STEP BY STEP MALWARE ANALYSIS LAB SET-UP



Contents

HYPERVISOR INSTALLATION	2
WINDOWS 10 OS INSTALLATION	4
REMnux INSTALLATION	. 13
FLARE VM INSTALLATION	. 15
SPECIAL NETWORK CONFIGURATION	. 20
NETWORK CONFIGURATION FOR VM	. 22
Windows 10 – Flare VM	. 22
REMnux VM	. 23
SET UP INETSIM	. 25
References:	. 30

HYPERVISOR INSTALLATION

1. Go to <u>https://www.virtualbox.org/wiki/Downloads</u> and choose the installer according to your host architecture.



2. Once downloaded. Proceed with the installation with all default settings.



3. VirtualBox should launch automatically.

🦸 Oracle VM VirtualBox Manager		– 🗆 X
<u>File M</u> achine <u>H</u> elp		
Tools 🖉 \Xi	Preferences Import Export New Add	
	Welcome to VirtualBox!	
	The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.	
	popup a tools of currently selected element using corresponding element button. You can press the F1 key to get instant help, or visit <u>www.virtualbox.org</u> for more information and latest news.	

WINDOWS 10 OS INSTALLATION

1. To install the first OS, go to https://www.microsoft.com/en-us/evalcenter/evaluatewindows-10-enterprise to get the ISO.

Microsoft Evaluation Center Windows Vindows Server SQL Server More V All Microsoft 🗸

Windows 10 Enterprise

In page quick links $\, \smallsetminus \,$

Overview

This evaluation software is designed for IT professionals interested in trying Windows 10 Enterprise on behalf of their organization. We do not recommend that you install this evaluation if you are not an IT professional or are not professionally managing corporate networks or devices.

Get started for free

Please select your product experience: Download the ISO – Enterprise > wnload the ISO – LTSC Enterprise >

Description

Windows 10 Enterprise is designed to address the n ds of large and midsize organizations by providing IT profession

- Advanced protection against modern security threats
- Flexible deployment, update, and support options Comprehensive device and app management and control

Windows 10, version 22H2 makes it easier to protect your endpoints, detect advanced attacks, automate response to emerging threats, and improve your security posture. It also helps you streamline deployment and updates-and deliver enterprise-ready devices to your users straight from the manufacture

Looking for information on specific features? See what's new in Windows 10.

Languages

English (United States), English (Great Britain), Chinese (Simplified), Chinese (Traditional), French, German, Italian, Japanese, Korean, Spanish, Portuguese (Brazil)

Editions

Windows 10 Enterprise, version 22H2 | 64-bit and 32-bit ISO
Windows 10 Enterprise LTSC 2021 | 64-bit and 32-bit ISO

2. It will request certain information from you. Register details for your free ISO.

3. Once downloaded, go to VirtualBox – click New button to configure the VM details. Then click Next



4. Configure your Memory and Processor amount.

Ũ	Create Virtual Machine	2	?	×
		Hardware		
		You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.		
		Base Memory:	4096 MB	٢
		4 MB 16384 MB		
		Processors:		1 🖨
		Enable EFT (special OSes only)	8 CPUS	
_				
	Help	<u>B</u> ack <u>N</u> ext	<u>C</u> ance	1

5. For Virtual Hard Disk – you can set it to default. Then click Next.

🧿 Create Virtual Machin	e	?	×
anti William	Virtual Hard disk		
	If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.		
	<u>C</u> reate a Virtual Hard Disk Now		
	Dijsk Size:	50.	00 GB
	4.00 MB 2.00 TB		
	Pre-allocate <u>F</u> ull Size		
K	Use an Existing Virtual Hard Disk File		
	Empty		
	Do Not Add a Virtual Hard Disk		
Help	Back Next	<u>C</u> anc	el

6. Check the details to confirm the configuration before click Finish.

	Summary		
	The following table summarize When you are happy with the you can go back and modify t	es the configuration you have chosen for the ner configuration press Finish to create the virtual he configuration.	w virtual machine. machine. Alternatively
	* Machine Name and O	5 Type	
	Machine Name	Windows 10 OS - Flare VM	
	Machine Folder	E:/Malware Analysis Lab/Windows 10 O	S/Windows 10 OS - Flare VM
	ISO Image	D:/Windows OS/19045.2006.220908-0	225.22h2 release svc refresh
	Guest OS Type	Windows 10 (64-bit)	
	Skip Unattended Install	true	
	Hardware		
	Base Memory	4096	
Y-	Processor(s)	1	
	EFI Enable	false	
	🖸 Disk		
	Disk Size	50.00 GB	
	Pre-allocate Full Size	false	
Help		Back	Einish Cancel

7. After click Finish, initialize it by clicking Start and the machine will start installation process.

Windows 10 OS - Flare VM [Running] - Oracle VM VirtualBox	_		×
File Machine View Input Devices Help			
Windows Setup			
Language to install: English (United States)			
Keyboard or input method: US			
Enter your language and other preferences and click "Next" to continue.			
		🕽 🛃 Right	Ctrl 🐇

STEP BY STEP MALWARE ANALYSIS LAB SET-UP	
Video Memory: 128 MB	Bit is 1986 Tananan karan
📸 Windows 10 OS - Flare VM (Running) - Oracle VM VirtualBox File Machine View Input Devices Help	-
🖆 Windows Setup	
Windows	
Install now	
Repair your computer © Microsoft Corporation. All rights reserved.	
	🛡 💾 🗑 🚱 🔽 Right Ctrl

8. Choose Custom installation.

🞇 Windows 10 OS - Flare VM [Running] - Oracle VM VirtualBox		_		×
File Machine View Input Devices Help				A
🚱 💰 Windows Setup	—X—)			
Which type of installation do you want?				
Upgrade: Install Windows and keep files, settings, and applications The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.				
Custom: Install Windows only (advanced) The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.				
4 State Stat	-7 🕜 🗐 🖻] 🚝 🕅 🚳	Right	Ctrl .:

9. Click New then Apply before you click Next.

🔀 Windows	10 OS -	Flare VI	VI [Running] - Oracle	/M VirtualBox						_		\times
File Machine	View	Input	Devices Help									
		6	💰 Windows Setup						x			Ī
			Where do you	want to install Wi	ndows?							
			Name			Total size	Free space	Туре				- 1
			🛷 Drive 0 Un	allocated Space		50.0 GB	50.0 GB					- 1
			€ Refresh	Delete	⊘ E¢	ermat	<mark>∦</mark> N <u>e</u> w		-			
			Load driver	Extend	Size:	51200	€ MB	Apply Car	ncel			
				_								
								Ne	xt			
		_										
												- 1
												•
								🖸 💽 💽	P 🄌 🛑 🖸	9 💾 🛛 🔇	🛃 Right	Ctrl 📰

10. Let the installation process complete and this will takes sometimes depending on your resources.



11. The machine will go into booting screen before next step.

👪 Windows 10 OS - Flare VM [Running] - Oracle VM VirtualBox	_		\times
File Machine View Input Devices Help			~
			-
K 💿 🕅 d	7 🌶 🗐 💷 🖑 🔞	🛛 🛃 Right C	trl

Select Region, Keyboard based on your preferences.



12. You don't have to sign in with Microsoft, select Choose Domain join instead before click Next



13. Complete the necessary set-up process until you see the Windows desktop.



14. Then, go to Devices – Insert Guest Edition Cd image to set up better viewing display of your VM.

	Base Memory: 4096 M6 Boot Order: Floppy Ochical, Hard Disk Acceleration: Nested Paging, Hope-V Paravirtualization		
🐹 Windows 10 OS - Flare	VM [Running] - Oracle VM VirtualBox	-	×
File Machine View Inpu Recycle Bin Microsoft	t Devices Help Devices Help Make Optical Drives Make Dopposition Name Optical Drives Shared Clipboard Data Drop Make Drag and Drop Make Drag and Drop		
Edge	V Uggrade Guest Additions		

Go to This PC, and double click CD Drive then choose suitable configuration for the installation.



STEP BY STEP MALWARE ANALYSIS LAB SET-UP

It will reboot once you click Finish.



15. Don't forget to take snapshot at this phase before you proceed with next step. Just go to the TaskBar and select Machine.

Windows 10 05 - Flar	🖵 General	📃 Preview
Running	Name: Windows 10 OS - Flare VM Operating System: Windows 10 (64-bit)	
A	System	
	Base Memory 4006 MR	
🔀 Windows 10 OS - Flare VM [Running] - Or	acle VM VirtualBox	
File Machine View Input Devices Help		
🧲 🤴 Settings	Host+S	
🛐 👰 Take Snapshot	Host+T	
😥 🤢 Session Information	Host+N	
File Manager		
🐻 Show Log		
II Pause	Host+P	
D Reset	Host+R	
Micr 🗲 ACPI Shutdown	Host+H	
Edge		

Name the snapshot accordingly. This will allow you to return to this base phase if there is error prompted during next configuration.

Tak	e Snapshot of Virtual Machine			?	×
64	Snapshot <u>N</u> ame				
-40	Base Windows 10				
	Snapshot Description				
		Ok	Cancel	Help	
		OK	Caricer	ncip	

16. Then suspend your virtual machine to proceed with REMnux installation

REMnux INSTALLATION

17. Go to https://docs.remnux.org/install-distro/get-virtual-appliance, then select VirtualBox OVA. You will be able to download it from the Box.

M2.	
Step 1: D	Download the Virtual Appliance File
'he REMnux vir mport into your	tual appliance approximately 5 GB. It comes as an industry-standard OVA file, which you can r virtualization software. It's based on Ubuntu 20.04 (Focal).
ecide which O' ou're using Virt	VA file to download. Unless you're using Oracle VM VirtualBox, get the general OVA file. If tualBox, get the VirtualBox version. Download your preferred OVA file:
General OVA	VirtualBox OVA
This VirtualBo using other h	ox OVA file is specifically for VirtualBox. Get the general version from the other tab if you're ypervisors:
Download the	e VirtualBox OVA file from <u>Box</u> (primary) or <u>SourceForge</u> (mirror)
Some brow	vsers (e.g., <u>Brave</u>) change the extension of the OVA file after downloading it, possibly giving it the ovf extension. If that happens, rename the file so it has the .ova extension before proceeding.

18. Download the file into the same directory created just now for easy access. Go to the installer once download completed and choose Open with VirtualBox Manager.

	64 Windows 10 05 - F ()	📃 Gen	neral				📃 Previe	N	
		Name: Operating	g System: Windows 10 OS - Flare VM g System: Windows 10 (64-bit)				8		
W		🔳 Syst	stem				S.		
		Base Mem Boot Orde Accelerati	mory: 4096 MB ler: Floppy, Optical, Hard Disk tion: Nested Paging, Hyper-V Paravirtu	alization					
2	📙 📄 📑 = 🛛 REMnux							- 0	×
	File Home Share View								× ?
	← → ∽ ↑ 📘 → SSD (E:) → Malware	Analysis L	Lab → REMnux		ڻ ~				م
Vie	4 Quick access	Name		Date moo	lified	Туре			
		💗 ren	many v7 focal virtualboy	10/0/2022	17:58 AM	Open Virtualizi			
	- Downloads		Open						
	Documents		Scan with Microsoft Defender.						
h	Pictures #		Open with	>	VirtualBox	Manager		1	
	MacOS		G Unlock with File Locksmith	í í	VMware PI	aver			
			Rename with PowerRename		📵 VMware W	orkstation			
	Pictures		Restore previous versions		Search the	Microsoft Store			
	SOC HOME LAB		Send to	>	Choose an	other app			
	👝 OneDrive - Personal		Cut						
	— T : B		Сору						
			Create shortcut						
C	👝 Data (D:)		Delete					No preview available.	
ľ	👝 SSD (E:)		Rename						
	P Network		Properties						
	SYAMSUS-AIR								

19. Set the VM accordingly before you click Finish.

10015		New	Add Settings Di	scard Show						
Windows 10 05 - F	. ()	📃 Gene	eral					📃 Pro	eview	
UI Pauseo	🧿 Import Virtu	al Applian	ce					?	×	_
			Appliance se	ttings						
			These are the virtual VirtualBox machines. disable others using t	machines cont You can chang the check boxe	ained in the appliance and e many of the properties s below.	d the suggested shown by doub	d settings of the in ple-clicking on the	mported items an	d	
		m	Virtual System 1							
		1 Miles	😽 Name		REMnux - Malware Lab					Side Constant
		mmn and	🗭 Product		REMnux					
		Mary	👂 Product-URL		https://REMnux.org					
			旹 Guest OS Ty	/pe	🏏 Ubuntu (64-bit)					
			CPU							
			RAM		2048 MB					
					√					
			Machine Base Folder:	E: Malwa	re Analysis Lab\REMnux					
			MAC Address Policy:	Include only	NAT network adapter MA	C addresses				
			Additional Options:	✓ <u>I</u> mportha	rd drives as VDI					
			Appliance is not signed	d			When check	ed, all th	e hard (drives that belong to this ap
	Halp				Expert Mode		Finish	Cance	4	
		None								
		Dese								
		none								

Allow it to complete the set-up, then Power On the REMnux VM.

20. You should see REMnux VM running after the booting process completed.



Power Off REMnux machine.

FLARE VM INSTALLATION

21. First install chrome browser into the Windows 10 OS VM.



22. Then go to https://github.com/mandiant/flare-vm

REMnux - Malware Lab	System		O main sound sound 1 in O main sound sound 1 in O main sound sound the so D main sound the sound sound the sound so	0.0 0.0 0.00000 Vistalii 0.001	
Windows 10 OS - Flare VM (Base Windows 10) [Running] - Oracle VM VirtualBox		Con Stan & D.Maam # S	— []	>
Machine View Input Devices Help					
✓ O GitHub - mandiant/flare-vm: A ⊂ ×	+			- 🗆	×
← → C 🔄 github.com/man	diant/flare-vm		C	: 🖈 💄	:
≡	Ģ			Sign in	^
🛱 mandiant / flare-vm (Publi	٥	Q Notifications	양 Fork 889 ☆ St	tar 6.3k 👻	
<> Code	Pull requests 3 ③ Actions 🗄 Project	s () Security 2	⊻ Insights About		
Ana06 Merge pull request #60	2 from Ana06/new-tools 🚥 8080	806 · last week 🕚	A collection of softwa installations scripts fo	are or Windows	
.github/ISSUE_TEMPLATE	Update and simplify the documentati	10 months ago	setup and maintain a	reverse	
Images	Update and simplify the documentati	10 months ago	engineering environn VM.	nent on a	
🗋 .gitattributes	Updated install.ps1 and updated Win	3 years ago	reverse-engineering		
🗋 .gitignore	Updated install.ps1 and updated Win	3 years ago	malware-analysis flar	/e	
CustomStartLayout.xml	[CustomStartLayout.xml] Fix VisualStu	4 months ago	💭 Readme		

Copy link address of installer.ps1



STEP BY STEP MALWARE ANALYSIS LAB SET-UP

23. Open Windows PowerShell by run it as Administrator.



24. Then run this command Set-ExecutionPolicy Unrestricted

Power	ed Off Base Memory: 4006 MR
👪 Windows 10 OS	- Flare VM (Base Windows 10) [Running] - Oracle VM VirtualBox —
File Machine Viev	v Input Devices Help
6	🖉 Administrator: Windows PowerShell — 🗆
Recycle Bin	Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved.
	Try the new cross-platform PowerShell https://aka.ms/pscore6
	PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted
Microsoft	
Edge	
Google	
Chrome	

REMnux - I	Malware Lab System	An Tractice and the Structure of the second s	il 101-1010 fi conte a 10-11-1010 fi conte a	
🛣 Windows 10 OS - I	Flare VM (Base Windows 10) [Running] - Oracle VM VirtualBox		- 0]
File Machine View	Input Devices Help			
	27 Administrator: Windows PowerShell	-)
Recycle Bin	Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved.			
	Try the new cross-platform PowerShell https://aka.ms/pscore6			
	PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted			
Microsoft Edge Google Grirome	Execution Policy Change The execution policy helps protect you from scripts that you do not trust. Changing the execution policy you to the security risks described in the about_Execution_Policies help topic at https:/go.microsoft.com/fwlink/linkID=135170. Do you want to change the execution policy? [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y PS C:\Windows\system32>	/ might	: expose	

25. Run wget https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1

-UseBasicParsing -outfile <your desktop directory>

W REMnux - Malware	Lab System Base Memory 4096 MB (Base Windows 10) (Running) - Oracle VM VirtualRox			×
File Machine View Input D	Devices Help			
Recycle Bin Recycle Bin Microsoft Edge Google Chrome	Administrator: Windows PowerShell PS C:\Windows\system32> wget https://raw.githubusercontent.com/mandiant/flare-vm/main/i outfile C:\Users\Gaban\Desktop\install.ps1_	_ Install.ps1 -UseBa	C.	× •

After that you should see install file in the desktop.

Edge	
Google Chrome	
install	

26. Change directory to desktop - cd <your desktop directory> . Then run command .\install.ps1

	PS C:\Windows\system32> PS C:\Windows\system32> cd C: PS C:\Users\Gaban\Desktop> di	\Users∖Gab r	pan\Desktop					
2	Directory: C:\Users\Gaban	\Desktop						
crosoft Edge	Mode LastWrit	eTime	Length Name					
0	-a 8/18/2024 5: -a 8/18/2024 4:	52 PM 41 PM	46457 install.ps1 2348 Microsoft Edge.lnk					
oogle hrome	PS C:\Users\Gaban\Desktop> .\ [+] Checking if PowerShell ve [+] Installing with P	install.ps rsion is c	51 compatible version 5 1 19041 1682					
	<pre>[+] Checking if script is run [+] Running as admini [+] Checking if execution pol</pre>	<pre>[+] Instaining with version versi</pre>						
nstall	[+] Execution policy [+] Checking to make sure Ope [+] Installing on Win [+] Checking for spaces in th	is unrestr rating Sys dows versi e username	Ficted stem is compatible ion 19045 e					
	 [+] Username '' does not contain any spaces. [+] Checking if host has enough disk space [1] A minimum of 60 GB hand drive space is preferred. Please increase hard drive space of the VM, reboot, and retry install 							
	[+] If you have multi %RAW_TOOLS_DIR% in config.xml [+] However, packages on	or GUI provided	s, you may change the tool installation location via the envrionment variable from the Chocolatey community repository will install to their default locati					
	<pre>[+] See: https://stac nother-drive [-] Do you still wish to proc</pre>	koverflow. eed? (Y/N)	.com/questions/19752533/how-do-i-set-chocolatey-to-install-applications-onto-a): _					

27. This installation will take a long time, so allow it to complete the installation. Proceed with default installation till VM reboot and complete installation. Don't forget to take snapshot for base Flare VM. You should see new desktop feature once everything installed.



SPECIAL NETWORK CONFIGURATION

28. For special network configuration, go to VirtualBox – Tools – Network Manager.



29. Then click Create to duplicate another adapter for this setting. So, both VM will only communicate with each other to prevent your host get infected with malware once detonated.

30. Enable the DHCP Server and configure the adapter manually to 10.0.0.1 for $\ensuremath{\mathsf{IPV4}}$

Oracle VM VirtualBox Manager		= U >
ile <u>M</u> achine <u>N</u> etwork <u>H</u> elp		
	- 🛂 🧏 🖾	
	Create Remove Properties	
	, Host-only Networks NAT Networks Cloud Networks	
Windows 10 OS - Flare VM (B		
	Name VirtualBox Host-Only Ethernet Adapter	IPv4 Prefix IPv6 Prefix DHCP Server 192, 168, 56, 1/24 Enabled
🖾 👝 REMnux - Malware Lab	VirtualBox Host-Only Ethernet Adapter #2	192.168.169.1/24 Disabled
Powered Off		
	Adapter DHCP Server	
	Configure Adapter Automatically	
	Configure Adapter Manually	
	IPv4 Address: 192.168.169.1	
	IPv4 Network <u>M</u> ask: 255.255.255.0	
L		
Ad		
Auc		
•	Configure Adapter <u>A</u> utomatically	
•	Configure Adapter Manually	
	IPv4 Address: 10.0.0.1	
	1994 Network <u>M</u> ask: 255.255.255.0	
	IPv6 Address: fe80::5623:a8b:662b:114b	
	IPv6 Prefix Length: 64	
		Analy
		Apply Reset

31. Then go to DHCP Server tab to change the Server Address to 10.0.0.2. Change Lower and Upper accordingly as well. Click apply

Adapter DHCP Server			
✓ <u>E</u> nable Server			
Server Add <u>r</u> ess:	10.0.0.2		
Server <u>M</u> ask:	255.255.255.0		
Lower Address Bound:	10.0.0.3		
Upper Address Bound:	10.0.0.254		
		Apply	Reset

NETWORK CONFIGURATION FOR VM

Windows 10 – Flare VM

32. Go to Settings then Network, change Attached to Host Only Adapter. For safety purpose check another Adapter as well. Then click OK

Windows 10 OS - F ()	General Genera	Preview X
REMnux - Malware Lab	General Network Image: System Adapter 1 Adapter 2 Adapter 3 Adapter 4	/indows Flare
	Display ✓ Enable Network Adapter Image: Storage Attached to: Host-only Adapter Image: VirtualBox Host-Only Ethernet Adapter #2 Image: VirtualBox Host-Only Ethernet Adapter #2 Image: VirtualBox Host-Only Ethernet Adapter #2	•
	Network Serial Ports USB	
	Shared Folders User Interface	
	OK Cancel Hel	p
	Description	

REMnux VM

33. Go to Settings then Network, change Attached to Host Only Adapter. For safety purpose check other Adapter as well. Then click OK



34. Power ON both VM to check their connectivity



Launch Terminal for both VM

Check adapter internet setting in REMnux VM and Flare VM.

By running the command ip a for REMnux VM and ipconfig for Flare VM.



35. You also can try to run ping command for both VM to 8.8.8.8 to check the connection.

Then ping each other VM to see if they can communicate with each other

7	REMnux	- Malwa	re Lab [Running]	- Oracle VM Virtual	Вох				—		\times	
Fil	e Machine	e View	Input Devices	Help								
A	ctivities	<u>>_</u>	Terminal 🔻		Aug	g19 00:01				€ ĝ	ب ڻ	
1	Ð				remnu	ux@remnux: ~	,	Q =	-	•	×	
re	mnux@re	emnux	:~\$ ping 8	.8.8.8	_							
pi	ng: cor	nnect	: Network	is unreachab	ole							
re	mnux@re	emnux	:~\$ ping 1	0.0.0.3	<i>.</i>							
PI	NG 10.0	9.0.3	(10.0.0.3) 56(84) byt	es of dat	ta.						
64	bytes	Trom	10.0.0.3:	1cmp_seq=1	ttl=128 1	time=0.500	ms					
04 64	bytes	from	10.0.0.3:	icmp_seq=2	++1-120	LIME=0.945	ms					
04 64	bytes	from	10.0.0.3:	icmp_seq=3	++1-120	time=0.951	ms ms					
64 64	bytes hvtes	from	10.0.0.3	icmp_seq=4	++1=128 1	time=0.932	ms					
64	hvtes	from	10.0.0.3.	icmp_seq=6	++1=128 1	time=0.937	ms					
64	bytes	from	10.0.0.3:	icmp_seq=0	ttl=128 t	time=1.01 r	ns					
64	bvtes	from	10.0.0.3:	icmp_seq=8	ttl=128 t	time=0.935	ms					
64	bytes	from	10.0.0.3:	icmp_seq=9	ttl=128 t	time=0.989	ms					
64	bytes	from	10.0.0.3:	icmp_seq=10) ttl=128	time=0.969	9 ms					
64	bytes	from	10.0.0.3:	icmp_seq=11	. ttl=128	time=0.990	9 ms					
64	bytes	from	10.0.0.3:	icmp_seq=12	ttl=128	time=0.982	2 ms					
64	bytes	from	10.0.0.3:	icmp_seq=13	ttl=128	time=0.967	7 ms					
64	bytes	from	10.0.0.3:	icmp_seq=14	ttl=128	time=0.937	7 ms					
64	bytes	from	10.0.0.3:	icmp_seq=15	ttl=128	time=0.967	7 ms					
64	bytes	from	10.0.0.3:	icmp_seq=16	5 ttl=128	time=0.952	2 ms					
64	bytes	from	10.0.0.3:	icmp_seq=17	ttl=128	time=0.914	1 ms					
64	bytes	from	10.0.0.3:	icmp_seq=18	ttl=128	time=0.957	7 ms					
S6	4 bytes	s from	n 10.0.0.3	:_icmp_seq=1	.9 ttl=128	B time=1.01	l ms					
64	bytes	from	10.0.0.3:	1cmp_seq=20) ttl=128	time=1.02	ms					
64 64	bytes	from	10.0.0.3:	1cmp_seq=21	. ttl=128	time=0.750	9 ms					
04	bytes	Trom	10.0.0.3:	sed=22	111=128	time=0.34	/ ms					

STEP BY STEP MALWARE ANALYSIS LAB SET-UP

Windows – Flare VM



SET UP INETSIM

Internet Simulator

36. Open Terminal then run inetsim to check the services. All up and running except DNS server.



37. Hence terminate inetsim CTRL + C. Run sudo nano /etc/inetsim/inetsim.conf

🏏 REMnux -	Malware Lab [Running] - Oracle	VM VirtualBox				_		×
File Machine	View Input Devices Help							
Activities	⊵ Terminal 🔻	Aug	g19 00:16				● ∰	ტ 🗕
Ð		remnu	x@remnux: ~		۹ =] -	•	×
GNU nan	o 4.8	/etc/inet	sim/inetsim.com	nf		Мо	difie	ed
5 <mark>#</mark> ######	*****	#######################################	*****	####				
# # INetSim #								
+ ##########								
#########								
# Main co								
#########	"******	#####################	*****	###				
#########								
# start_s								
# # The ser	vices to start							
#								
# Syntax:								
# # Default								
#								
# Availab	le service names ar							
# ans, nt # time ud	tp, smtp, pop3, tTt p. davtime tcp. dav	p, TTp, NTp, T1M time udp. echo t						
		[Read 1	.932 lines]					
^G Get He	lp ^0 Write Out	^W Where Is	^K Cut Text	^J Justif	y ^C	Cur Po	os.	
~X Exit	<u>^R</u> Read File	Replace	<mark>^U</mark> Paste Text	T To Spe	ιι ^_	Go To	Line	e
P- remnux	Ørempuv: ~							1/2

*Uncommented start_service dns and





38. Open another Terminal to run ip a to ensure the ip address of REMnux box.

CNTRL + O then CNTRL + X to save and exit. Run inetsim again to see the changes.



Go to Flare VM, then open browser key in the REMnux ip address to check.

STEP BY STEP MALWARE ANALYSIS LAB SET-UP

39. It shows the default HTML page or HTTP server fake mode is successful.



LAST STEP

40. In Flare VM, go to START menu and open Network Connection

🔀 Window	s 10 OS - Flare VM (Base Flare VM) [Running] - Oracle VM VirtualBox			_	\Box \times
File Machine	e View Input Devices Help				
	Control Panel/Network and Internet/Network Connections	-		×	
	ϵ ϵ \rightarrow \checkmark \uparrow \blacksquare « Network and Internet \Rightarrow Network Connections \Rightarrow \checkmark \circlearrowright Search	Network Co	nnections	P	
Recycle Bin	faken Organize 🔻		•	•	
	Ethernet Unidentified network Intel(R) PRO/1000 MT Desktop Ad				
vailable_p					
config.xml	To				
S_Transcri	inste				
isual Studio Code	desk			==	prise Evaluation valid for 90 days
م #	D Type here to search	38℃	^ € ⊄	9:56)) 8/18	ase.191206-1406 5 PM /2024

Double click then open Properties

👻 < Network a	nd Internet > Network (Connections v 🖸 Search Network Connections ,					
Disable this netwo	Ethernet Status	× on » 📲 🔹 🔟					
t	General	Ethernet Properties ×					
entified network (R) PRO/1000 MT De	Connection IPv4 Connectivity: IPv6 Connectivity: Media State: Duration: Speed: Details	Networking Connect using: Intel(R) PRO/1000 MT Desktop Adapter Configure This connection uses the following items: Image: Client for Microsoft Networks Image: Client for Microsoft Networks					
	Bytes:	Install Uninstall Properties					
	Properties	Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.					

41. Choose Internet Protocol Version 4, click Properties. Configure as below picture:

Set the IP address for DNS server to the INETSIM in the REMnux Box.

Disable this netwo	Ethernet Status		× 🛛 🛪 📲 🗸 🛄 😮
hernet	General	🖗 e	Internet Protocol Version 4 (TCP/IPv4) Properties X
Undentified network Intel(R) PRO/1000 MT De	Connection Ne IPv4 Connectivity: C IPv6 Connectivity: Media State: Duration: Speed: T Details	Netv Co	General Alternate Configuration 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: Letter in the appropriate IP settings.
	Bytes:	< <	Obtain DNS server address automatcally Image: Se
em selected			OK Cancel Valid for 90 days
rch	<u></u>	<u>1</u>	Ĵ10:02 PM 8/18/2024
			🧕 💿 🎾 🗗 🌶 🛑 🖳 🚱 🔽 Right Ctrl 🔬

Click OK and EXIT.

42. With this by typing any web address in browser, it will direct you to the Fake HTML page provided INETSIM is running in the REMnux Box.

ecycle Bin	available_p			
•	sm INetSim d	efault HTML page	×	+
÷	→ C	▲ Not secure f	akedns.	com
			This	s is the default HTML page for INetSim HTTP server fake mode.
				This file is an HTML document.
4				
le				

Now you are ready to play with some malwares!!!

References:

https://www.youtube.com/watch?v=qA0YcYMRWyI&t=3224s

https://www.youtube.com/watch?v=i8dCyy8WMKY