Executive Summary

This lab focused on setting up a malware analysis environment using a virtualbox, flare-vm and windows operating system. The key activities were pre-installation process in configuring the vm which included allocating enough storage capacity disabling windows updates, windows defender and creating a snapshot. Flare-vm was installed together with other necessary configurations.

Lab objectives

The primary goal of this lab was to set up a malware analysis environment that will conduct reverse engineering.

The goal is to use Flare-VM to ensure the environmment is fit for malware analysis.

Tools and Resources used

Oracle Virtualbox: To host our windows 10 OS Windows ISO file: To host our Flare VM Flare-VM : Our malware analysisi and reverse engineering environment

Methodology

I had an already pre-installed oracle virtual machine. I downloaded windows 10 ISO file from microsoft official store. After download was complete, I started the process of adding the ISO file to my oracle virtualbox. I ensured therewas a storage capacity of more than 60GB and a ram of atleast 2GB.

Create Virtual Machine	2			×			
	> Name and <u>O</u> perating System						
	🕨 Unattended Install 🧄						
	> Hardware						
	✓ Hard Disk						
	<u>C</u> reate a Virtual Hard Disk Now						
	Hard Disk File Location and Size						
	C:\Users\ADMIN\VirtualBox VMs\Flare VM\Flare VM.vdi		· 🖌 🚦				
			62.61 G	В			
	4.00 MB	2.00 TB					
	Hard Disk File <u>Typ</u> e and Variant						
	VDI (VirtualBox Disk Image)						
	Use an Existing Virtual Hard Disk File						
	Do Not Add a Virtual Hard Disk						
<u>H</u> elp			Canc	el			

Figure 1: Allocating storage capacity for flare vm

🛛 况 Create Virtual Machine	9			-		×
	> Name ar	nd <u>O</u> perating System				
	> <u>U</u> natten	ded Install 🚸				
	✓ H <u>a</u> rdwar	e				
	Base <u>M</u> emory:		2822 ME	\$		
		4 MB		8192 MB		
	Processors:				3	
		1 CPU			8 CPUs	
r	<u>E</u> nable EFI	(special OSes only)				
	> Hard Dis	k				
<u>H</u> elp					Cano	el

Figure 2: Allocating RAM and CPUs using oracle VM

After installing the windows vm, I had to install guest addition tools that include full screen and shared folder capability where I selected my documents folder from my host OS and save a snapshot.



Figure 3: Inserting guests additions

Flare VM (Confi	gurations) [Running] - Oracle	VirtualBox						
le Machine	View Input Devices Hel							
9 = = 1	Manage This PC							- 0
te Computer N	lew Drive Tools							
	is PC >						୍ ଓ Search	This PC
Cuick access	~ Folders (7)							
E Desktop #	3D Objects	Desktop	Documents	Downloads	Music	Pictures		
🕹 Downloads 🖋					.			
Documents #	Videos							
Pictures st	1							
Music	Oevices and drives (2)							
This PC	Local Disk (C:)	CD Drive (D.) VirtualBox Gues	at .					
- INSPC	30.1 GB free of 66.2 GB	0 bytes free of 56.9 MB						
							Activate Windows	

Figure 4: Continuation of inserting guest additions on windows

🌞 Flar	e VM - Settings)	ð	×
Bas	ic Expert							p 👂
	General	🗸 Enable []58 Controller						
	System	USR 1,1 (OHCI) Controller						
	Display	 USB 2.0 (OHCI + EHC) Controller USB 2.0 (rHC) Controller 						
2	Storage	USB Device <u>F</u> ilters						
٠	Audio		🔅 Add Share					1
5	Network		Folder Path:	C:\UsereDrive\Docume	ents 💌			4
	Serial Ports		Folder Name:	Documents				
1	USB		Mount point:					
-	Chanad Falders			<u>R</u> ead-only				
	Shared Folders	Shared Folders		✓ <u>A</u> uto-mount				
•	User Interface	Name Path		Make Permanent		Access Auto Mount		
		Machine Folders		UK C				22
		Transient Folders						
		User Interface						
		I compare and and and						_11

Figure 5: Linking shared folder

The next step was to disable windows updates using group policy. Unlike group policy, pausing windows updates manually is only temporary.



Figure 6: Disabling windows updates using group policy

The next step was to disable windows defender by using group policy. Also turning off tamper protection in the windows security in the virus and threat protection section is required. Aside from that, turning off real time protection is key since it acts as an immediate layer of defense.



Figure 7: Disabling windows defender

To ensure all files and folders are visisble, I had to enable shared folder and uncheck hidden extensions.



Figure 8: Making hidden folders and files visible

Powershell played a key role in installing flare vm following a step by step command from mandiant github repository. After a couple of hours, my flare vm was fully installed.



Figure 9: Flare VM

Challenges and Solutions

I had a error in installing ghidra.vm. The flare vm had downloaded an outdated ghidra and I had to uninstall and install manually using the commands 'choco uninstall ghidra -y' and 'choco install ghidra -y to fix the errors'.

Dependencies such as ida.plugin.xrefer, idr.vm, malware-jail and sfextract gave errors and had to be installed manually. Aside from that, errors kept coming up while installing flare vm because of not properly disabling windows defenders. To fix the error I had to turn off tamper protection to completely disable micrososft antivirus.

Conclusion

Flare vm installation encompasses a wide area in virtualbox configuration for example guest additions and using group policy to disable security policies. It also teaches the virtue of patience and carefully following instructions.

For quicker and successful installation, one has to ensure thete is stable internet and be patient during the installation.

Recommendations

Taking snapshots is necessary to revert changes when necessary. Stable internet is highly recommended for smooth and quicker installation. Ensuring windows defender is completely disabled before installation of the flare vm.

References

- Downloading windows 10. Retrieved from https://support.microsoft.com/en-us/windows/create-installation-media-for-windows-99a58364-8c02-206f-aa6f-40c3b507420d
- Denham, B., & Thompson, D. R. (2022, October). Ransomware and malware sandboxing. In 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0173-0179). IEEE.
- Franko, A. (2024). A Practical Approach to Malware Exploration: Setting up a Dedicated Analysis Lab.
- Installing flare vm. Reterived from https://github.com/mandiant/flare-vm
- Windows defender (2024, March. Retrieved from <u>https://answers.microsoft.com/en-us/windows/forum/all/how-can-i-permanently-disable-or-remove-windows/7e3ce6d4-231f-4bee-912c-3cc031a9bf8d</u>