

Configuration Manual

MSc Internship MSc in Cyber Security

Niall O'Brien Student ID: x20196474

School of Computing National College of Ireland

Supervisor: Michael Pantridge

I. INTRODUCTION

This configuration manual was developed to show requirements needed to setup a virtual lab environment to install windows and Linux machines. From there the manual will cover the installation of Threat hunting tools Velociraptor and Hayabusa. Snort intrusion detection tool and lastly malware analysis tool PeStudio. The manual will also show examples of attack simulations and malware that was used to conduct research into the Cyber hacking group known as Cozy Bear, APT29.

II. SYSTEM REQUIREMENTS

Windows 10 laptop with the below System information was used to setup a lab environment to allow this author to then install tools and run tests.

A. Windows 10

Nystem Information				-	٥	×
File Edit View Help						
System Summary	Item	Value				^
Hardware Resources	OS Name	Microsoft Windows 10 Pro				
Components	Version	10.0.19044 Build 19044				
Software Environment	Other OS Description	Not Available				
	OS Manufacturer	Microsoft Corporation				
	System Name	DESKTOP-8NMJP1T				
	System Manufacturer	Dell Inc.				
	System Model	Latitude E5470				
	System Type	x64-based PC				
	System SKU	06DE				
	Processor	Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz, 24	196 Mhz, 2 Core(s), 4 Logical P	r		
	BIOS Version/Date	Dell Inc. 1.17.3, 17/08/2017				
	SMBIOS Version	3.0				
	Embedded Controller Version	255.255				
	BIOS Mode	UEFI				
	BaseBoard Manufacturer	Dell Inc.				
	BaseBoard Product	ОНСРОК				
	BaseBoard Version	A05				
	Platform Role	Mobile				
	Secure Boot State	On				
	PCR7 Configuration	Elevation Required to View				
	Windows Directory	C:\WINDOWS				
	System Directory	C:\WINDOWS\system32				
	Boot Device	\Device\HarddiskVolume1				
	Locale	Ireland				
	Hardware Abstraction Layer	Version = "10.0.19041.1806"				
	User Name	DESKTOP-8NMJP1T\Niall				
	Time Zone	GMT Daylight Time				
	Installed Physical Memory (RAM)	16.0 GB				~
Find what:			Find C	lose Find		
Search selected category only	Search category names	s only				

B. VirtualBox 6.1.

The latest version of Oracle VirtualBox¹ was then installed on the windows 10 machine to allow configuration of Ubuntu and Windows virtual machines to install software tools on.

¹ "Oracle VM VirtualBox," no. 1, accessed August 15, 2022, https://www.virtualbox.org/.



C. Lab Virtual Machines

Installed ubuntu 20.04² linux machine and 2 x Microsoft Windows 11 machines in Oracle VirtualBox Manager console using developer³ images.



² "Install Ubuntu Desktop | Ubuntu," no. 2, accessed August 15, 2022, https://ubuntu.com/tutorials/install-ubuntu-desktop#1-overview.

³ deepakmsft, "Download a Windows Virtual Machine - Windows App Development," no. 3, accessed August 15, 2022, https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/index.html.

III. SOFTWARE TOOLS USED

A. Velociraptor

Installed Velociraptor⁴ v0.6.5 threat hunting tool on Ubuntu 20.04 machine linux machine. Can also be installed directly on Windows machines but preferred method is to install on Linux as master server then install client service on Windows machines to view from the master window below and query these machines from here.



B. Hayabusa

Installed Hayabusa⁵ v1.4.2 Threat hunting tool on one of the Windows 11 machines in the lab. From the command window below a user can point the Hayabusa.exe file against a target to get file information to spot potential malicious files.

⁴ "Install and Setup Velociraptor on Ubuntu 20.04 - Kifarunix.Com," no. 4, accessed August 15, 2022, https://kifarunix.com/install-and-setup-velociraptor-on-ubuntu-20-04/.

⁵ "About Hayabusa," Rust (2020; repr., Yamato Security 大和セキュリティ, August 14, 2022), no. 5, https://github.com/Yamato-Security/hayabusa.

an Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.795] (c) Microsoft Corporation. All rights reserved.
C:\Windows\system32>target\release\hayabusa.exe The system cannot find the path specified.
C:\Windows\system32>cd C:\Users\User\Desktop\Playing\hayabusa
C:\Users\User\Desktop\Playing\hayabusa>target\release\hayabusa.exe
by Yamato Security
USAGE: hayabusa.exe -f file.evtx [OPTIONS] / hayabusa.exe -d evtx-directory [OPTIONS]
OPTIONS: European-time Output timestamp in European time format (ex: 22-02-2022 22:00:00.123 +02:00)
RFC-2822 Output timestamp in RFC 2822 format (ex: Fri, 22 Feb 2022 22:00:00 -0600)

C. Neo4j

Installed NeO4j⁶ v1.4.15 on one of the windows 11 machines in the lab. Neo4j is a graph database management system that allows a user to import data from JSON, CSV, GraphML, Cypher script and txt files to identify vulnerabilities, analyze network health, and visualize its unpredictable patterns.

P Neo File Edi	4j Desktop - 1.4.15 t View Window Help Developer		×
۲ ۵	Projects 🕂 🛛 New	No active DBMS	٩
00	🗅 Example Project	Project	Add -
	D Project	ee Graph DBMS 4.4.5	Start 🕞 Open - •••
		File	Reveal files in File Explorer
?			Add project files to get started.
¢			
ঠ্য			
6			
\$			

D. Snort

Installed Snort⁷ v2.9.7.0 network intrusion system on the ubuntu 20.04 machine where it can be pointed to monitor traffic on the ubuntu or windows machines used in the lab.

⁶ "Windows Installation - Operations Manual," no. 5, accessed August 15, 2022,

https://neo4j.com/docs/operations-manual/4.4/installation/windows/.

⁷ "Snort - Network Intrusion Detection & Prevention System," no. 6, accessed August 14, 2022, https://www.snort.org/.



E. PeStudio

Installed PeStudio⁸ v9.38 a static analysis tool used for analyzing malware without running it.



⁸ "Winitor," no. 7, accessed August 15, 2022, https://www.winitor.com/download.

IV. TESTS CONDUCTED

A. Velociraptor Artifact Query

An executable file installed on one of the Windows 11 machines in the lab used for this paper is picked up by running an Artifact process called 'Windows.System.Pslist artifact' from the Velociraptor window pointed towards the connected Windows machine. From this VQL query you can get the hash of a file and enter the hash on Virustotal.com site to see if it is malicious.

Voluntu 2 File Mach	G Uburtu 2014 (Running) - Orack W VirtusBox									- a >			
Activities	Activities 💙 Firefor Web Browser + Jul 20 15:55 •										A ● @		
	😒 Ve	lociraptor	Response	IR 372: Inv	estigating a PU ×								
	←	\rightarrow C		O 🗛 http	s:// 10.0.2.16 :888	9/app/index.html#/col	lected/C.d81629b	61788b523/F.CBC1E5HENU898/results			☆		© ± ≡
9	≡	all 😡			۹ -			١	Fest2.home 😑 Connected				😔 admin
	*	+	ф <u>т</u>										
	Φ	State 4		FlowId	Artif	acts	\$	Created \$	Last Active 🗢	Creator	\$	Mb ¢	Rows \$
0	ş	~	F	CBC1E5HENU898	Window	vs.System.Pslist		2022-07-20T14:54:14Z	2022-07-20T14:54:16Z	admin			
	۲	~	F	CBC0QRJG1PVGO	Generio	c.Client.Info		2022-07-20T14:13:02Z	2022-07-20T14:13:04Z	InterrogationService			
	≡	Windo	ws.Syster	n.Pslist									Ý
Â			- 11	± 8 T									
	브	Pid	Ppid	TokenIsElevated	Name	CommandLine	Exe	Hash		Authenticode	Username	WorkingS	etSize
 ? ? ? 	1 0 A	761:	<u>.</u> 4592	false	pup4message .exe	°C.\pup4message.e xe*	C:\pup4messa ge.exe	<pre>* { "M05": "a53bfca803e217b9 "SHA1": "da0935468e6ca86 "SHA15": "da0935468e6ca86 "H04bd8bc30e36fbcfa39295 cc3a42608d88e9" }</pre>	d599c7c774970550" 805dafc301566d1a1285ad054" ia8b5e3623834d1282f7eb082c	<pre>*{ "filename": "C:\pup4message.exe" "ProgramName": www. "PublisherLink": www. "MoreInfolink": www. "SerialNumber": www. "IssuerName": www. "SubjectName": www. "Timestamp": www. "Trusted": "untrusted" "_ExtraInfo":{ }</pre>	TEST2\User	9433088	

B. Run Hayabusa against attack samples

For this example a container for windows events samples that have been associated with specific attacks and post exploitation techniques from Github⁹ was used to run the Hayabusa tool against on one of the Windows 11 machines on this authors lab.



⁹ "GitHub - Sbousseaden/EVTX-ATTACK-SAMPLES: Windows Events Attack Samples," no. 8, accessed August 15, 2022, https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES.

C. Import of Hayabusa attack samples file into Ne04j desktop

Imported txt file(password infected) of attack samples picked up in the Hayabusa scan above with command below executed within Neo4j run window to produce critical alert (critical attacks) found in this file.

//Critical View MATCH (h: Host)-[:Severity{level:"critical"}]-(a: Alert) RETURN h, a

	R	^ _ e	×
neo4j\$ MATCH (h: Host)-[:Severity{level:"critical"}]-(a: Alert) RETURN h, a	•	습	±
Node Properties a			>
			Gi.
A The American			(à
	\$	~ 2	×
neo4j\$ MATCH (n) RETURN n	•	☆	٤
	\$7	~ .*	×
neo4j\$ LOAD CSV WITH HEADERS FROM 'file:///playing/alerts-transform1.txt' AS row MERGE (a:Alert{name:row.RuleTitle}) MERGE (h:Host{name:row.Computer}) MERGE (a)-[:Sev		☆

D. Run Snort to pickup Nmap scan

Run Snort command to pickup all network traffic generated on ubuntu machine in the lab while running Nmap scan from one of the Windows 11 machines pointing towards the IP of the ubuntu machine to generate snort alert 'TCP Port Scanning'.

🛃 Ubuntu 20	0.04 [Running] - Oracle VM VirtualBox		– 0 ×
File Machi	ine View Input Devices Help		
Activities	s 🕒 Terminal 🔻	Aug 8 22:09 •	📥 🐠 🌆 👻
·😂	A hacker		
9		hacker@hacker-VirtualBox: ~ 🔍 📃 🗕 🗆 😣	
	Trash Trash Frash ERROR: Can't start DAQ Fatal Error, Quitting	sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3 x:~\$ sudo snort -A console -q -c /etc/snort/snort.conf -i 10.0.2.15 (-1) - SIOCGIFHWADDR: No such device!	
0	hacker@hacker-VirtualBo ^Chacker@hacker-Virtual 08/08-22:08:53.572398 08/08-22:08:53.572587	x:-\$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3 Box:-\$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3 [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50321 -> 10.0.2.16:80 [**] [1:0000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50323 -> 10.0.2.16:80	
	08/08-22:08:53.714041 2.16:80 08/08-22:08:53.789437	<pre>[**] [1:1000006:2] "TCP Port Scanning" [**] [Priority: 0] {TCP} 10.0.2.15:50321 -> 10.0. [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50324 -> 10.0.2.16:80 [***] [0.100000000012] [0.1000000000000]</pre>	
Â	08/08-22:08:54.005017 analyser@192.08/08-22:08:54.005017 68.56.107 08/08-22:08:54.246333	[**] [1:10000100:5] http test [**] [Priority: 0] (TCP) 10.0.2.15:50327 -> 10.0.2.16:80 [**] [1:10000100:5] http test [**] [Priority: 0] (TCP) 10.0.2.15:50327 -> 10.0.2.16:80 [**] [1:10000100:5] http test [**] [Priority: 0] (TCP) 10.0.2.15:50329 -> 10.0.2.16:80	
?	08/08-22:08:54.315382 08/08-22:08:54.455140 08/08-22:08:54.696395 08/08-22:08:54.907195	<pre>[**] [::10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50330 -> 10.0.2.16:80 [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50333 -> 10.0.2.16:80 [**] [1:10000100:5] http test [**] [Priority: 0] {TCP} 10.0.2.15:50335 -> 10.0.2.16:80</pre>	
· >_	Lab_01-2.malv 08/08-22:09:00.169759 re 15:50338	[**] [1:1000006:2] "TCP Port Scanning" [**] [Priority: 0] {TCP} 10.0.2.16:445 ↔ 10.0.2.	
	re		
			🔲 🗐 🔐 🔯 🚫 💽 Right Ctrl

E. Open Cozy Bear Wellmess Malware using PeStudio

Downloaded Wellmess malware with Hash:

953b5fc9977e2d50f3f72c6ce85e89428937117830c0ed67d468e2d93aa7ec9a onto Windows 11 machine and then opened it using PeStudio to get information including its vendor rating from virustotal.com

estudio 9.38 - Malware Initial Assessment - www.wi file settings about	nitor.com [c:\953b5fc9977e2	2d50f3f72c6ce85e89428937117830c0ed67d46	8e2d93aa7ec9a]	_	
📽 🖬 🗡 📋 🤶					
	engine (70/70)	score (58/70)	date (dd.mm.yyyy)	age (days)	
Jul indicators (33)	Bkay	W32.AIDetectNet.01	28.07.2022	9	
virustotal (58/70)	Elastic	malicious (high confidence)	23.06.2022	44	
dos-header (64 bytes)	MicroWorld-eScan	Gen:Variant.Razv.279280	28.07.2022	9	
dos-stub (64 bytes)	FireEve	Generic.mg.f18ced8772e9d1a6	28.07.2022	9	I
P rich-header (n/a)	CAT-QuickHeal	Trojan.Wellmess	28.07.2022	9	
Tile-neader (Mar.2018)	McAfee	Generic Trojan.nm	28.07.2022	9	
directories (5)	Cylance	Unsafe	28.07.2022	9	
Sections (97.62%)	VIPRE	Gen:Variant.Razy.279280	27.07.2022	10	
libraries (mscoree.dll)	Sangfor	Suspicious.Win32.Save.a	22.07.2022	15	
functions (145)	K7AntiVirus	Trojan (0056ac501)	28.07.2022	9	
	Alibaba	Trojan:Win32/WellMess.fb822752	27.05.2019	1167	
tis-callbacks (n/a)	K7GW	Trojan (0056ac501)	28.07.2022	9	
	Cybereason	malicious.772e9d	30.03.2021	494	
	Cyren	W32/MSIL_Wellmess.A!Eldorado	28.07.2022	9	
abc strings (size) *	Symantec	Trojan.Gen.2	28.07.2022	9	
i	ESET-NOD32	MSIL/Agent.CYA	28.07.2022	9	
≝ Windows (C:)	॥ î↓ Sort	~ = View ~			- 0
\leftarrow \rightarrow \checkmark \uparrow \blacksquare \rightarrow This PC \rightarrow Windows (C	:)		~ C	,	h Windows (C:)
🔁 import Name	Dat	e modified Type	Size		
playing	72c6ce85e89428937 2/2	0/2022 2:38 AM File	168 KB		

REFERENCES

- "About Hayabusa." Rust. 2020. Reprint, Yamato Security 大和セキュリティ, August 14, 2022. https://github.com/Yamato-Security/hayabusa.
- deepakmsft. "Download a Windows Virtual Machine Windows App Development." Accessed August 15, 2022. https://developer.microsoft.com/en-us/windows/downloads/virtualmachines/index.html.
- "GitHub Sbousseaden/EVTX-ATTACK-SAMPLES: Windows Events Attack Samples." Accessed August 15, 2022. https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES.
- "Install and Setup Velociraptor on Ubuntu 20.04 Kifarunix.Com." Accessed August 15, 2022. https://kifarunix.com/install-and-setup-velociraptor-on-ubuntu-20-04/.
- "Install Ubuntu Desktop | Ubuntu." Accessed August 15, 2022. https://ubuntu.com/tutorials/installubuntu-desktop#1-overview.
- Neo4j Graph Data Platform. "Neo4j Desktop Neo4j Browser." Accessed August 14, 2022. https://neo4j.com/docs/browser-manual/4.4/deployment-modes/neo4j-desktop/.
- "Oracle VM VirtualBox." Accessed August 15, 2022. https://www.virtualbox.org/.
- "Snort Network Intrusion Detection & Prevention System." Accessed August 14, 2022. https://www.snort.org/.
- "Windows Installation Operations Manual." Accessed August 15, 2022. https://neo4j.com/docs/operations-manual/4.4/installation/windows/.