Cuckoo Sandbox Hands-on Activity Report

Gursimran Singh LNU
Computer and Information Science
Rochester Institute of Technology
Rochester, New York, USA
gl2840 at rit.edu

I. Introduction

Cuckoo Sandbox is an open-source automated malware analysis system designed to analyze malware in a safe virtual environment. It detects and analyzes malware that can evade traditional security measures, providing detailed reports on its behavior, including network traffic, file system activity, and system changes. Its analysis process involves submitting a sample, creating a virtual machine, executing malware, analyzing its behavior, and generating a report. Cuckoo Sandbox is useful in various scenarios such as incident response, threat hunting, malware research, vulnerability testing, and education and training. The expected outcome of using Cuckoo Sandbox is to improve an organization's ability to detect, analyze, and defend against malware threats, which can help make informed security strategies and help them stay ahead of evolving threats.

II. Web Interface

A Django application serving as the full-featured web interface is offered by Cuckoo. You can upload files, examine the reports, and do a search across all the analysis results using this interface. The reporting.conf must have MongoDB installed and enabled. We can access the web interface by launching the built-in development server(used here) or by setting up an uWSGI + NGINX configuration for a production environment.

In order to set up the web interface, first, we need to go follow the steps given in Fig. 1, in which we are modifying reporting.conf file, restarting the Cuckoo Sandbox and starting the web interface on any non-occupied port of choice (by default 8000). After we are able to load the web interface, we need to follow the steps in Fig. 2 to select a file for analysis through the web interface, select some options like network routing, memory dump,etc, run the analysis and get the analysis result.

The last image in Fig. 2 shows the output of the file analysed using the web interface. It shows a summary of the file analysed and it's malicious score, which is 6.4/10. It also has a left-sidebar, which has detailed analysis results for different categories like network analysis, behavior analysis, memory analysis and so on. This web interface is makes look through the analysis results much easier.

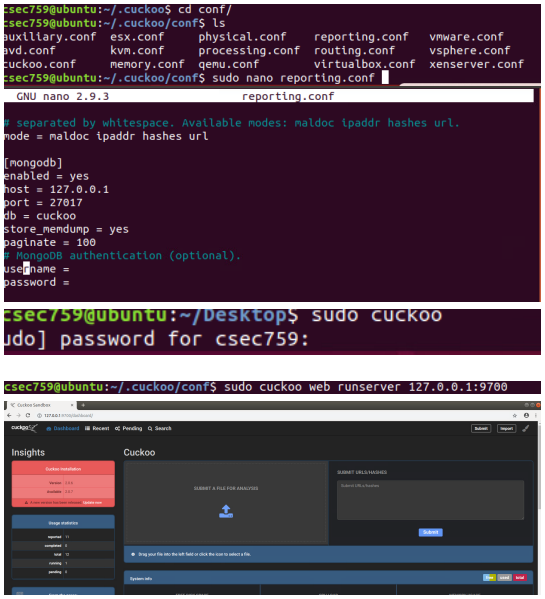

Fig. 1. Setting up the web interface

III. Inetsim

Inetsim is a tool that can be used in conjunction with Cuckoo Sandbox, a popular open-source malware analysis platform. Inetsim is designed to simulate various network services and protocols, which allows analysts to better understand how a particular malware sample behaves in a networked environment.

When used with Cuckoo, Inetsim can be used to create a sandboxed environment where a malware sample can be executed and its behavior observed. The simulated network services provided by Inetsim can then be used to monitor the malware's network activity and help identify any communication with a command-and-control server or other malicious activity.

Overall, Inetsim can enhance the capabilities of Cuckoo Sandbox by providing a more complete understanding of how a malware sample behaves in a networked environment, which can aid in malware analysis and help identify potential threats.

In Fig. 3, we are setting up Inetsim for analysis. First, we make sure that Inetsim is running on a terminal window, also, note down the port it is listening on. Next, we enable Inetsim in routing.conf file and also modify the server IP to the one

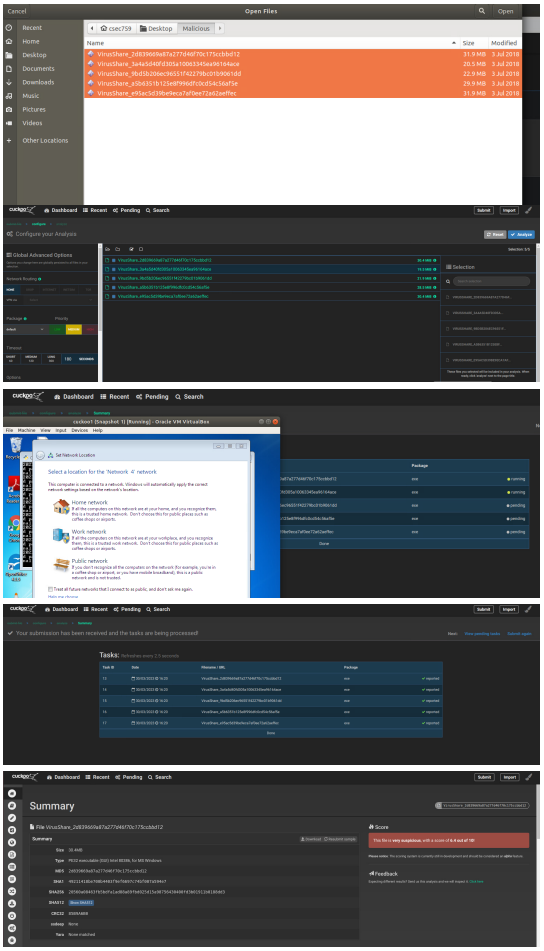

Fig. 2. Analysis using web interface

given in the terminal window of running Inetsum instance. Next, we follow the similar pattern as in the last section to start a web interface and select a file to analyse. After that, we need to select the network routing as Inetsim as highlighted in second last image in Fig. 3 and then run the analyses.

Finally, we get the output of the analysis (last image of Fig. 3) where we can see that the file tried to connect to some servers, however, since we were using Inetsim instead of the real internet, we tracked it's activity without the risk of contacting a malicious c&c server.

IV. Suricata

Suricata is an open source intrusion detection and prevention system that can be used to detect and prevent a wide range of security threats. Cuckoo is an automated malware analysis system that can be used to analyze and detect malware.

Cuckoo can be integrated with Suricata to improve its malware detection capabilities. When a file is submitted to Cuckoo for analysis, Suricata can be used to inspect the network traffic generated by the file. Suricata can detect and alert on any malicious network activity that is associated with the file.

Once Suricata is integrated with Cuckoo, any malicious network activity associated with a file will be detected and alerted on by Suricata during the analysis process. This can help improve the accuracy of malware detection and provide additional context for analyzing malware.

In order to set up Suricata, we first need to download the respective package for our machine, i.e., Ubuntu, by following the instruction from official Suricata Documentation. Next, we update Suricata to get the default available free rules (which can be changed), and then we create a Suricata group and change its ownership so that cuckoo sandbox can access it without needing root permissions. The processing.conf should also be modified to enable Suricata in processing phase.

After running the analysis, Suricata Alerts can be access under Network Analysis tab. The last image of Fig. 4 shows the Suricata TLS but there are no alerts for this file. However, it is more likely to detect some malicious traffic when checking a file on a machine with internet access.

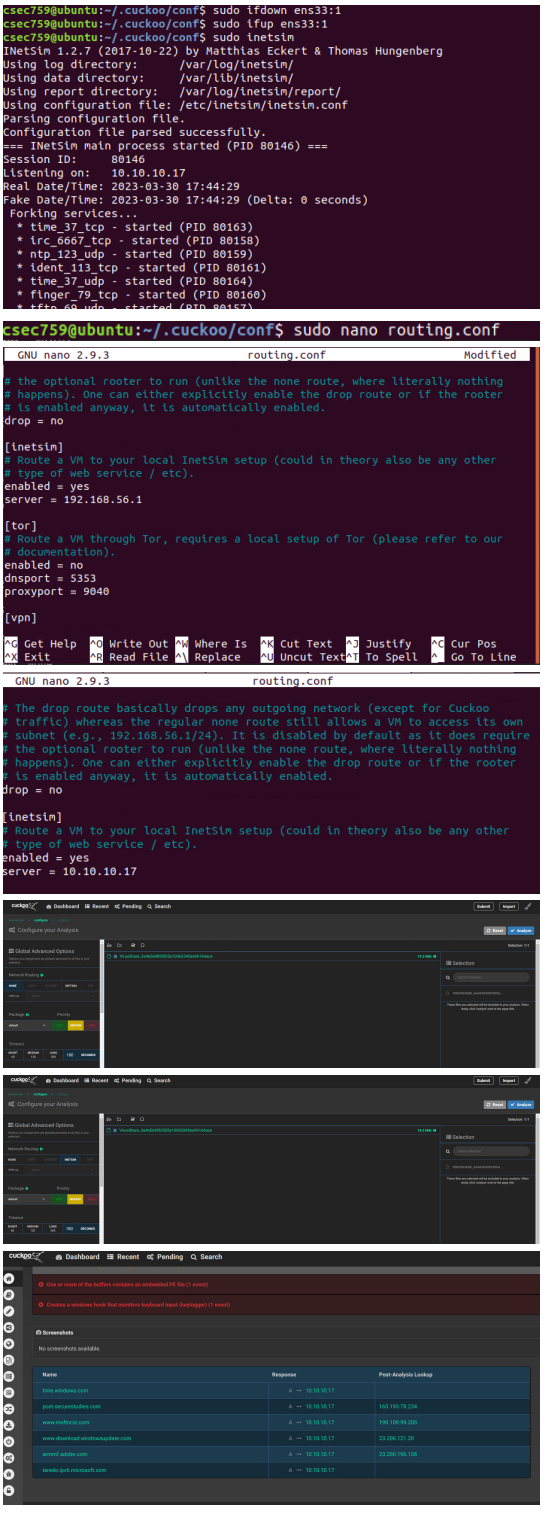

Fig. 3. Analysis using Inetsim

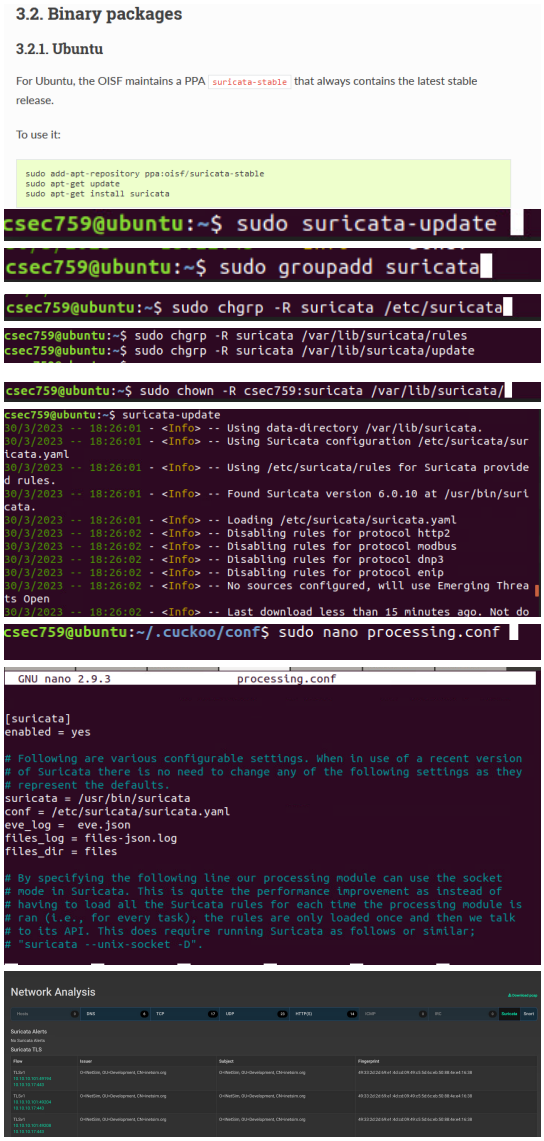

Fig. 4. Setting up Suricata

Malware File	Malicious Score	Interesting Behavioral Signature
1	7.2/10	Resumed a suspended thread in a remote process
2	1.4/10	Queries the disk size, to detect a virtual machine
3	6.0/10	Deletes a large number of files from the system
4	13.4/10	Attempts to detect Cuckoo Sandbox through a file's presence
5	4.8/10	A Process created a hidden window

Fig. 5. Most Interesting Behavior of each Malicious File and their Malicious Score

V. Conclusion

During this study, I found some very interesting and useful functionalities that can be used with Cuckoo Sandbox, that can help make analysis much more easier (web interface), safe (using Inetsim) and robust (Suricata). I also looked into all 5 given malicious files and Fig. 5 shows each of their malicious score and most interesting behavioral signature. Overall, I think Cuckoo Sandbox is a very interesting and useful tool for automating malware analysis, and there are lot of additional

functionalities that can be added to it to make it much stronger tool for malware analysis. In the future, I will explore more additional tools and functionalities with Cuckoo Sandbox like Snort, Volatality, etc.

REFERENCES

[1] "Documentation," Suricata, 02-Jun-2021. [Online]. Available: https://suricata.io/documentation/. [Accessed: 30-Mar-2023].