Prepared by: Amrit Chhetri, Cyber Security Researcher (RCS)| AI Forensics Researcher| Quantum Computing Researcher| Sr. Technical & Managing Editor with ICSRJ, IQCRJ & IMLRJ

Labs. Configuration Guide

for

Malware Investigation with Memory Forensic and Threat Hunting

Contents

Malware Analysis Sandbox and Tools Requirements:

Malware Analysis Labs of this workshop requires:

1. 1 Windows Virtual Machine - Sandbox and Digital Forensics Workstation
2. 1. Linux Virtual Machine - Sandbox and Forensics Workstation
3. 1 Windows and 1 Linux Workstations
4. Memory Forensics Tools, Forensics Images and Case Management Tools
5. Active Accounts in GitHub, ThreatConnect, Splunk Enterprise and Utility Tools
6. SDKs-Python, Java, Julia and PHP and IDEs- PyCharm and Jupyter Lab

Malware Labs Configuration:

Follow the steps below to prepare Forensics Labs for this Workshop:

1. Create this folder, C:\MALWARE-INVESTIGATIONS-WORKSHOP in C-Drive
2. Clone all resources using git ***clone*** ***https://github.com/AmritChhetriB/MalwareAnalysisUsingMemoryForensics.git***
3. Configure Virtual Machines and Sandboxes mentioned above using Tools mentioned below
4. 1 Windows and Linux Workstations Malware Analysis-Tools:

peripherals/Infrastructure	Peripherals/Infrastructure	Specifications	URLs
Virtual Machines	1 Windows Workstations(Victim Machine)	Window 10/11/2019 Pro 64x	
	1 Windows Workstations(Sandbox)	Window 10/11/2019 Pro 64x	-
	Linux Sandbox	RumNux	-
		RUN.ANY	-
Workstation Pre-requisites	Operating System	Windows 10(Pro), 64-Bits	-
	RAM	8-12 GB	-

	Storage/HDD	30 GB	
	CPU	X86-64 Architecture	
	Network Bandwidth/Internet	Internet/LAN	

Prepared by: Amrit Chhetri, Cyber Security Researcher (RCS)| AI Forensics Researcher| Quantum Computing Researcher| Sr. Technical & Managing Editor with ICSRJ, IQCRJ & IMLRJ

#	Function	Category Domain	Platform/Forensic Tools	URL
0	**Malware Sample(OSS)**	Forensic Images	R2D2(pw: infected)	https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples
1	**Acquiring Memory Images**	Forensic Imagers	FTK Imager	
			Belkasoft RAM Capturer	
			Magnet Forensics RAM Capture	
2	**Virtual Machine Sandbox- Windows**	Hypervisor	VMWare Player Workstation	
		Windows Virtual Machines	Windows 2019/2022	
		Sandboxing Tools	ExpressVPN	
			INetSim	
			FakeNet	
		Write Blocker(Software)		
3	**Virtual Machine Sandbox-Linux**	Hypervisor	VMWare Player Workstation	
		Linux	Ubuntu 20.04	
		Sandboxing Tools	ExpressVPN	
			INetSim	
			FakeNet	
4	**Malware Scanning Tools**	Malware Detection	Virus Total	https://www.virustotal.com/gui/
		Process Analysis	ProcessMonitor	https://learn.microsoft.com/en-us/sysinternals/downloads/procmon
		Process and TCP Analysis	TCPView	https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview
5	**Memory Forensics Tools**	Memory Forensics Tool(Commandline)	Volatility	
		Memory Forensics Tool(GUI)	Volatility Workstation	
		Malware Rule Engine	Yara	
		Commercial Memory Forensic Tool	Belkasoft X	
6	**Pre-configured Malware Sandbox**	Malware Analysis Sandbox-VM	RumNux	
		Malware Analysis Sandbox-Online	ANY.RUN	
7	**Vulnerability Analysis**	Vulnerability Scanner	MegaPing	https://magnetosoft.com/product-megaping/
			Nmap	https://nmap.org/download#windows
			Nessus	
8	**Forensic Threat Intelligence**	CTI Tools	ThreatConnect	
			IBM Threat Exchange	
9	**Threat Hunting**	Threat Hunting Tools	APT Hunter	https://github.com/ahmedkhlief/APT-Hunter
			CyberChef	
10	**Network Evidences Analysis**	Network Traffic/Packet Analyzers	Network Miner	https://www.netresec.com/?page=NetworkMiner
			Capsa Network Analyzer	https://www.colasoft.com/capsa-free/
			Splunk Enterprise/Free	
11	**Forensic Case Management**	Digital Forensics Triage	Autopsy	https://www.autopsy.com/download/
			Belkasoft X	https://belkasoft.com/x
12	**Forensic Triage**	Computer/Memory Forensic Triage	Mangent AXIOM Cyber	https://www.magnetforensics.com/products/magnet-axiom-cyber/
			FireEye Redline	https://fireeye.market/apps/211364
			CyberTriage	
13	**Incident Response**	Memory Incident Response	Mandient Redline	
			Redline Memoryze	

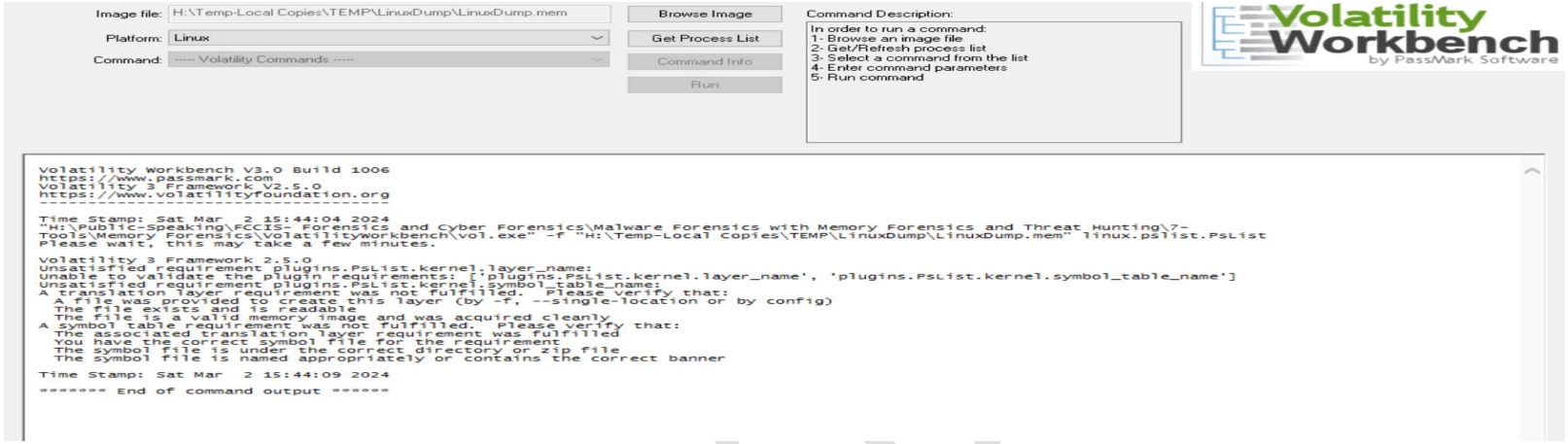
Security Labs for Digital Payments-Configurations:

Follow the steps below to install and configure all necessary tools. All details are for Tools for advanced settings.

1. **Configuration of Volatility:**
    1. Download Volatility and extract inside ***C:\MALWARE-INVESTIGATIONS-WORKSHOP\FORENSIC-SCRIPTS-TOOLS***
    2. Then set ***C:\MALWARE-INVESTIGATIONS-WORKSHOP\FORENSIC-SCRIPTS-TOOLS\Memory-Forensics\volatility_2.6_win64_standalone*** in PATH
    3. Download https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples and unzip inside evidence folder
    4. Run to check the configuration: ***volatility -f Evidence.vmem --profile=WinXPSP2x86 psxview***

```
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x015a9020 winlogon.exe            632 True   True   True     True   True  True    True
0x018da020 services.exe            676 True   True   True     True   True  True    True
0x0156c5a0 alg.exe                1616 True   True   True     True   True  True    True
0x018d63d0 VMwareTray.exe          184 True   True   True     True   True  True    True
0x019757f0 svchost.exe             916 True   True   True     True   True  True    True
0x015c4020 lsass.exe               688 True   True   True     True   True  True    True
0x01972ca8 vmacthlp.exe            832 True   True   True     True   True  True    True
0x019a34b0 cmd.exe                 544 True   True   True     True   True  True    True
0x0187e9d0 svchost.exe             848 True   True   True     True   True  True    True
0x017daca8 svchost.exe            1020 True   True   True     True   True  True    True
0x01954990 VMwareService.e        1444 True   True   True     True   True  True    True
0x018c6da0 svchost.exe             964 True   True   True     True   True  True    True
```

    5. Alternatively, download and use Volatility Workbench



2. Configuration of Yara:

1. Download Yara from and extract and then extracted folder into PATH variable
2. Run yara64.exe MalwareAnalysis2019.yara Evidence.vmem to test the configuration

```
C:\AUTOMATIONS-AI-CS-DFIR SCRIPTS\Digital-Forensics\Malware Analysis-Yara\Lab2-Malware-Analysis> yara64.exe Ma
lwareAnalysis2019.yara Evidence.vmem
MaliciousSite_Detection Evidence.vmem

C:\AUTOMATIONS-AI-CS-DFIR SCRIPTS\Digital-Forensics\Malware Analysis-Yara\Lab2-Malware-Analysis> yara64.exe Ma
lwareAnalysis2019.yara Evidence.vmem
MaliciousSite_Detection Evidence.vmem

C:\AUTOMATIONS-AI-CS-DFIR SCRIPTS\Digital-Forensics\Malware Analysis-Yara\Lab2-Malware-Analysis>
```

Network Security Coding Snippets:

1. Create a folder "Python4RNetworkSecurity" in a Drive and also install Git from URL given earlier
2. Open Command Prompt and check out the code using '***git clone https://github.com/AmritChhetriB/MalwareAnalysis.git***'

Registration and Accounts Creations:

1. Register Account with VirusTotal, Online Anti-Virus Solution powered by AI at https://www.virustotal.com/gui/
2. Account Registration for Cyber Crimes Reporting
   Open https://cybercrime.gov.in in a Browser and complete the registration to get ready to report Digital Payments Crimes.

Quantum Circuits, Algorithms and QML for Network Security (Extra Bites, Optional):

1. Create an account with IBM and login to IBM Quantum site to get API key
2. Install Jupyter Notebook and PyCharm(add qiskit plugin)
3. Use Q-Kit and Composer to design Quantum Circuits for different Algorithms and use Qiskit to write that Circuits Design into Quantum Algorithms.

Yara Configuration:

Follow steps below to configure Yara in Standalone Mode:

1. **Yara Configuration on Windows:**
   a. Get Yara Executable, yara-4.3.2-2150-win64.zip from
   b. Keep Executable in PATH
   c. Prepare two files- Yara Rule and Text Evidence as given in folder
      i. Yara Rule: DetectionRule.yara

```
rule MaliciousSite_Detection
        {
        meta:
                author = "Amrit Chhetri"
                date   = "07-01-2024"
                Purose = "Malware Detection"
        strings:
                $MaliciousWeb1 = "www.xxx2.com"
                $MaliciousWeb2 = "www.xxx1.com"
                $Maliciousweb3 = "www.yyyy2.com"
```

```
        $AttackerName1 = "hackx1203"
        $AttackerName2 = "Hackor"
        $AttackerName3 = "Hax"

    condition:
    any of them
    // $MaliciousWeb1 and $MaliciousWeb2 and $MaliciousWeb2
    }
```

ii. Text Evidence: EvidenceURLs.txt

```
www.xxx1.com
www.xxx2.com
www.xxx.com
hackx1203
Hackor
```

d. And run *yara64.exe MalwareAnalysis.yara Evidence.vmem*

2. Running Yara with Volatility:

a. volatility –f Evidence.vmem --profile=WinXPSP2x86 yarascan -Y "https:"
b. volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan -p 1956 -Y "https:"
c. volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan -Y "com"
d. volatility –f Evidence.vmem --profile=WinXPSP2x86 yarascan -Y "172.16.98.1"
e. volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan --yara-file=TrojanAnalysis.yara