Configuration Manual

MSc Internship
MSc in Cyber Security

Niall O'Brien
Student ID: x20196474

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

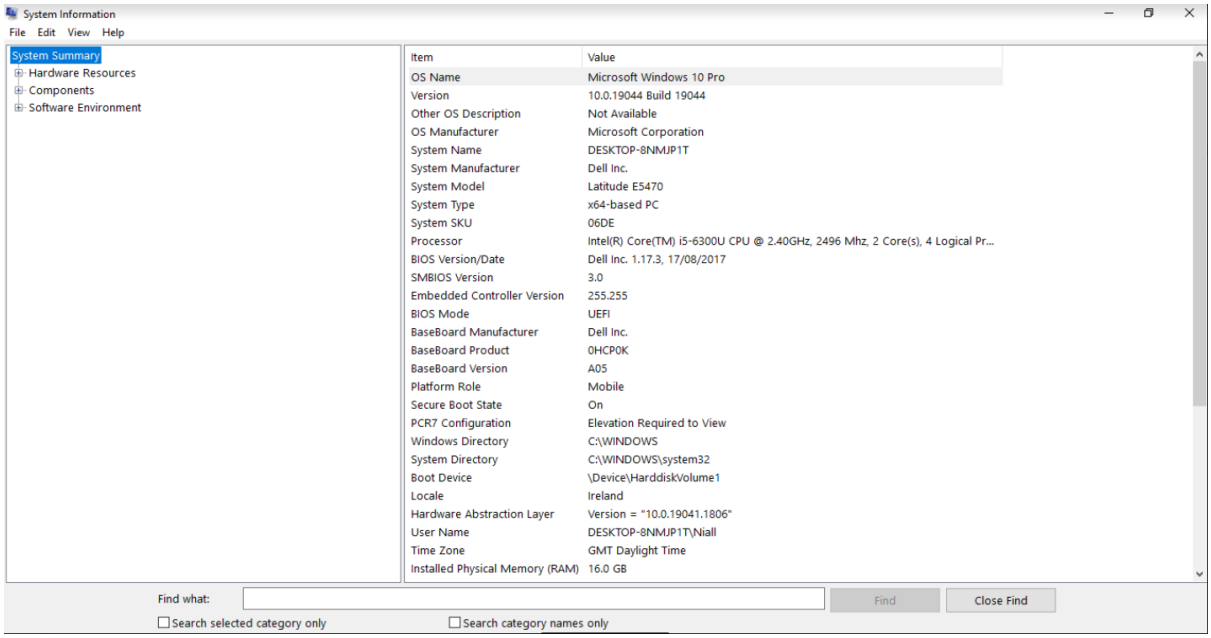
I. INTRODUCTION

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.

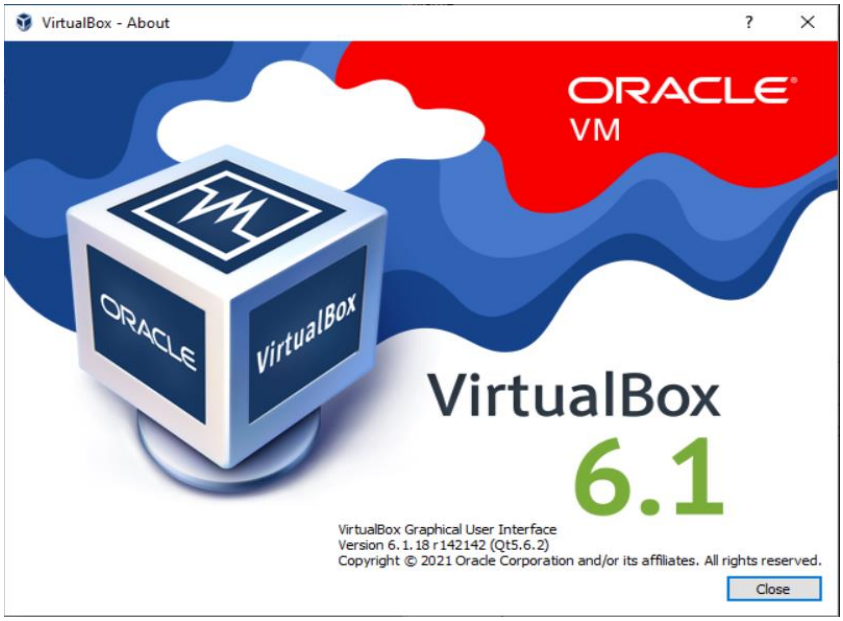
A. Windows 10



B. VirtualBox 6.1.

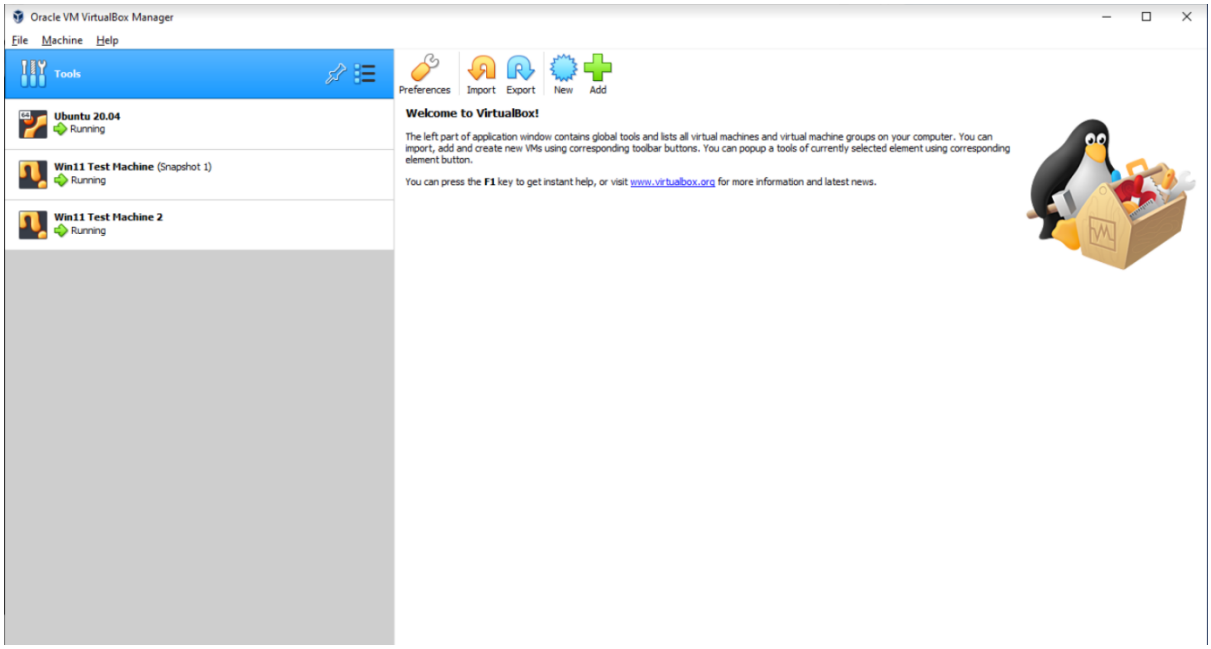
The latest version of Oracle VirtualBox[1] was then installed on the windows 10 machine to allow configuration of Ubuntu and Windows virtual machines to install software tools on.

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



C. Lab Virtual Machines

Installed ubuntu 20.04[2] linux machine and 2 x Microsoft Windows 11 machines in Oracle VirtualBox Manager console using developer[3] images.

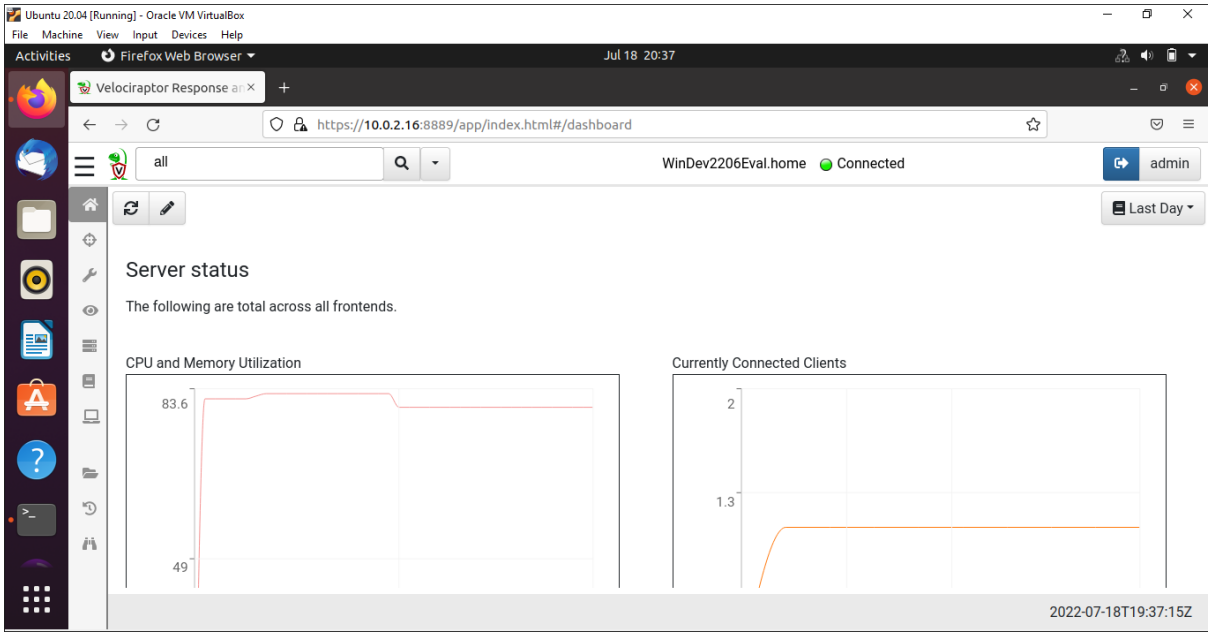


[2] "Install Ubuntu Desktop | Ubuntu," no. 2, accessed August 15, 2022, https://ubuntu.com/tutorials/install-ubuntu-desktop#1-overview.
[3] deepakmsft, "Download a Windows Virtual Machine - Windows App Development," no. 3, accessed August 15, 2022, https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/index.html.

III. SOFTWARE TOOLS USED

A. *Velociraptor*

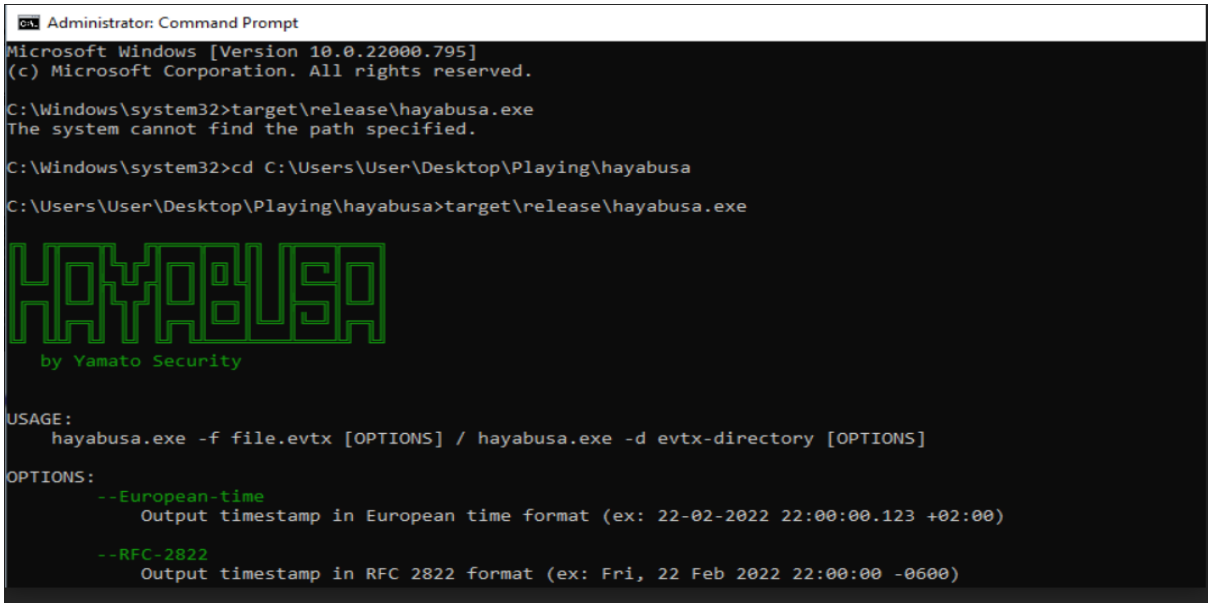
Installed Velociraptor[4] v0.6.5 threat hunting tool on Ubuntu 20.04 machine linux machine. Can also be installed directly on Windows machines but preferred method is to install on Linux as master server then install client service on Windows machines to view from the master window below and query these machines from here.



B. *Hayabusa*

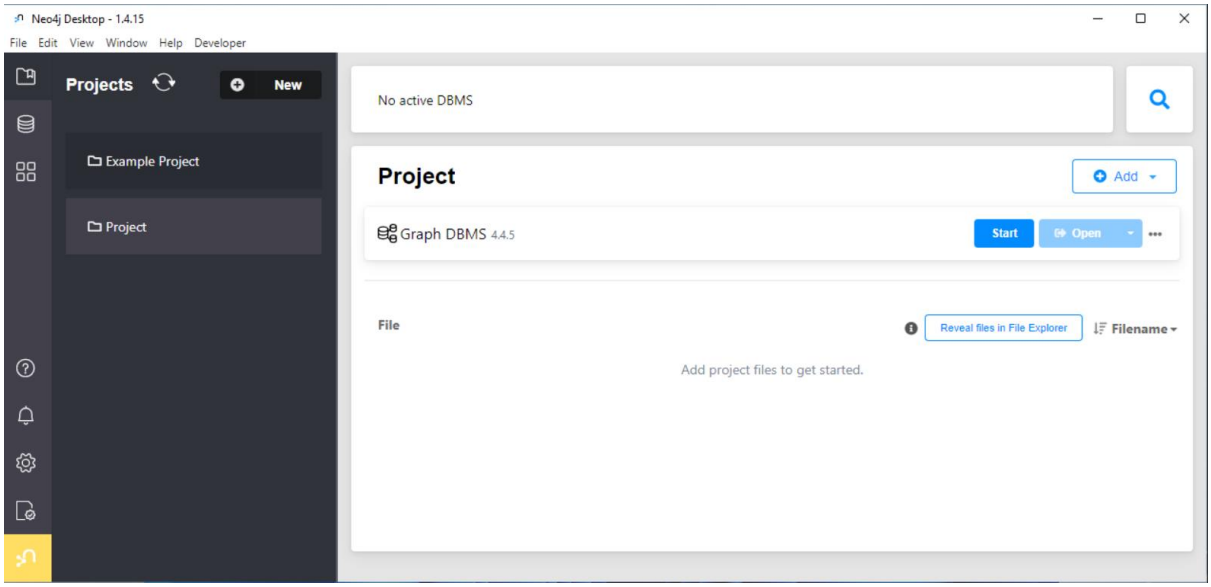
Installed Hayabusa[5] v1.4.2 Threat hunting tool on one of the Windows 11 machines in the lab. From the command window below a user can point the Hayabusa.exe file against a target to get file information to spot potential malicious files.

[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.



C. Neo4j

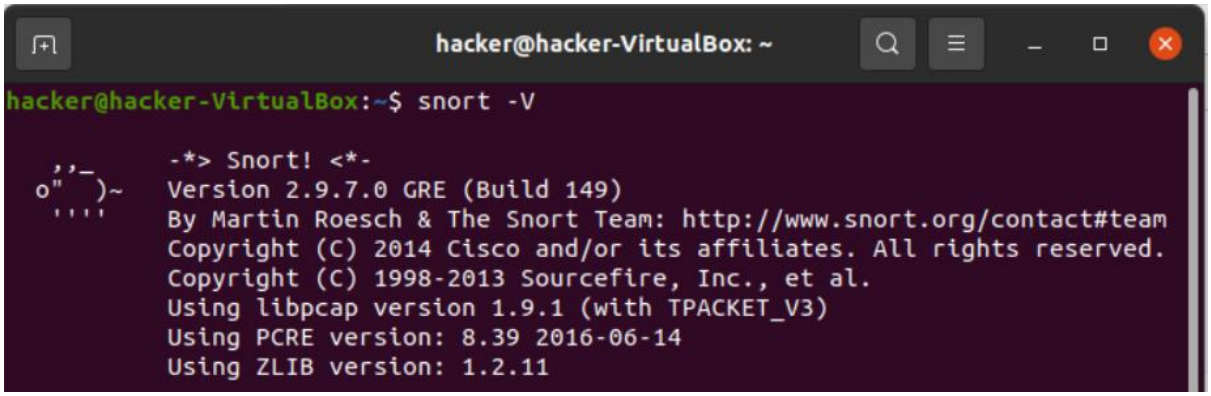
Installed Ne04j[6] v1.4.15 on one of the windows 11 machines in the lab. Neo4j is a graph database management system that allows a user to import data from JSON, CSV, GraphML, Cypher script and txt files to identify vulnerabilities, analyze network health, and visualize its unpredictable patterns.



D. Snort

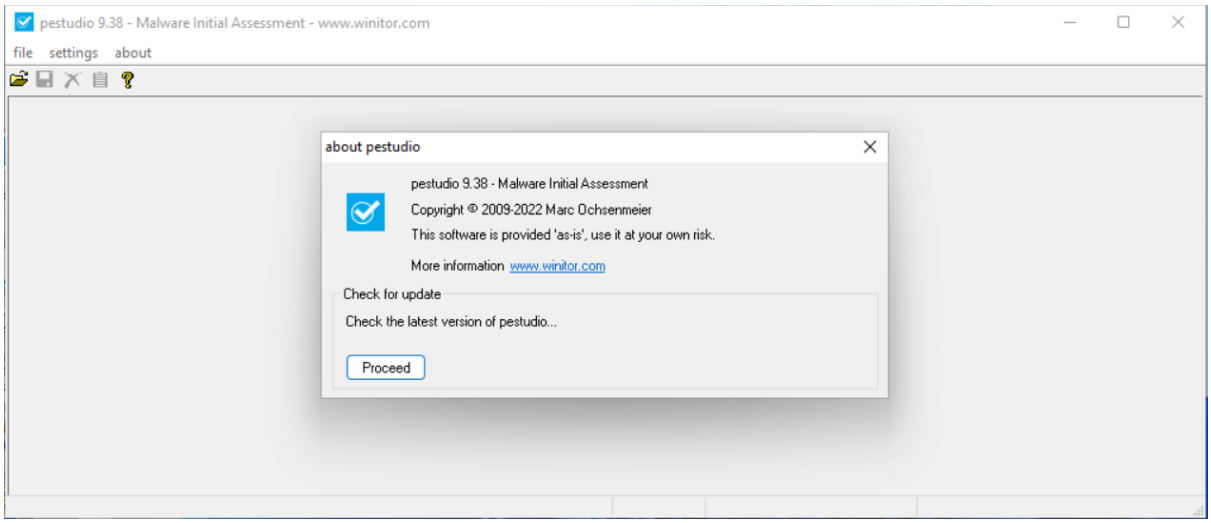
Installed Snort[7] v2.9.7.0 network intrusion system on the ubuntu 20.04 machine where it can be pointed to monitor traffic on the ubuntu or windows machines used in the lab.

[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 PeStudio[8] v9.38 a static analysis tool used for analyzing malware without running it.

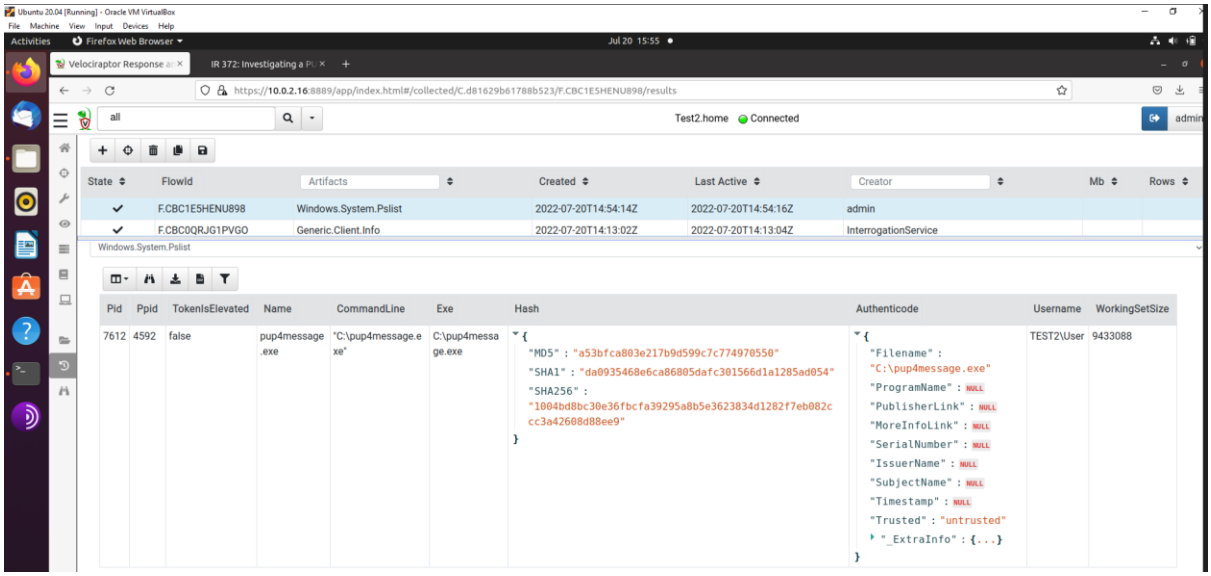


[8] "Winitor," no. 7, accessed August 15, 2022, https://www.winitor.com/download.

IV. TESTS CONDUCTED

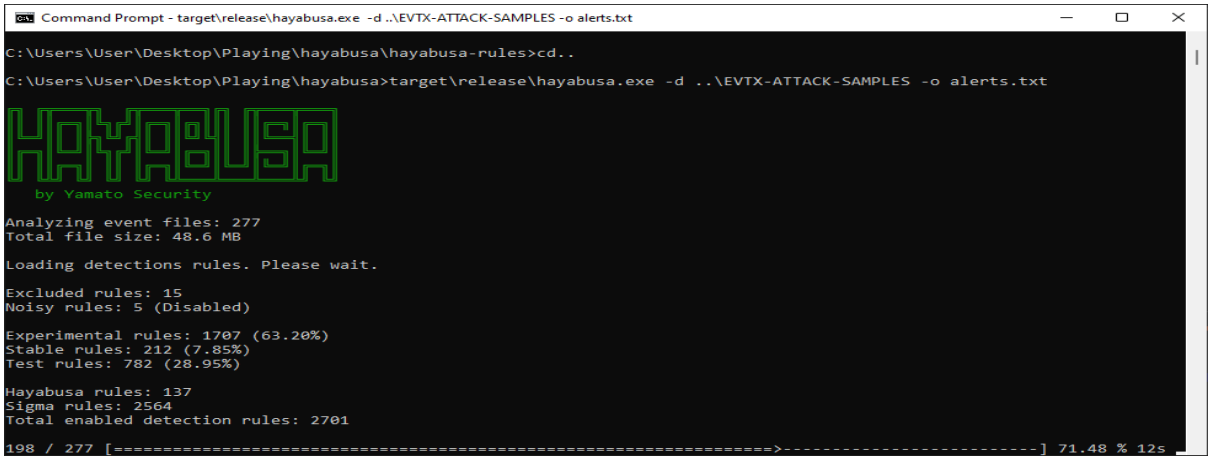
A. *Velociraptor Artifact Query*

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.



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 Github[9] was used to run the Hayabusa tool against on one of the Windows 11 machines on this authors lab.

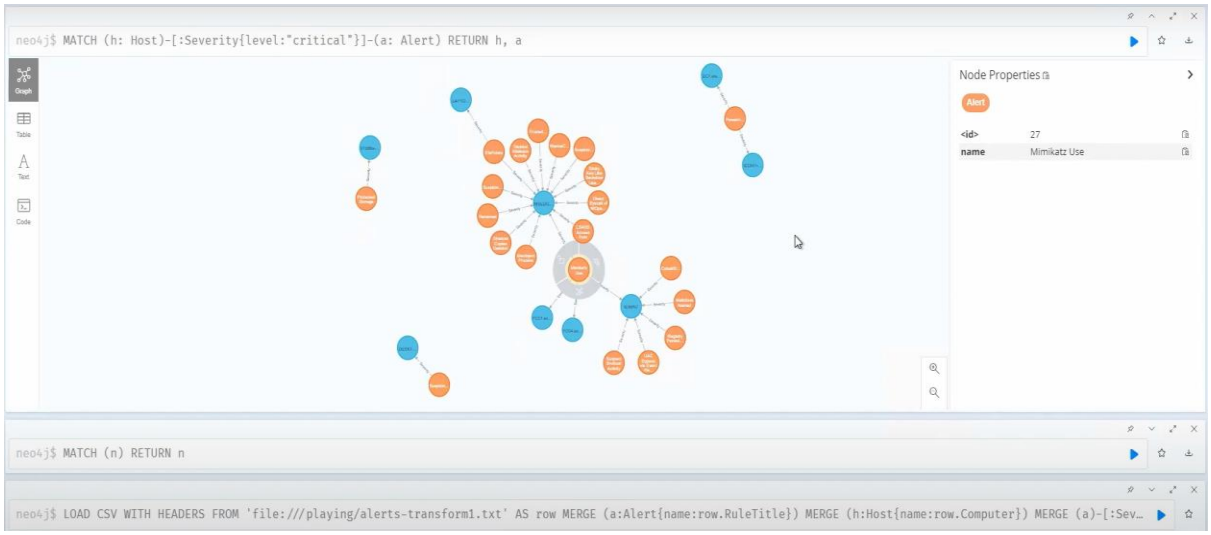


[9] "GitHub - Sbousseaden/EVTX-ATTACK-SAMPLES: Windows Events Attack Samples," no. 8, accessed August 15, 2022, https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES.

C. Import of Hayabusa attack samples file into Ne04j desktop

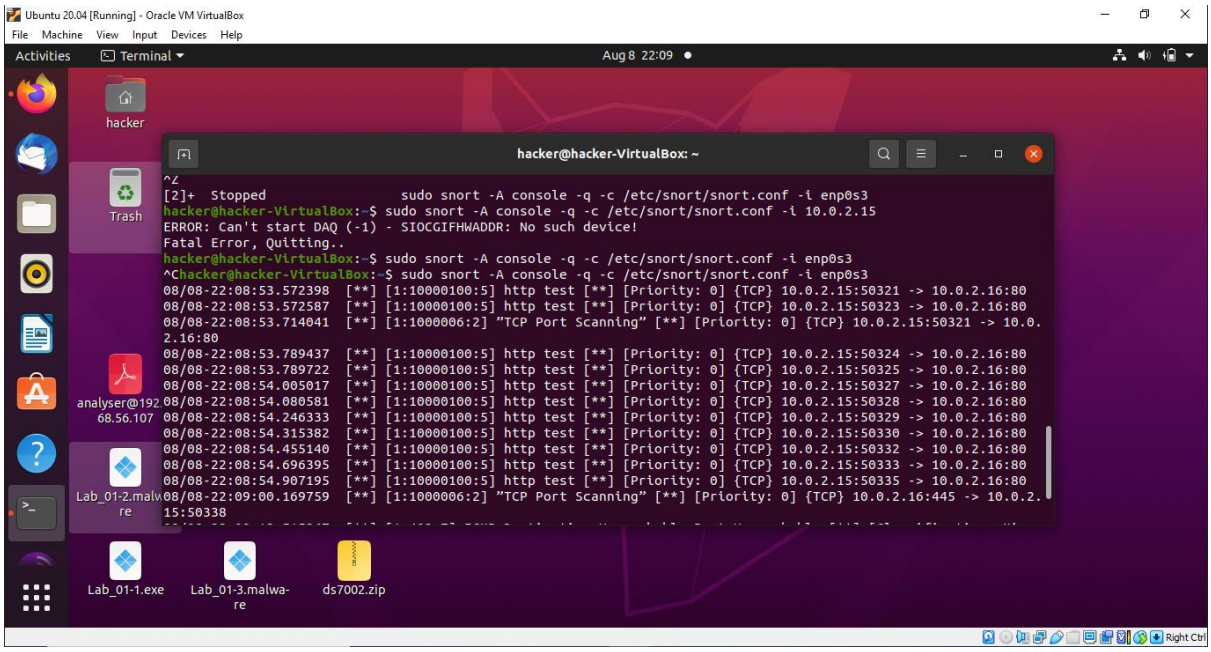
Imported txt file(password infected) of attack samples picked up in the Hayabusa scan above with command below executed within Neo4j run window to produce critical alert (critical attacks) found in this file.

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



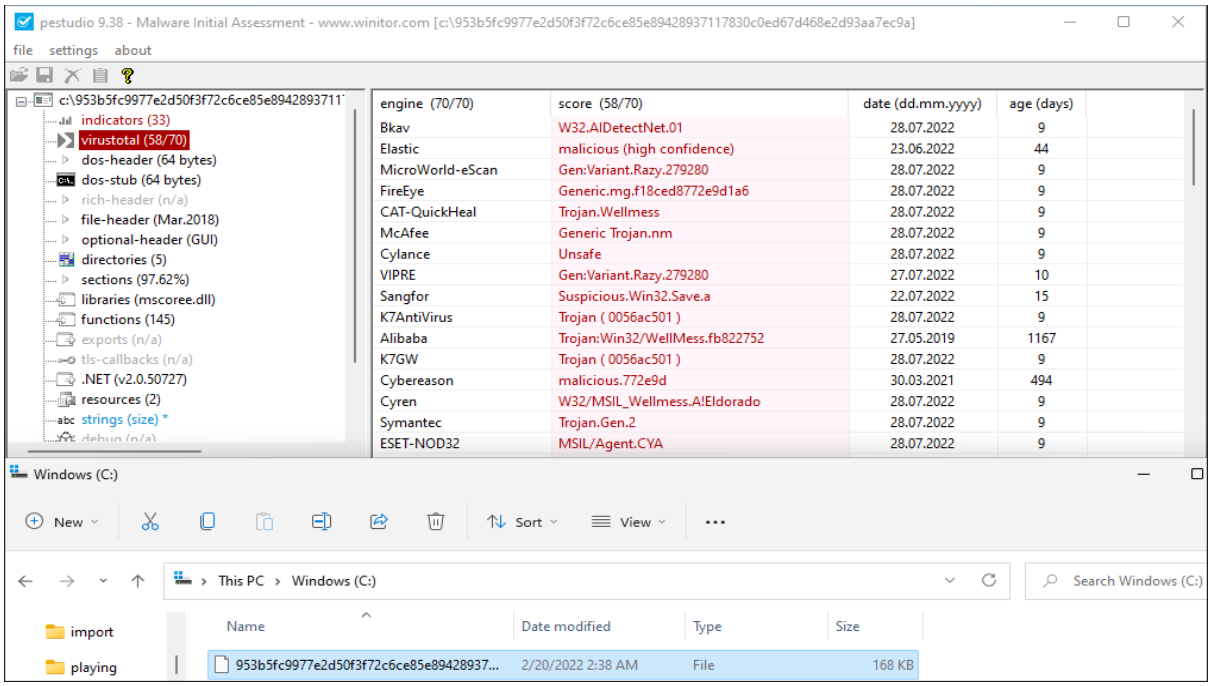
D. Run Snort to pickup Nmap scan

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'.



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



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/virtual-machines/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/install-ubuntu-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/.