
▸ Transmission Control Protocol, Src Port: 51157, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  00 0c 29 ac 0a 49 00 0c  29 f0 e4 12 08 00 45 00   ··)··I·· )·····E·
0010  00 34 fa 25 40 00 80 06  70 b9 0a 01 02 64 b9 41   ·4·%@··· p····d·A
0020  ca 3e c7 d5 01 bb ba 89  cd 23 00 00 00 00 80 02   ·>······ ·#······
0030  fa f0 92 fc 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Detonating malware can save a lot of time before diving deep into reverse engineering as it allows you to gather insight and create an unbiased hypothesis. In this example, when we detonated this trickbot sample there were three callouts that stuck out:

> The callouts were to fetch files from Microsoft Updates site; these cab files called were automatic updaters of untrusted certificates. A certificate trust list is a predefined list of items signed by a trusted entity. These requested cab files are used to update and expand the existing functionality by adding known untrusted certificates to the untrusted certificate store by using a certificate trust list.


File Edit View Search Terminal Tabs Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source

```
GNU nano 2.9.3                    /var/log/inetsim/report/report.3942.txt

2020-12-14 20:49:39  HTTP connection, method: GET, URL: http://www.intel.com/repository/CRL/Intel%20External%20Basic%20Issuing%20CA%203B(2).crl, file name: /var/lib/ine
2020-12-14 20:49:39  HTTP connection, method: GET, URL: http://certificates.intel.com/repository/CRL/Intel%20External%20Basic%20Issuing%20CA%203B(2).crl, file name: /va
2020-12-14 20:49:41  DNS connection, type: A, class: IN, requested name: ocsp.verisign.com
2020-12-14 20:49:41  HTTP connection, method: GET, URL: http://ocsp.verisign.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS
2020-12-14 20:49:41  HTTP connection, method: POST, URL: http://ocsp.verisign.com/, file name: /var/lib/inetsim/http/postdata/
2020-12-14 20:49:41  DNS connection, type: A, class: IN, requested name: crl.verisign.com
2020-12-14 20:49:41  HTTP connection, method: GET, URL: http://crl.verisign.com/pca3-g5.crl, file name: /var/lib/inetsim/http/fakefiles/sample.html
2020-12-14 20:49:41  DNS connection, type: A, class: IN, requested name: sf.symcd.com
2020-12-14 20:49:41  HTTP connection, method: GET, URL: http://sf.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBT
2020-12-14 20:49:41  HTTP connection, method: POST, URL: http://sf.symcd.com/, file name: /var/lib/inetsim/http/postdata/
2020-12-14 20:49:41  DNS connection, type: A, class: IN, requested name: sf.symcb.com
2020-12-14 20:49:41  HTTP connection, method: GET, URL: http://sf.symcb.com/sf.crl, file name: /var/lib/inetsim/http/fakefiles/sample.html
2020-12-14 20:49:46  HTTP connection, method: GET, URL: http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS
2020-12-14 20:49:46  HTTP connection, method: POST, URL: http://ocsp.digicert.com/, file name: /var/lib/inetsim/http/postdata/
2020-12-14 20:49:46  HTTP connection, method: GET, URL: http://crl3.digicert.com/sha2-assured-cs-g1.crl, file name: /var/lib/inetsim/http/fakefiles/sample.html
2020-12-14 20:49:46  HTTP connection, method: GET, URL: http://crl4.digicert.com/sha2-assured-cs-g1.crl, file name: /var/lib/inetsim/http/fakefiles/sample.html
2020-12-14 20:49:59  DNS connection, type: A, class: IN, requested name: disc601.prod.do.dsp.mp.microsoft.com
2020-12-14 20:49:59  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:50:04  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:50:11  DNS connection, type: A, class: IN, requested name: disc601.prod.do.dsp.mp.microsoft.com
2020-12-14 20:50:11  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:50:11  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:50:16  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:50:16  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:50:19  DNS connection, type: A, class: IN, requested name: geo.prod.do.dsp.mp.microsoft.com
2020-12-14 20:50:19  DNS connection, type: A, class: IN, requested name: disc601.prod.do.dsp.mp.microsoft.com
2020-12-14 20:50:19  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:50:19
2020-12-14 20:50:24
2020-12-14 20:50:24 update.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?4d7431
2020-12-14 20:50:31
2020-12-14 20:50:31 update.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?cef2a9
2020-12-14 20:50:31
2020-12-14 20:51:10 update.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?4
2020-12-14 20:51:10
2020-12-14 20:51:15
2020-12-14 20:51:15
2020-12-14 20:51:55  DNS connection, type: A, class: IN, requested name: disc601.prod.do.dsp.mp.microsoft.com
2020-12-14 20:51:55  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:00  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:11  DNS connection, type: A, class: IN, requested name: disc601.prod.do.dsp.mp.microsoft.com
2020-12-14 20:52:11  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:16  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:19  DNS connection, type: A, class: IN, requested name: geover.prod.do.dsp.mp.microsoft.com
2020-12-14 20:52:19  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:24  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:27  DNS connection, type: A, class: IN, requested name: kv601.prod.do.dsp.mp.microsoft.com
2020-12-14 20:52:27  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:27  DNS connection, type: A, class: IN, requested name: disc601.prod.do.dsp.mp.microsoft.com
2020-12-14 20:52:27  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:27  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:32  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:32  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:32  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:47  DNS connection, type: A, class: IN, requested name: disc601.prod.do.dsp.mp.microsoft.com
2020-12-14 20:52:47  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:47  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:52  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:52:52  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:53:31  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:53:31  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa
2020-12-14 20:53:31  DNS connection, type: PTR, class: IN, requested name: 100.2.1.10.in-addr.arpa

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo    M-A Mark Text  M-] To Bracket  M-▲ Previous
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo    M-6 Copy Text  ^Q WhereIs Next M-▼ Next
```

```
*ens37

http.host==ctldl.windowsupdate.com

No.  Time           Source
498  199.808080464  10.1.2.100
499  199.836571699  10.1.2.100
500  199.867225751  10.1.2.100

o
T /msdownload/update/v3/static/trustedr/en/authrootstl.cab
T /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab
T /msdownload/update/v3/static/trustedr/en/disallowedcerts

bits), 334 bytes captured (2672 bits) on interface ens37, id 0
(00:0c:29:f0:e4:12), Dst: VMware_ac:0a:49 (00:0c:29:ac:0a:49)
10.1.2.100, Dst: 10.1.2.1
Port: 51201, Dst Port: 80, Seq: 1, Ack: 1, Len: 280

0000  00 0c 29 ac 0a 49 00 0c  29 f0 e4 12 08 00 45 00   ..)..I.. )....E.
0010  01 40 0a f5 40 00 80 06  56 5c 0a 01 02 64 0a 01   .@..@... V\...d..
0020  02 01 c8 01 00 50 38 fc  67 d4 e5 db 38 53 50 18   .....P8. g...8SP.
0030  04 02 b7 15 00 00 47 45  54 20 2f 6d 73 64 6f 77   ......GE T /msdow
0040  6e 6c 6f 61 64 2f 75 70  64 61 74 65 2f 76 33 2f   nload/up date/v3/
0050  73 74 61 74 69 63 2f 74  72 75 73 74 65 64 72 2f   static/t rustedr/
0060  65 6e 2f 61 75 74 68 72  6f 6f 74 73 74 6c 2e 63   en/authr ootstl.c
0070  61 62 3f 34 64 37 34 33  31 62 63 37 64 37 31 33   ab?4d743 1bc7d713
0080  65 32 35 20 48 54 54 50  2f 31 2e 31 0d 0a 43 6f   e25 HTTP /1.1..Co
0090  6e 6e 65 63 74 69 6f 6e  3a 20 4b 65 65 70 2d 41   nnection : Keep-A
00a0  6c 69 76 65 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   live..Ac cept: */
```

Although Trickbot is one of the more prolific malware strains today and is more complex than a few callouts, it is a good starting point if you are in the beginning stages of research and have never encountered this binary.

I've been successfully using this lab setup for many years. A real-world example of using this lab setup occurred when I was brought in to help with an incident at short notice back in 2016. I didn't have time for an initial triage of the binary as I was joining a war room call for the briefing by the investigation team lead. I started both VMs from snapshots and detonated the binary while being brought up to speed about the incident. Within 5 minutes, I informed the investigation lead about an IP that the specific binary was calling out to, which was enough to give the threat hunters a place to begin. After the war room call, I started reversing the malware and extracting additional IOCs and TTPs.

Conclusion

A lab environment setup and configuration varies during malware analysis. When analyzing malware you need different tools to dissect and do deep analysis. I hope the SentinelLabs RevCore Tools and configurations in this setup assists, but there might be a time that you need to analyze something different, like a dot net file, and may need an additional tool to fully disassemble the binary. The journey of reversing malware is a marathon and not a sprint; growing your skill and learning from every malware analyzed should be the goal.

Resources

https://support.microsoft.com/en-us/help/2677070/an-automatic-updater-of-untrusted-certificates-is-available-for-window

https://askubuntu.com/questions/191226/dnsmasq-failed-to-create-listening-socket-for-port-53-address-already-in-use

https://gallery.technet.microsoft.com/scriptcenter/Change-the-Desktop-b5b2141c

https://gist.github.com/trietptm/b84ccad9db01f459ac7e