Cyber security

Name of student

Name of professor

University

Course

Date

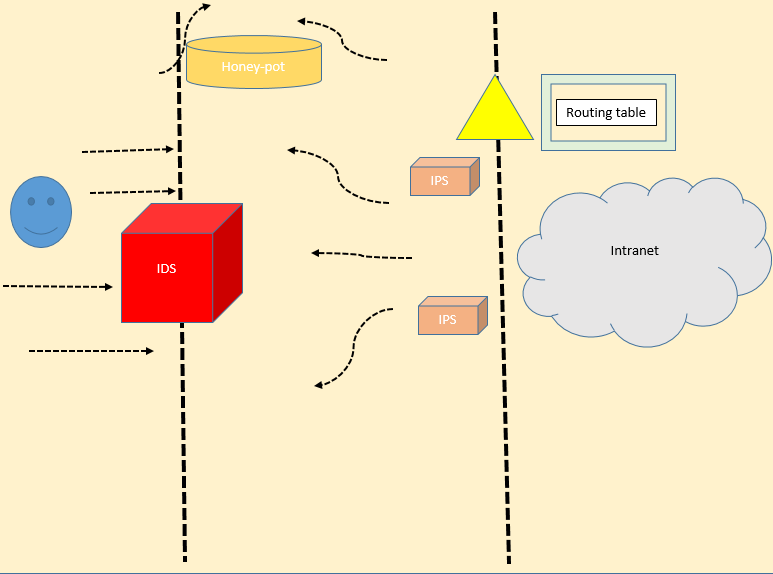
Information security and cyber security are terms that are used interchangeably. The success of any information system relies on its ability to secure the information components that it so keeps and upholds. There are a number of tools, both open source and private that have been developed and deployed over the years to help protect the various information systems that organizations uphold and keep.

Securing the information systems is an activity that includes the following resource environments:

1. The organizational network
2. The organizational databases
3. The organizational systems and applications
4. The organizational hardware material and peripherals
5. The organizational physical security mechanisms
6. The users policies and procedures

The attack on the above resources and infrastructural materials have been on the rise with the development of cyber warfare tools and materials. They include Trojan horses, malwares, ransom wares, worms, viruses. Other techniques include cross site scripting, sol injection attacks and man in the middle attacks.

However, as a technique to curb and protect information systems within an enterprise, organizations are now implementation tools and properties that can help to protect the network. Observe the architecture below:



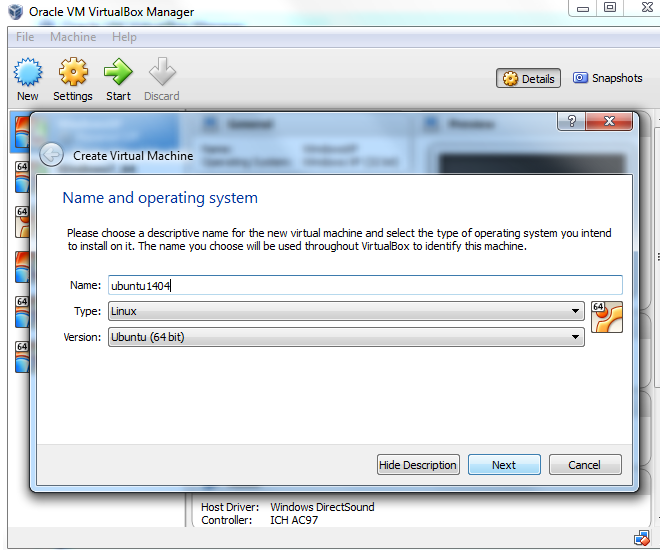
The illustration from the above architecture indicates the way traffic is flowing in a typical organization network. The intrusion detection system (IDS) located at the open end of the organization is supposed to flag out any suspicious or malicious traffic activity approach their normal network.

Once this suspicious it has been flagged, the IPS can prevent them by either directing them to the honey pot where they can wait “arrest” or bounce them back to the outside. The routing memory tables contains the list of all the allowed IPs within the network, as well as the list of all allowed IPS. What the router does whenever there is an oncoming or outgoing traffic is to register its IP in the memory and later use this to either allow or block the incoming traffic. Some kind of intelligent learning.

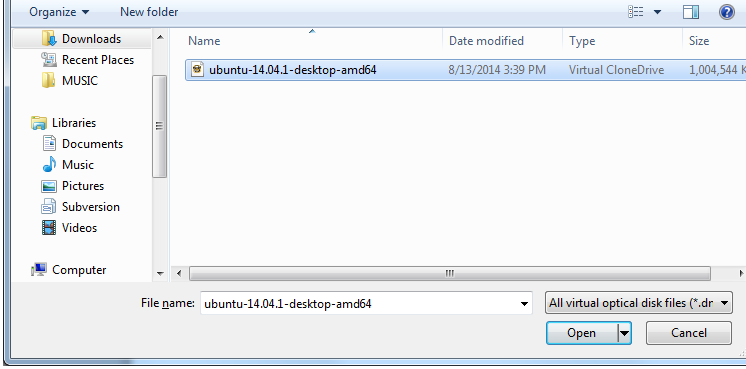
In this exercise, the below processes are followed in the installation of the Sucricata software on Ubuntu virtual box machine, with Kali Linux tools. The first step is to install Virtual box:



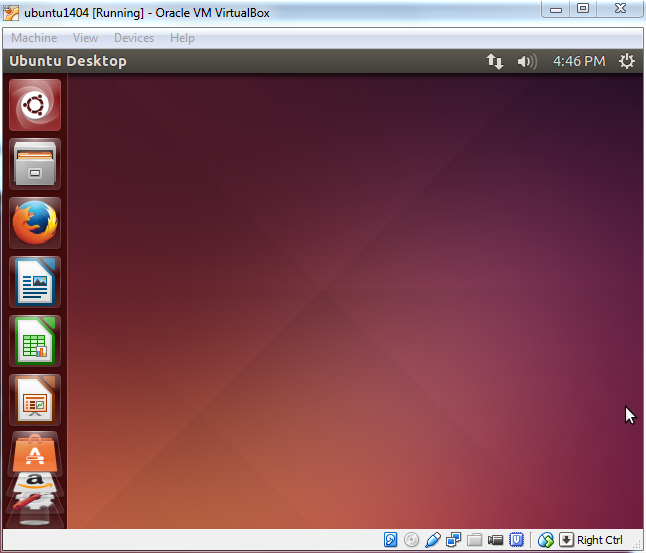
Then install Ubuntu as an ISO image

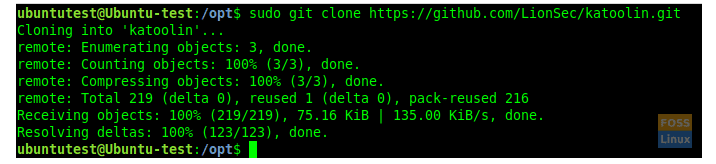


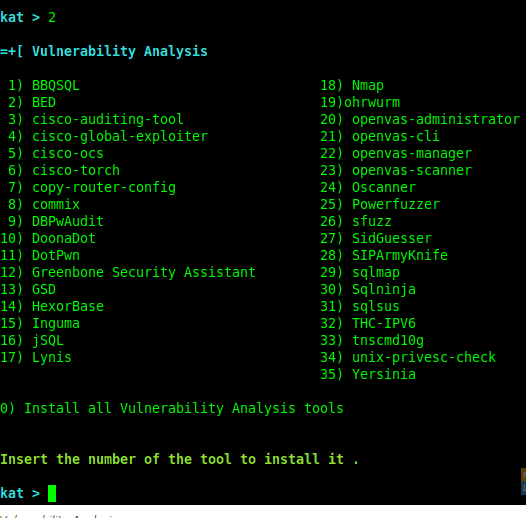
Then load the ISO image



After Ubuntu installation



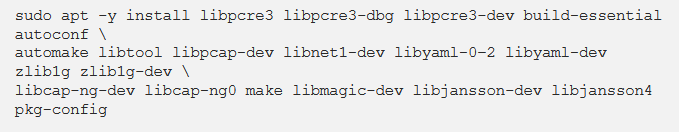




Then install Suricata



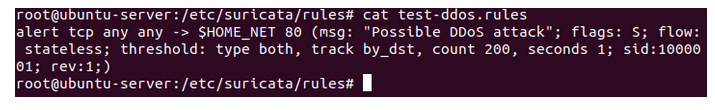
Then install all the dependencies needed for Suricata to detect the network or anomalies within the network. Below command installs the necessary packages needed by the Suricata application.



Next we install all the required tools required for the Suricata to function;



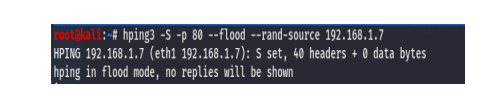
Once Suricata is installed, we use a new file to detect any possible DDoS on the network as below. In this case, my local IP address is 192.168.1.7 in the HOM\_NET directory. Then we pass rules to tit as below:



Then run Suricata in live mode from another PC and initiate attack from another host say Kali Linux as below:



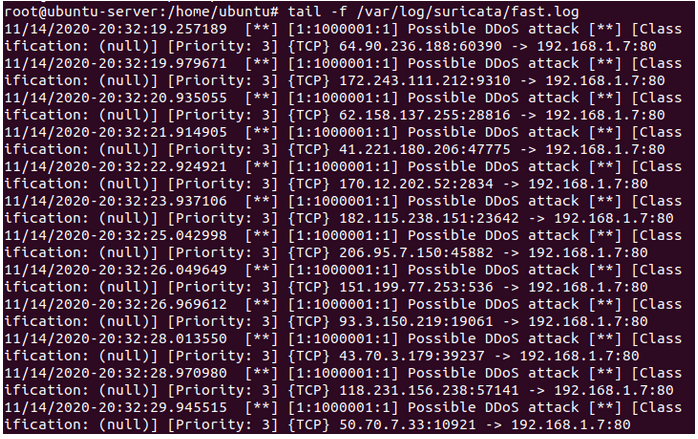
Then performing the attack from Kali Linux;



Once attack is finished, we can go to the Suricata host and check the var log directory for the attack logs using the below command;



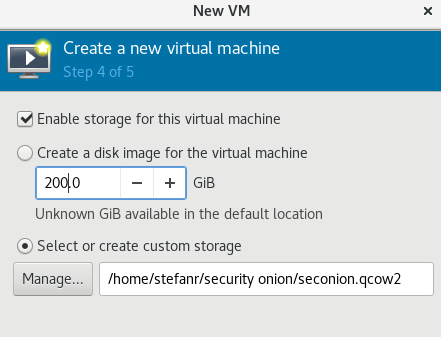
As we can see from the log file that a possible DoS was initiated and Suricata tried to capture it as below:



The above results is shown by the suricata on the potential IP addresses that were scanned during the network vulnerability reporting. One of the signified discoveries from this activation was the trend that certain potential threats seemed to have becoming from the some or slightly altered source port. A criminal dictate could easily have access to the system, capture the main packets and use them for their own bet

**Security opinion installation**

The next step is to install the security onion that comes with the pap installation already added as module. Within virtual box we have to create the new VM which in this case is the Security onion



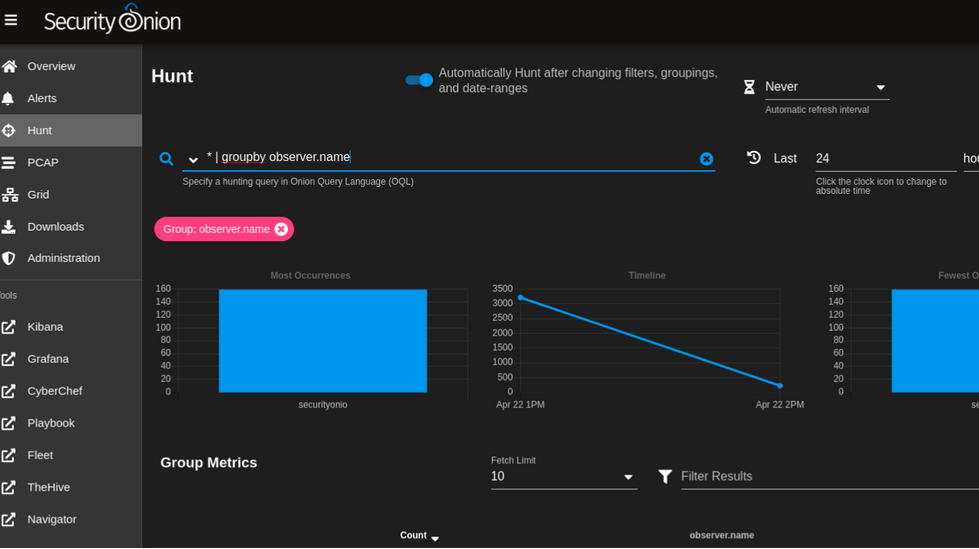
Once the installation is complete it looks as below



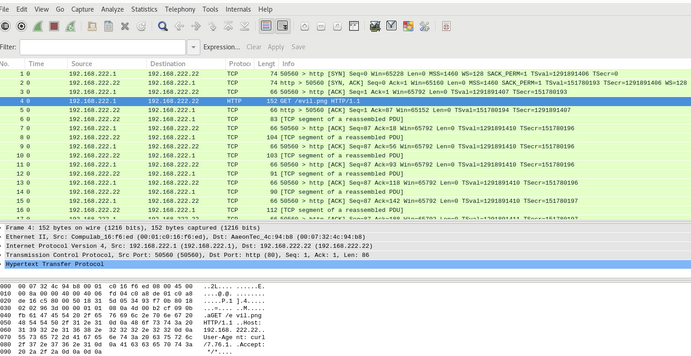
In the next step we configure the networks by whitelisting certain it addresses that are closely related to the local machine



In the next step we try to capture data packets using wire show sharks and the illustration of the security onion dashboard.



Then we use wireshark to capture the various streams of data that are coming to the network



As a prevention policy for avoiding further, future attacks, policies can be reviewed to promote the care handling of information by staff. Also, firewalls and routers can be configured to only accept allowed IP addresses.

Prevention policies are significant in ensuring that the way and method of handling organization security matters and issues. Even if internal staff are trained on this, there is still need to uphold the security procedures and controls in place.

References

Smaha, Stephen E. "Haystack: An intrusion detection system." *Fourth Aerospace Computer Security Applications Conference*. Vol. 44. 1988.

Liao, Hung-Jen, et al. "Intrusion detection system: A comprehensive review." *Journal of Network and Computer Applications* 36.1 (2013): 16-24.

Zhang, Xinyou, Chengzhong Li, and Wenbin Zheng. "Intrusion prevention system design." *The Fourth International Conference onComputer and Information Technology, 2004. CIT'04.*. IEEE, 2004.

de Sousa Araújo, Tiago Emílio, Fernando Menezes Matos, and Josilene Aires Moreira. "Intrusion detection systems' performance for distributed denial-of-service attack." 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON). IEEE, 2017.