

Configuration Manual

MSc Research Project
Programme Name

Preetam Kolekar
Student ID: x21179352

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name:Preetam Kolekar

Student ID:x21179352.....

Programme:Msc in Cybersecurity (MSCCYB1) **Year:**2023.....

Module:Research Project.....

Lecturer:Michael Pantridge.....

Submission Due Date:18/09/23.....

Project Title:Tackling the Cyber Kill Chain in A Lab Environment.....

Word Count:700..... **Page Count:**8.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:Preetam Kolekar.....

Date:18/09/23.....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

The overall configuration includes:

1. Kali VM,
2. Windows VM,
3. SIEM Tool,
4. Snort,
5. OSSEC,
6. YARA

1. Kali and Windows system Credentials.

Kali credentials:

Username – **Kali**

Password – **Kali**

IP address: **192.168.8.32/24**

Windows credentials:

Username – **Admin**

Password (not required) –

IP Address: **192.168.8.45/24**

2. SIEM

The implemented SIEM can be accessed using: <https://elk-0d06b5.kb.us-central1.gcp.cloud.es.io:9243/app/home#/> as it is hosted on the cloud. (Strand, 2022)

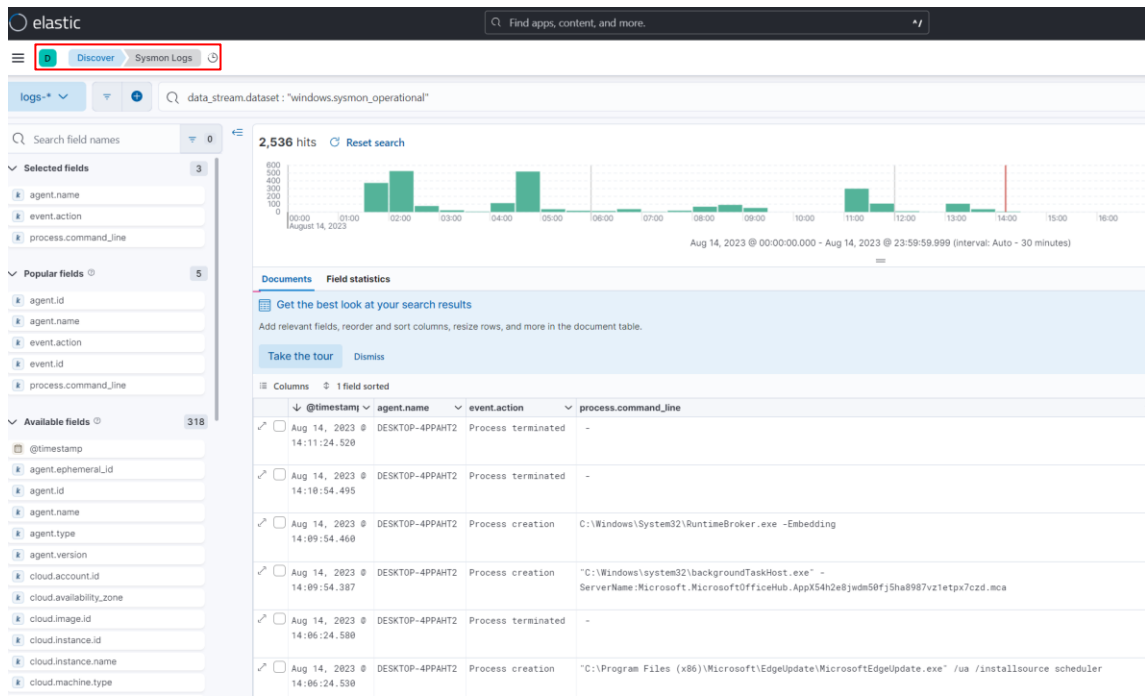
The assessor can login with the credentials:

Username: pritamkolekar7@gmail.com

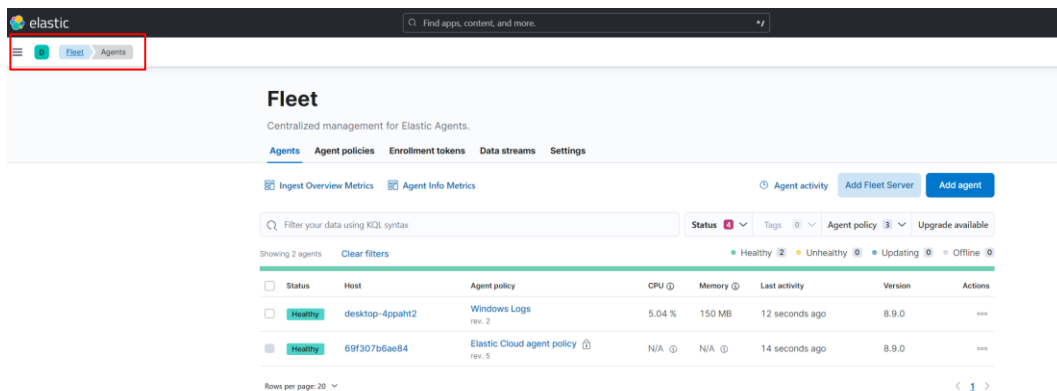
Password: Thesis*Aug23

To be able to see the Sysmon logs running on the system, you can navigate to:

Discover > Sysmon Logs >



You can play around the search filters to be able to see the parameters as per your liking.



You can navigate to Management > Fleet. There you can see the agent which is the Windows 10 Lab.

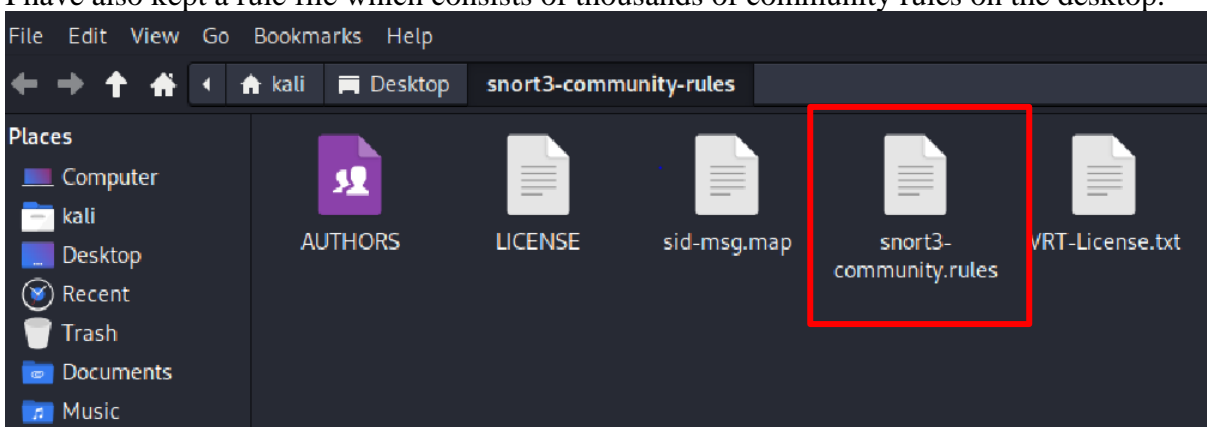
3. NIDS (Snort)

Snort is installed in the kali system: and can be run using the command: `“sudo snort -q -l /var/log/snort -i eth0 -A console -c /etc/snort/snort.conf”` this command will actively monitor the network and display alerts based on the alerts written in the local.rules file. (Talos Detectio Team, n.d.) (Roesch and Cisco, 2013)

Upon running the command you can see that the snort is actively providing alerts on the network traffic:

```
(root@kali)-[~kali]
└─# sudo snort -q -l /var/log/snort -i eth0 -A console -c /etc/snort/snort.conf
08/14-14:22:57.775038  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.8.45 → 192.168.8.32
08/14-14:22:57.775038  [**] [1:100001:1] Alert: ** ICMP Ping was detected ** [**] [Priority: 0] {ICMP} 192.168.8.45 → 192.168.8.32
08/14-14:22:57.775038  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.8.45 → 192.168.8.32
08/14-14:22:57.775073  [**] [1:100001:1] Alert: ** ICMP Ping was detected ** [**] [Priority: 0] {ICMP} 192.168.8.32 → 192.168.8.45
08/14-14:22:57.775073  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.8.32 → 192.168.8.45
08/14-14:22:58.786195  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.8.45 → 192.168.8.32
```

You can also change the local.rules file in the “/etc/snort/rules/local.rules”.
I have also kept a rule file which consists of thousands of community rules on the desktop.



4. HIDS (OSSEC) -

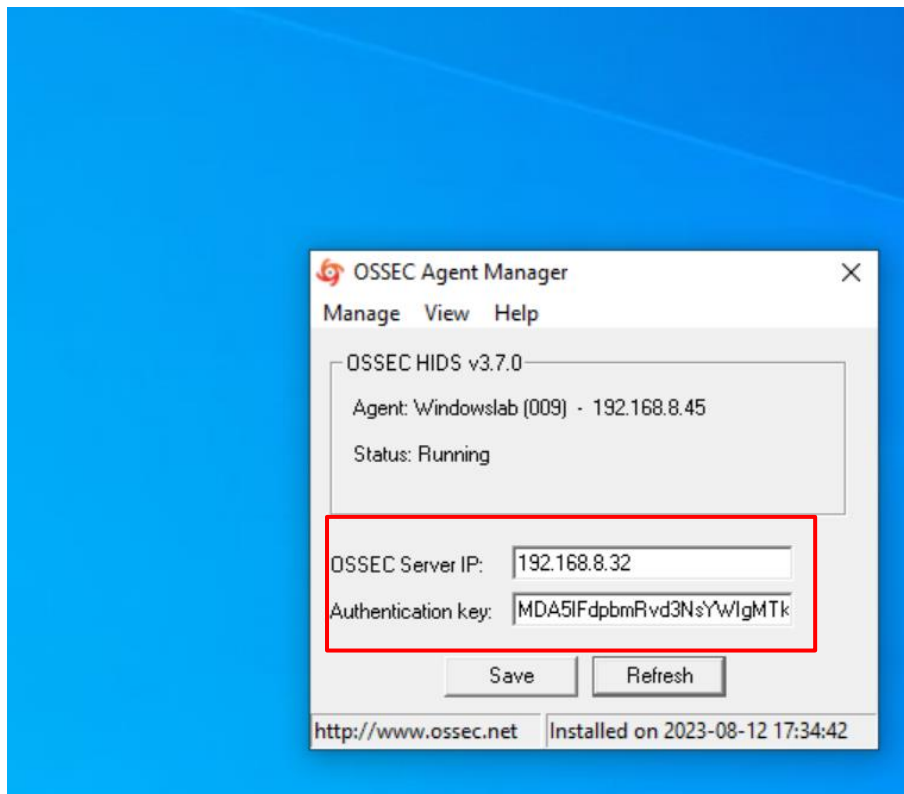
```
root@kali: /var/ossec/bin
File Actions Edit View Help
~/var/ossec-4.3.2/rules

└─# sudo /var/ossec/bin/agent_control -lc

OSSEC HIDS agent_control. List of available agents:
  ID: 000, Name: kali (server), IP: 127.0.0.1, Active/Local
  ID: 009, Name: Windowslab, IP: 192.168.8.45, Active

(root@kali)-[~/var/ossec/bin]
└─#
```

OSSEC service is installed on kali and it is actively monitoring the Windows 10 VM using the agent that is installed on the Windows machine. We can see the Windows 10 IP as 192.168.8.45. (www.ossec.net, n.d.)



Above is the OSSEC Agent installed on the Windows machine and sending Windows Event Logs and File Integrity checks to Linux server that has the IP 192.168.8.32. Here is the OSSEC configuration file which includes the configuration to scan windows event logs and file integrity checks.

```
ossec - Notepad
File Edit Format View Help
-->

<ossec_config>

<!-- One entry for each file/Event log to monitor. -->
<localfile>
  <location>Application</location>
  <log_format>eventlog</log_format>
</localfile>

<localfile>
  <location>Security</location>
  <log_format>eventlog</log_format>
</localfile>

<localfile>
  <location>System</location>
  <log_format>eventlog</log_format>
</localfile>

<localfile>
  <location>Windows PowerShell</location>
  <log_format>eventlog</log_format>
</localfile>
```

Above code scans for Windows Event Logs

```

<!-- Syscheck - Integrity Checking config. -->
<syscheck>

<!-- Default frequency, every 20 hours. It doesn't need to be higher
- on most systems and one a day should be enough.
-->
<frequency>3600</frequency>

<!-- By default it is disabled. In the Install you must choose
- to enable it.
-->
<disabled>no</disabled>

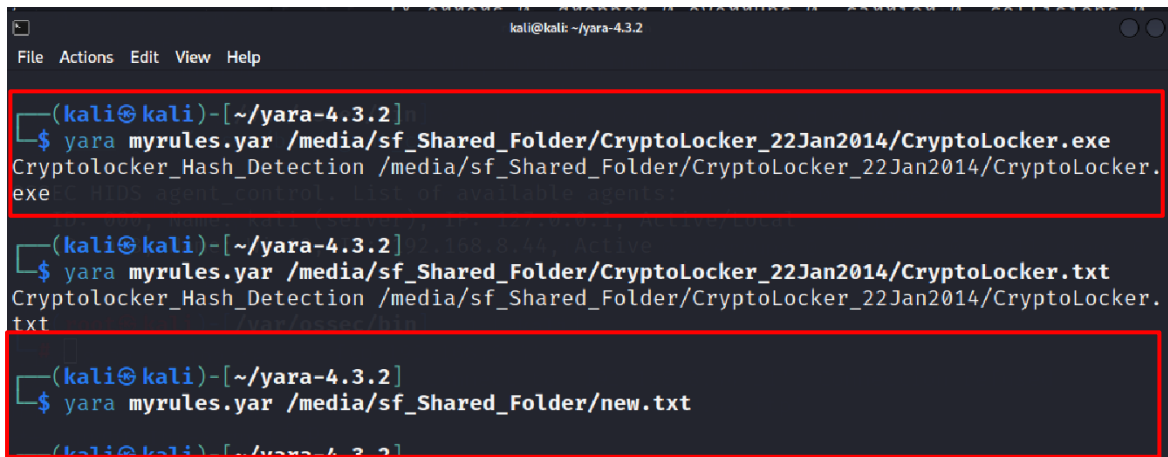
<!-- Default files to be monitored - system32 only. -->
<directories check_all="yes">%WINDIR%/win.ini</directories>
<directories check_all="yes">%WINDIR%/system.ini</directories>
<directories check_all="yes">C:\autoexec.bat</directories>
<directories check_all="yes">C:\config.sys</directories>
<directories check_all="yes">C:\boot.ini</directories>

```

Above code is for the File integrity check at every 1 hour frequency.

5. YARA:

Yara can be run using the command : **yara myrules.yar (/location of the file)**



```

kali@kali:~/yara-4.3.2
File Actions Edit View Help

(kali@kali)~/yara-4.3.2
$ yara myrules.yar /media/sf_Shared_Folder/CryptoLocker_22Jan2014/CryptoLocker.exe
Cryptolocker_Hash_Detection /media/sf_Shared_Folder/CryptoLocker_22Jan2014/CryptoLocker.exe

(kali@kali)~/yara-4.3.2
$ yara myrules.yar /media/sf_Shared_Folder/CryptoLocker_22Jan2014/CryptoLocker.txt
Cryptolocker_Hash_Detection /media/sf_Shared_Folder/CryptoLocker_22Jan2014/CryptoLocker.txt

(kali@kali)~/yara-4.3.2
$ yara myrules.yar /media/sf_Shared_Folder/new.txt

```

Above is the example of yara scanning for CryptoLocker malware hash. The file CryptoLocker.exe and CryptoLocker.txt contain hash values of CryptoLocker, thus it is detecting the hash based on the set rules. (Si et al., 2022)

As the file new.txt does not contain hash signatures, yara gives no response upon scanning.

6. Squid:

Squid is configured to facilitate gateway and Proxy services as well as malicious URL Blocking. (Adams, 2021)

Below is the configuration of Squid inside the location “/etc/squid/squid.conf”

```
squid.conf [Read-Only]
/etc/squid

1 # WELCOME TO SQUID 5.7
2
3
4 #
5 acl bad_urls dstdomain "/etc/squid/blocked.acl"
6 http_access deny bad_urls
7
8
9 http_port 3128
10
11 acl localnet src 192.168.8.0/24 # RFC1918 possible internal network
12 http_access allow localnet
13 http_access allow localhost
14
15 # And finally deny all other access to this proxy
16 http_access deny all
17
18 # Squid normally listens to port 3128
19 visible_hostname myproxy
20
```

The Configuration file denotes, squid is running on the network 192.168.8.0/24 and is using the file “/etc/squid/blocked.acl” which contains a list of malicious URL which will be blocked for HTTP access.

Below is an example:



The following error was encountered while trying to retrieve the URL: <http://zenpat.com/>

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel t incorrect.

Your cache administrator is [webmaster](#).

References:

Strand, J. (2022). *IntroLabs*. [online] GitHub. Available at: https://github.com/strandjs/IntroLabs/blob/master/IntroClassFiles/Tools/IntroClass/md/elk_in_the_cloud.md.

Talos Detectio Team, C. (n.d.). *Snort 3 Rule Writing Guide - Snort 3 Rule Writing Guide*. [online] docs.snort.org. Available at: <https://docs.snort.org/>.

www.ossec.net. (n.d.). *Centralized agent configuration — OSSEC*. [online] Available at: <https://www.ossec.net/docs/docs/manual/agent/agent-configuration.html>.

Roesch, M. and Cisco (2013). *SNORT Users Manual 2.9.15*. [online] Amazonaws.com. Available at: <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/>.

Si, Q., Xu, H., Tong, Y., Zhou, Y., Liang, J., Cui, L. and Hao, Z. (2022). Malware Detection Using Automated Generation of Yara Rules on Dynamic Features. *Science of Cyber Security*, pp.315–330. doi:https://doi.org/10.1007/978-3-031-17551-0_21.

Adams, D. (2021). *Squid proxy configuration on Linux*. [online] <https://linuxhint.com/>. Available at: <https://linuxhint.com/squid-proxy-configuration-linux/> [Accessed 14 Aug. 2023].