My Very First Cyber Security Lab: a Discussion on the Concepts, Components & Software Involved in the Development of a Virtual Cyber Security Lab

Jane Pierre

The Knowledge House

Cyber Security & Networking: End-of-Phase 1 Project

Instructor George Robbins

December 14, 2022

There comes a time in a cyber security student's life where they have to bring together their knowledge and experience, shirk off the chains of fear, the occasional bouts of imposter syndrome, and create their first cyber security lab environment. To put their learning to the test, suffer and endure the downloading and installation process, and create a network in which various simulations can be tested and cyber security solutions developed. The purpose of this paper is to explain the various components and software involved in the development of a cyber security lab. It also serves as a written accompaniment to this lab, explaining the screenshots UTM hypervisor displaying the virtual machines (VMs) used titled, tkh_if_cse_p1_end_project_utm_vm_setup(pierre_jane) and the topology of the lab titled, (tkh_if_cse_p1_end_project_topology(pierre_jane) and the video demonstrating the server (server@workstation.cluster.local) ssh-ing into workstations node1 (node1@node1.cluster.local) and node2 (node2@node2.cluster.local) titled, tkh_if_cse_p1_end_project_video_server_ssh_nodes_(pierre_jane). This paper will discuss the following concepts, components and tools that were used in the accompanying cyber security lab: virtual machines (VMs), security information and event management (SIEM), intrusion detection system (IDS), intrusion prevention system (IPS), firewall, server, workstations, Ubuntu, Kali Linux, Security Onion, Metasploitable, Suricata, Snort, and PfSense.

A cyber security lab is a small-scale environment designed to simulate different types of virtual environments in order to evaluate the use of a network in a specific instance (Justabouttechie, 2022). Cyber security labs are usually run through a virtualized box

called virtualization (Justabouttechie, 2022). Additionally, virtualization can be done through the local host or cloud-based. The lab set up being discussed, was done through a local host.

There are several reasons for a student or cyber security professional to use this method to hone their skills. Cyber security labs provide a legal way to practice hacking, intrusion and intrusion prevention, detection and remediation (Jigsaw Academy, 2022). In some instances, during testing, some techniques could cause damage leading to the breaking of the hardware (Jigsaw Academy, 2022). Additionally, during testing, if the researcher is using tools that involve malware, it could spread to other internet connected environments (Jigsaw Academy, 2022). The creation of “dummy” versions of software or operating systems that won’t affect host machines is essential to developers and security specialists to test software and isolate infected files within a safe, quarantined environment, without the threat of malware or bugs impacting other parts of their system or network (Ghimiray, 2022). With cyber security labs, the researcher can maintain an isolated development environment. Virtualization is a time tested way to ensure that cyber security students and professionals are up to date, familiar with cyber safety tools, proficient with industry software and knowledgeable about the threats facing them (Jigsaw Academy, 2022).

Understanding the role of virtualization in a cyber security lab requires knowing how to create and use virtual machines. A virtual machine is a program that allows the user to build and use a computer without the need for physical hardware like motherboards,

monitors and mice. A virtual machine runs entirely on software and in essence is a simulated computer inside a real computer (Ghimiray, 2022). Virtual machines function like normal computers and contain operating systems (OS), store files, run programs, and even have virtual hardware components (Ghimiray, 2022). However, with VMs being entirely software-based, they need to “borrow” hardware resources from a physical host computer (Ghimiray, 2022). For example, in a virtual machine, the physical host’s network adapter is used to model a virtual network adapter card (Ghimiray, 2022). One host computer can run multiple VMs simultaneously, with all the completely independent operating systems and functionality (Ghimiray, 2022). Additionally, a single host could run VMs with different operating systems in a simulated virtual environment. A MacOS based computer can host a Linux virtual machine, WindowsOS based VM, fully functioning within the VM as the operating system. A Windows based computer can host a MacOS or Linux virtual machine with it fully functioning as the different operating system. Virtual machines help companies save money and optimize performance – specifically when it comes to providing server security and cloud software solutions (Ghimiray, 2022).

In the cyber security lab, the virtual machines were hosted by a physical laptop, a MacBook Air 2020 featuring the M1 chip running Ventura MacOS with a software called UTM acting as the hypervisor. On UTM there were nine virtual machines in use, eight of them utilizing the Ubuntu 22.04 Linux OS and one of them using Kali Linux as its OS. Three of them were used to host programs for SIEM through the program Spring Onion (spring_onionbuntu), IPS through Snort (snortbuntu) and IDS through Suricata

(suricatabuntu). One Ubuntu Linux OS VM was used to host the firewall running the program pfSense (firewall), and another was used as the target machine running the program Metasploitable, while a different VM using Kali Linux OS served as the attack machine (kali_linux attack_machine). Finally the last three Ubuntu VMs were used as a server (workstation.cluster.local) and two workstations (node1.local.cluster and node2.local.cluster) respectively. The topography showing the configuration of this cyber security lab was made using Cisco Packet Tracer.

Once a researcher has their virtual machines configured, a SIEM is needed. SIEM is short for security information and event management (IBM, 2022). SIEM is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure (Buckbee, 2022). SIEM offers a real-time monitoring and analysis of events in addition to tracking and logging security data for compliance and auditing purposes (IBM, 2022). Utilizing user behavior anomalies and artificial intelligence (AI), SIEM automates many of the manual processes associated with threat detection and incident response (IBM, 2022). It is an essential aspect of modern-day security operation centers (SOCs), security and compliance management use cases and learning and research through cyber security lab simulations (IBM, 2022). The SIEM process is as follows: data is collected from various sources (network devices, servers, domain controllers, etc) (Buckbee, 2022). Then the collected data is normalized, aggregated and analyzed to discover and detect threats (Buckbee, 2022). Security breaches are pinpointed allowing organizations to investigate alerts (Buckbee, 2022). For students and cyber security professionals, SIEM allows real-time reporting

and forensics about security incidents and alerts based on analytics that match a certain rule set, indicating a security issue (Buckbee, 2022). SIEM software helps organizations detect and build a defense much faster than regular security specialists can (Katz Cybersecurity Blog, 2022). Through a multi-layered approach, SIEM tools increase the chances of detecting a ransomware infection before it deploys, which gives cyber security professionals more time to identify to stop, remove, and repair any threat that emerges (Katz Cybersecurity Blog, 2022).

An Ubuntu 22.04 Linux OS virtual machine running Security Onion served as the SIEM software for this cyber security lab. Security Onion is an open-source, free Linux distribution for log management, enterprise security monitoring and intrusion detection. Security Onion utilizes many tools including: NetworkMiner, CyberChef, Squert, Sguil, Wazuh, Bro, Suricata, Snort, Kibana, Logstash, Elasticsearch and more (Jigsaw Academy, 2022). At its core Security Onion is a Kibana (ELK), Logstash and Elasticsearch stack, including the Wazuh end of the open-sourced host-based intrusion detection system, with both Suricata and Snort rule-based network intrusion detection system, as well as Zeek providing analysis on network traffic (Jigsaw Academy, 2022).

In addition to virtual machines and SIEM, an intrusion detection system (IDS) is another essential part of the cyber security lab. IDS is a network security technology originally built for detecting vulnerability exploits against a target application or computer (Palo Alto Networks, 2020). IPS extended intrusion detection system (IDS) solutions by adding the ability to block threats in addition to detecting them and has become the

dominant deployment option for IDS/IPS technologies (Palo Alto Networks, 2020). TAP or SPAN ports are often used by IDS solutions to analyze a copy of the inline traffic stream (Palo Alto Networks, 2020). An IDS is also a listen-only device (Palo Alto Networks, 2020). An IDS monitors traffic and reports its results to an administrator, but they cannot automatically take action to prevent a detected exploit from taking over the system (Palo Alto Networks, 2020).

An Ubuntu 22.04 Linux OS virtual machine running Suricata served as the IDS software for this cyber security lab. Suricata is an open-source detection engine that can act as an intrusion detection system (IDS) and an intrusion prevention system (IPS) (Viglione, 2022). Developed by the Open Information Security Foundation (OSIF), it is a free tool using a rule set and signature language to detect and prevent threats (Viglione, 2022). Suricata can do both intrusion detection and alert to threats and also take action on the event and attempts to block the traffic (Viglione, 2022). Suricata is multi-threaded meaning that the tool can use multiple cores at once, allowing for greater load balancing (Viglione, 2022). This allows the user to process more data without dialing back on the number of rules that need to be implemented (Viglione, 2022).

An intrusion prevention system (IPS) is another critical part of a virtual cyber security lab. An IPS is networking security software or hardware that continuously monitors networks for malicious activity and takes action to prevent it, in the form of reporting, blocking or dropping it when the activity occurs (VMWare, 2022). Unlike an IDS, intrusion prevention systems can take action beyond alerting an administrator, it is

capable of scanning high volumes of traffic without slowing down network performance (VMWare, 2022). An IPS works by being placed inline, in the flow of network traffic between the source and destination and usually “sits” behind the firewall (VMWare, 2022). An IPS utilizes the following techniques to identify threats: signature-based, anomaly-based and policy based (VMWare, 2022). Moreover, there are several types of IPS each with a slightly different purpose: Network intrusion prevention system (NIPS), Host intrusion prevention system (HIPS), Network behavior analysis (NBA) and Wireless intrusion prevention system (WIPS). Once the malicious activity is detected, an IPS can take actions (in addition to alerting administrators) such as dropping the packets, blocking traffic from the source address, or resetting the connection (VMWare, 2022). Some IPSs also utilize the “honeypot” technique, or employ a decoy high-value data to attract attackers and prevent them from reaching their targets (VMWare, 2022). An IPS offers the benefits of additional security, increased efficiency for other security controls, time saving, compliance and customization (VMWare, 2022).

An Ubuntu Linux OS virtual machine running Snort served as the IPS software for this cyber security lab. According to the company that produces the software, Snort is “the foremost Open Source Intrusion Prevention System (IPS) in the world” (Snort, 2022). Snort as an intrusion prevention system software uses a series of rules that help define malicious network activity (Snort, 2022). It uses those rules to find packets that match against them and generates alerts for users (Snort, 2022). To stop these packets, Snort can be deployed inline (Snort, 2022). Snort is used for mainly three reasons: As a packet sniffer like tcpdump, as a packet logger (useful for network traffic debugging), or

it can be used as a full-blown network intrusion prevention system (Snort, 2022). Snort can be downloaded and configured for personal and business use (Snort, 2022).

A cyber security lab is not complete without a firewall. Since the mid 1990s, firewalls have offered the first line of defense in network security systems (Rouse, 2022). Firewalls were developed as a security device to protect your network from unauthorized access to private data (Rouse, 2022). Firewalls provide surveillance on attempts by unwanted traffic to access your operating system by forming barriers between computers and other networks (Rouse, 2022). Firewalls also serve as traffic controllers, managing and validating a network's access (Rouse, 2022). Most operating systems and anti malware software have a pre-installed firewall (Rouse, 2022). Firewalls can be either hardware or software and typically come in 4 forms: packet filtering, proxy service firewall, stateful inspection firewall and next-generation firewall (Rouse, 2022). Firewalls can be configured with an IPS to block malware and application-layer attacks (Rouse, 2022). A firewall will usually allow incoming connections that are authorized to access a network (Rouse, 2022). The security systems in place will then allow or block data packets based on existing security rules (Rouse, 2022). A firewall creates checkpoints that filter web traffic and allows the user to review and act upon rogue network traffic before the targeted network experiences any adverse effects (Rouse, 2022).

In this instance, pfSense was created and virtualized to be used as the firewall within the network of the cyber security lab. pfSense was first created in 2004 as part of the project "m0n0wall" that aimed to create fully-featured, embedded firewall software (Ot,

2021). pfSense is a firewall and router software that is free to use if the user has the correct hardware, meaning it can be configured on hardware from a specialized router to, say a Windows 7 PC that is fully functioning (Ot, 2021). pfSense is mainly used as router and firewall software, and can be configured as DHCP, DNS, VPN servers as well as a WiFi access point all while running on the same hardware device (TekLager). In addition, pfSense allows for installation of third party open source software such as Snort or Squid through a built-in Package Manager (TekLager). pfSense is appealing as it can be installed on any hardware turning, for example, a 15-year-old working computer into a brand new router (if it has at least 2 network cards) (TekLager).

What would a cyber security lab be without a server and workstations to interact with? In this instance, workstations are desktop and tower computers or laptops that perform tasks for the client requiring access to the internet and thus vulnerable to attacks. A server, though, has a specific function within a network (Indeed Editorial Team, 2021). While a server can be any type of device that shares and saves information, it can also both store and process information within their own system or request it from another (Indeed Editorial Team, 2021). There are several kinds of servers including: web, proxy, virtual machines, file transfer protocol (FTP), application, file, database, mail, print, collaboration, domain name systems (DNS) and gaming (Indeed Editorial Team, 2021). Servers work as data processors for public, commercial and private use (Indeed Editorial Team, 2021). Additionally servers are large data storage and processing devices that exist either as hardware or as virtual storehouses located on the internet in the form of cloud software (Indeed Editorial Team, 2021). Also, computers or software

systems act as servers that connect to a network (Indeed Editorial Team, 2021). For this cyber security lab, the server is being used as an application, database, file and web server.

Many cyber security labs utilize an attack machine representing either malware or some form of unauthorized access. The accompanying cyber security lab also uses an attack machine in the form of a VM that is running on the Kali Linux OS system within the same network. Kali Linux, developed by Mati Aharoni and Devon Kearns, is a security distribution of Linux born from Debian and designed for computer forensics and advanced penetration testing (Williams, 2022). Kali Linux contains over 600 pre-installed penetration testing applications with unique flexibilities and use cases (Williams, 2022). In this lab, it was used as a malicious actor with designs on penetrating the targeted machine.

Like many cyber security labs, this one also features a virtual machine built using Ubuntu Linux 22.04 OS that was used as a target machine running the Metasploit Framework software. The Metasploit Framework is software that can be used by cybercriminals as well as ethical penetration testers to probe systematic vulnerabilities on networks and servers (Buckbee, 2022). Due to its status as an open-source framework, it can be customized and used with most operating systems (Buckbee, 2022). Metasploit can be used ready-made or custom coded and in this case, configured on a network as a target machine, configured to be purposely vulnerable allowing for cyber security solutions to be tested out (Buckbee, 2022).

In summary, cyber security laboratories are beneficial to the learning and development of protocols to prevent or remedy cyber based attacks. They can be set up physically or in this instance virtually with the aid of various tools such as VMs, SIEMs, intrusion detection systems, intrusion prevention systems, firewalls, servers and workstations. In both lab environments numerous open-sourced operating systems and programs can be employed such as Ubuntu, Security Onion, Suricata, Snort, pfSense, Kali Linux penetration programs and Metasploitable. Being able to create and learn from a cyber security laboratory environment is essential to the advancement of cyber security solutions.

References

Buckbee, M. (2022, February 24). What is Metasploit? The beginner's guide. Varonis. Retrieved December 11, 2022, from https://www.varonis.com/blog/what-is-metasploit

Buckbee, M. (2022, June 6). What is Siem? A beginner's guide. Varonis. Retrieved December 11, 2022, from https://www.varonis.com/blog/what-is-siem

Ghimiray, D. (2022, October 6). What exactly is a virtual machine and how do they work? Avast Security: Other Threats. Retrieved December 11, 2022, from https://www.avast.com/c-virtual-machine

IBM. (n.d.). What is Security Information and Event Management (SIEM)? IBM. Retrieved December 11, 2022, from https://www.ibm.com/topics/siem

Indeed Editorial Team. (2021, January 13). Types of computer servers and how they function . Indeed.com. Retrieved December 11, 2022, from https://www.indeed.com/career-advice/career-development/types-of-servers

Justabouttechie. (n.d.). Retrieved December 11, 2022, from https://sites.psu.edu/mariasoyosocapuder/how-to-build-your-own-homelab-for-cyber-security-testing/

Katz School of Science and Health, Yeshiva University. (2022, August 18). The 10 best open source siem tools for cybersecurity experts. Katz Cybersecurity Blog. Retrieved December 11, 2022, from https://online.yu.edu/katz/blog/the-10-best-open-source-siem-tools

Ot, A. (2021, February 3). 6 reasons why you should be using pfsense Firewall. MUO. Retrieved December 11, 2022, from https://www.makeuseof.com/reasons-use-pfsense-firewall/

Rouse, G. (2022, May 31). What is a firewall and why is it important in cyber security? Datto. Retrieved December 11, 2022, from https://www.datto.com/blog/what-is-a-firewall-and-why-is-it-important-in-cyber-security#:~:text=A%20firewall%20is%20a%20security,networks%20and%20untrusted%20outside%20networks.

Security onion: An interesting guide for 2021. Jigsaw Academy. (2022, July 6). Retrieved December 11, 2022, from https://www.jigsawacademy.com/blogs/cyber-security/security-onion/

Viglione, M. (2022, March 27). Suricata: What is it and how can we use it. Infosec Resources. Retrieved December 11, 2022, from https://resources.infosecinstitute.com/topic/suricata-what-is-it-and-how-can-we-use-it/

What are Cyber Labs and the importance of cyber security? Jigsaw Academy. (2022, November 4). Retrieved December 11, 2022, from https://www.jigsawacademy.com/blogs/cybersecurity/what-are-cyber-labs-and-the-importance-of-cyber-security/#:~:text=The%20company's%20IT%20department%20is,access%20to%20computers%20and%20networks.

What is an intrusion detection system? Palo Alto Networks. (n.d.). Retrieved December 11, 2022, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids

What is an intrusion prevention system?: Vmware glossary. VMware. (2022, December 1). Retrieved December 11, 2022, from https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html#:~:text=What%20is%20an%20intrusion%20prevention,it%2C%20when%20it%20does%20occur.

What is pfSense - introduction to open source router/firewall operating system. TekLager. (n.d.). Retrieved December 11, 2022, from https://teklager.se/en/pfsense-introduction-open-source-router-firewall/

What is Snort? Snort. (n.d.). Retrieved December 11, 2022, from https://www.snort.org/#:~:text=What%20is%20Snort%3F,and%20generates%20alerts%20for%20users.

Williams, L. (2022, November 12). Kali Linux tutorial for beginners: What is, how to install & use. Guru99. Retrieved December 11, 2022, from https://www.guru99.com/kali-linux-tutorial.html#:~:text=Kali%20Linux%20is%20a%20security,Devon%20Kearns%20of%20Offensive%20Security.