**The Importance of CyberSecurity Services & Tools In the Security Industry**

Tianna Green

The Knowledge House

Cybersecurity 2022 Cohort

December 8th,2022

Cybersecurity components that were a part of the security lab were: ubuntu servers, pfsense, snort, Kali Linux and Metasploitable2. All of these tools/services play vital roles in the security industry. Ubuntu Server is a very popular operating system that can be used to serve websites, share files, push containers to their target environments, run Aws and other cloud services and it can also be used as an email server. Ubuntu/ Ubuntu server are important in the security industry because it "gives users the freedom of linux and a way to consume or use open source software with no toll on configuration,maintenance, security and so on.” (Kim,2022) This is an important ability to have in the security industry because a lot of security professionals need a space to do their work that is secure, and that is easy to navigate which Ubuntu servers are.

Pfsense is a free software that in this lab was used as a stateful firewall; a stateful firewall monitors the full state of the traffic within a network. In this lab we had to use pfsense to install and configure a firewall that we could access via the web and also install on our devices. Many people choose to use pfSense software because it is “Flexible, Open Source, user friendly, powerful and well-supported” (Sunny Valley Networks) It is flexible because it allows you to add extra features and can function as a basic firewall and also a complete security system. As an open source pfSense is free to use and the public can alter any of the code available. It is user friendly meaning that it is easy to manage unlike other firewall software. The strength of your firewall can be very powerful if you follow the rules that you set for it and the feature of the software makes it easy to ensure that your firewall adheres to the rules. Lastly, it is a well supported software meaning any questions you need answers to will be easy to find therefore making it easy to troubleshoot any problems. PfSense is an important tool because firewalls protect your network from unauthorized access to private data and they also secure computers from malicious software. Using a tool like pfSense allows companies to control their system’s entry points and stop virus attacks.

Snort is an open source intrusion detection system that can be configured in real time to monitor network traffic. An intrusion detection system detects suspicious activities and produces alerts when they are detected which then can be investigated so the appropriate next steps can be taken to ensure that the threat is contained. While running a snort rule there are five default rule actions that are used which tell snort what to do when it finds a packet that matches the rule criteria. The five default actions are: “Alert. Dynamic, Pass, Log, or/and Activate” (Cyvatar,2022) Alert is when an alert is generated using the selected alert method and then logs the packet (small segment of a larger message). Dynamic is when snort remains idle until activated by an activate rule and then it acts as a log rule. Pass is when snort ignores the packet. The default action, log, is when the packet gets logged. Finally, activate is when snorts alerts and turns on another dynamic rule. More rules types can be defined by the user and they can then be used as actions similar to the ones above. Snort is an important tool in the security industry because it is constantly watching and inspecting the traffic on a network to ensure all suspicious activity is caught and analyzed so that it does not become a threat.

Kali Linux in the project is used as our attack machine. Kali is an open source Linux tool that is utilized by both hackers and security administrators. Hackers use kali to identify and exploit weaknesses in security systems while security admins use kali to protect and detect any weaknesses in security systems that could potentially be used to infiltrate the parameters of the systems. Hackers like kali so much because “it does not leave any evidence of footprints after the user is used that would cause an information breach” (geeksforgeeks, 2022) which is ideal because it makes it hard for them to get caught or for someone to hack into their systems. Kali Linux is important in the security industry because it is very transparent which allows professionals to easily learn how to manipulate it to learn how to defend security systems against attacks that hackers could use the same operating systems to learn how to execute.

Metasploitable2 is used in the lab as the target machine. Metasploitable2 is defined as “an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities” (rapid7) It is an important tool in the security industry because it allows professionals to test their skills and tools in a controlled environment. In this lab Kali Linux, the attack machine will be used to simulate an attack on Metasplootable which will give us a realistic view of how hackers probe vulnerabilities on networks and servers.

All of these tools/services were utilized to create a security lab in a virtual environment of my choosing. This project taught me how to configure these tools and simulate an attack on a target machine as well as try to protect it from the attack.

**References**

Cyvatar. (2022, February 3). *Writing snort rules with examples and cheat sheet*. CYVATAR.AI. Retrieved December 11, 2022, from https://cyvatar.ai/write-configure-snort-rules/

*Metasploitable 2*. Metasploitable 2 | Metasploit Documentation. (n.d.). Retrieved December 13, 2022, from https://docs.rapid7.com/metasploit/metasploitable-2/#:~:text=The%20easiest%20way%20to%20get,and%20other%20common%20virtualization%20platforms.

Roesch, M. (2022). Writing Snort Rules. Retrieved December 11, 2022, from https://paginas.fe.up.pt/~mgi98020/pgr/writing\_snort\_rules.htm#:~:text=Rule%20Actions%3A&text=There%20are%20five%20available%20default,pass%2C%20activate%2C%20and%20dynamic.&text=You%20can%20also%20define%20your,more%20output%20plugins%20with%20them.

*What is pfSense® Software?* Sunny Valley Networks. (n.d.). Retrieved December 11, 2022, from https://www.sunnyvalley.io/docs/network-security-tutorials/pfsense

*Why hackers use Kali linux?* GeeksforGeeks. (2022, May 29). Retrieved December 11, 2022, from https://www.geeksforgeeks.org/why-hackers-use-kali-linux/