ISCS 3523-004

Lab 01: Intrusion Detection Tools

Christian Barba; fgb587

September 11, 2022

Table of Contents

Introduction

The purpose of this lab is to establish a virtual environment that will allow the user to simulate real world attacks in a risk-free zone. Many cybersecurity experts set sand boxes to dissect malicious code, test security features, and analyze attacks to obtain a deeper understanding on how to make their host computers a safer space. Without being able to view attacks head on, the ability to detect attacks and learn how to prevent them would become nearly impossible.

Setting up the Virtual Machine Lab

Setting up the virtual machines that are used for the rest of this course was not an easy process, and I had to troubleshoot multiple problems that I ran into. During this lab, I had to install a PfSense VM, a Kali Linux VM, two Ubuntu server VMs (IPS and SIEM), a Metasploitable VM, and finally a Windows 10 VM. The process of installing all these ISOs and OVAs took me around three days in total as a lot of the mistakes I was making were minor. The problems that was most drastic was not being able to install Suricata on IPS, but due to the availability of an OVA, I chose to download that instead. Figure **4.1** shows all of the virtual machines that are in my VirtualBox.

Verifications of a Working Environment

Due to the network topology that I had setup in the lab, I can ping Metasploitable 2 from my Kali machine as well as my PfSense, and I can browse the internet on Kali. The verification that I can ping Metasploitable 2 from my Kali machine is shown in figure **1.1**, and figure **1.2** shows that I am able to ping my Kali machine from Metasploitable 2. My IPS machine can connect to the internet through the Host-only networking that was set up in the network configuration. I can use the commands *curl -I https://google.com* and *nslookup google.com* to get proper feedback as shown in figure **2.1**. The *curl -I* returns the HTTP response headers from google.com, and the *nslookup* shows the NDS records for google.com. Through the Splunk website, I can inspect the activity and alerts that are detected on my SIEM VM. Figures **3.1** and **3.2** show that the website is functional and is reporting the activity that is

occurring on the VM. There have been no alerts because none of the commands I have used have been of concern.

When opening a Kali terminal and using the command *ip addr*, it displays 2 adapters shown in figure **5.1**. These are shown as lo and eth0, and lo is the loopback interface, which is how the system talks to itself, while eth0 shows the IP address for the machine and how everyone else will recognize it if someone decides to ping it. This is not the exact same case when I type in the *ipconfig and ipconfig /all* commands in the Windows 10 command prompt. In Windows, the *ipconfiog* command shows the IPv4 address, Subnet Mask, and the Default Gateway, but when you add the */all* extension, more information appears such as the DHCP server information. The physical address is also visible under this extension.

When using Wireshark on both Kali and Windows there was a noticeable difference. Figure **5.2** shows how a Windows version of Wireshark is presented. Wireshark on this OS gives out more information like the TCP packets that are regularly active during the system without any ping enabled from Kali. Windows also is able to show the TCP ports that were used when Windows ran into problems with some packets that came through the network. The TCP retransmissions are located throughout the report on the Windows machine, but in figure **5.3**, Kali only shows the ping requests and the replies that occurred during this exchange.

Six Applications used for Intrusion Detection on Kali Linux

Kali Linux is host to many cyber security applications that can be used to detect intrusions on a given system. Some of these applications include: “lbd”, “Wireshark”, “nmap”, “netmasks”, “wafw00f”, and “Suricata”. According to Packt, lbd is a tool used to detect load balancing on a given DNS or HTTP, and this would indicate if a router were getting throttled from a DDoS attack for example. Load balancing is important in a company environment because the network has to be function to a high standard to supply access to multiple users with proper internet access. If network traffic appears to be building up there will be an easier way to detect why this is happening due to lbd. Wireshark is used to see the traffic

coming into a network by displaying all the packets being sent and received. If there is to be believed that a surplus of network traffic, perhaps detected by the lbd, then Wireshark allows us to find the source of this traffic and understand why it is happening. The tool nmap is used to display the network topology on a given network, and this can show who is on the network, what OS they are running, and manage the host machine, as well as other services (Javapoint). A way hackers try to steal information is by exploiting a company's internet connections by logging onto their servers. Thanks to nmap, there is a way to detect who is on the server, and if there appears to be someone running a non-native OS then it will be easy to detect and shutdown. Netmasks can be used to find a subnet mask to identify hosts that may be connected to a network (Kali Linux, 2022). This appears to go hand in hand with nmap at detecting who is on a server. Wafw00f detects if the website a person is accessing is protected by a firewall by sending certain attacks to validate the website is official or not because a safe website should have an active firewall (mohdshariq). Dealing with co-workers may entale that they might encounter suspicious websites that appear to be friendly, but with wafw00f, it is now simpler to detect if these websites are actually valid. This application could be used to defend against SQL injections. Lastly, a tool that can be used for IPS is Suricata because Suricata is used to detect threats on a network by using deep packet inspection. All these tools are useful for intrusion detection because the main purpose of them tools is to detect any malicious traffic that may be flooding into the network a person is operating on. Whether it be monitoring the packets coming into the network or displaying the map of machines connected in a single topography, these tools can detect if something is wrong or out of place.

How this lab works and why it is useful

Installing multiple machines onto one host computer is one of the most important tools that a penetration tester, malware analysist, forensic analysist, et cetera, can use to obtain research. The topology of this lab is the most important part because we are able to load destructive material into the machines without being afraid that it will leach onto out host computers. This is due to PfSense acting as the router that connects all of the machines together. PfSense is able to use network management protocol

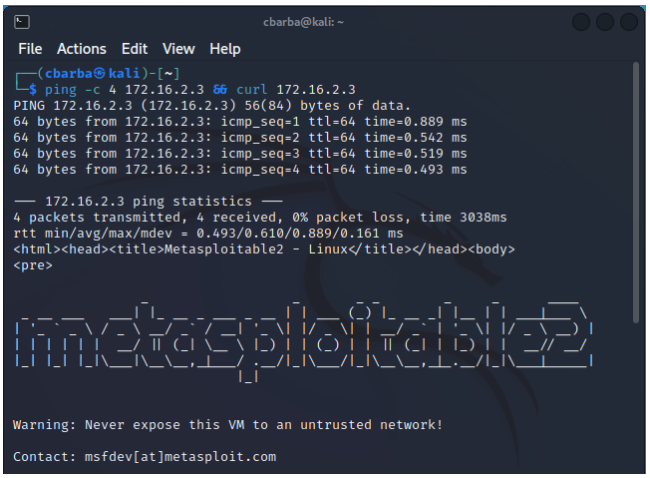
DHCP to establish a range of IP addresses and assign certain machines these IP addresses in order to keep everything on a specific range. This is especially useful when working with multiple virtual machines on a host computer as mapping out the network topology becomes organized and precise as to not mix up specific machines. Throughout the lab, we have taken multiple precautions like setting up firewall rules and squid proxy servers to ensure nothing can escape a Kali or a Metasploitable 2 machine through the network and reach the host computer. Both Kali and Metasploitable 2 are functioning on the intnet network setting, which will allow them to connect to the internet through the PfSense router we have established early on. On this virtual router we have disabled the IPv4 protocol for Metasploitable 2 to deny any packets from dispersing outwards as well as blocking out ports 80 and 21 to deny any HTTP and FTP requests to go out. However, through Suricata acting as a three-way handshake on our IPS machine, we are able to send packets from Kali to Metasploitable 2 and detect whether or not these packets violate the rules that Suricata has defined with the af_packet. Another feature we have disabled on these machines is the ability to drag and drop files from the VMs to the host computer. Since we will be dealing with malicious code, it is important that there is no possibility of a slip up that may cause the viruses to jump from the machines onto our host computer.

The purpose of setting up this virtual ecosystem is to have a place to load in malicious code as well as see how a network may be reacting to certain events that may occur by an attacker. Being able to simulate attacks that have been used before can allow an analysist to gain knowledge and get familiar with the tools that can help with attacks that may be coming in the foreseeable future. For penetration testing, we could use certain tools and applications that will allow us to test the defenses of our environment, and with this information, we can fortify our real-world systems to stop certain attacks from happening again. For forensics, being able to load a hard drive into a virtual machine would be the ideal situation for the analysist. This is due to not knowing what is on a hard drive that you may want to analyze because it could be full of malicious code. If this is the case, then the virtual machine will be able to take all of the damage and not the host computer. These situations appear a lot of the times throughout

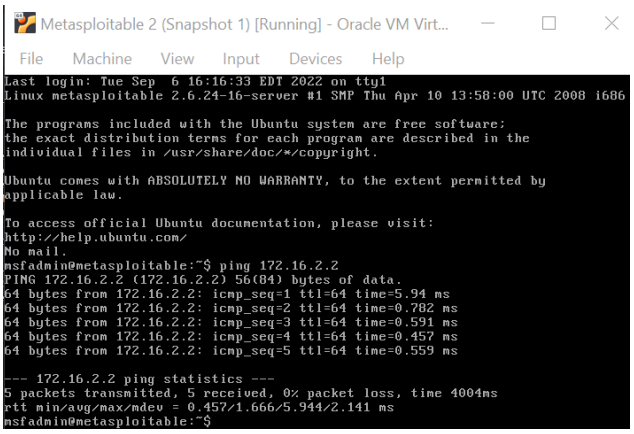
a cyber security experts' career. Having this virtual environment allows these security experts to have a sandbox to test anything that they may seem fit.

Appendix

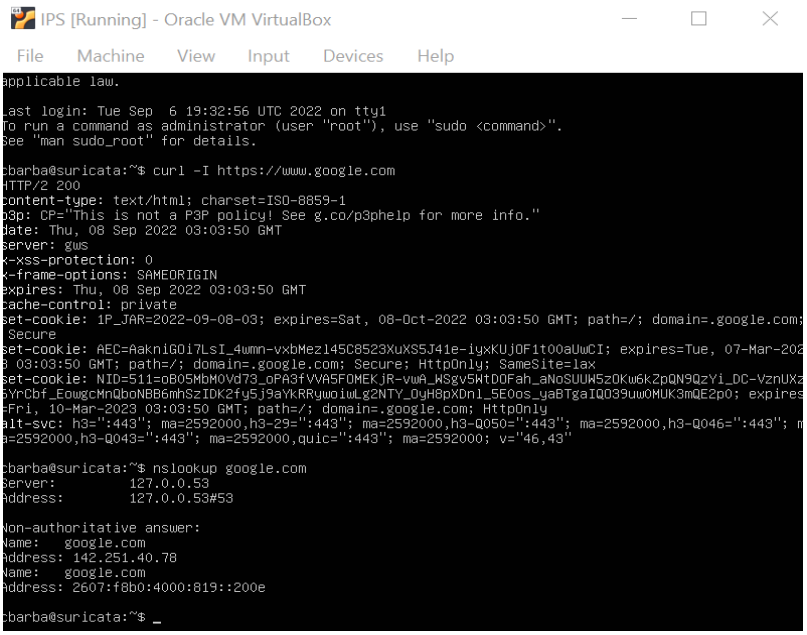
1.1- Pinging and Curling Metasploitable 2 from Kali Linux:



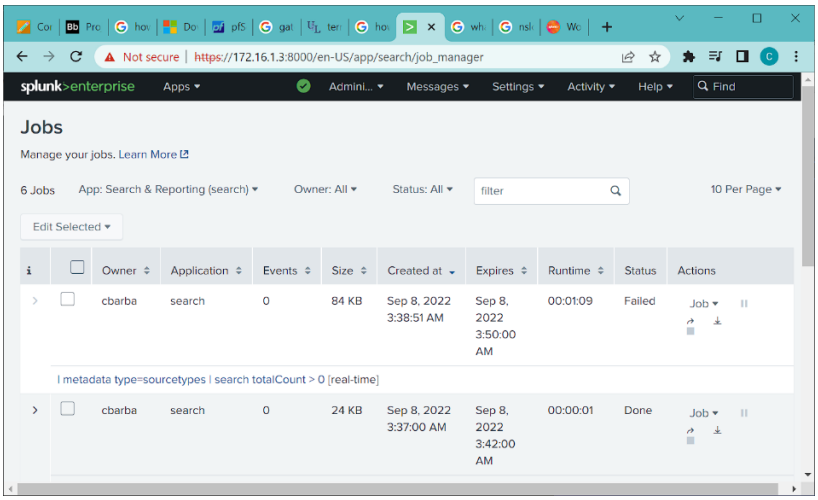
1.2- Pinging Kali Linux from Metasploitable 2:



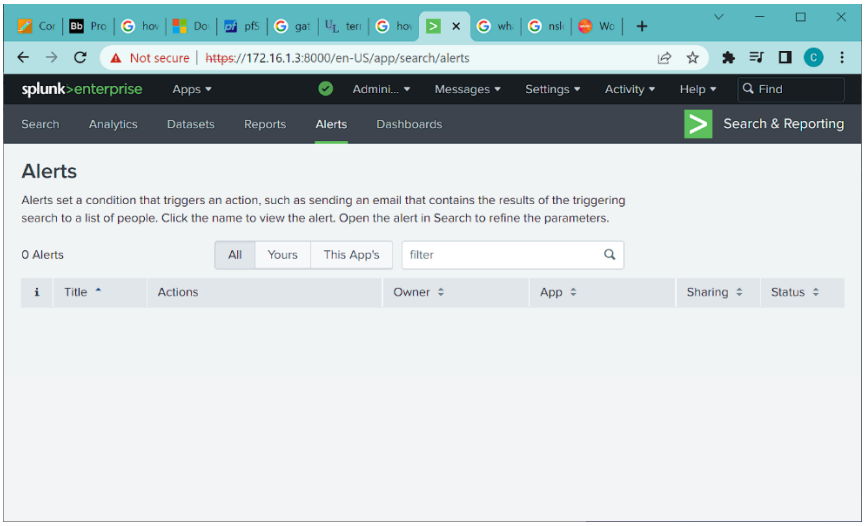
2.1- IPS being able to curl and Nslookup google.com:



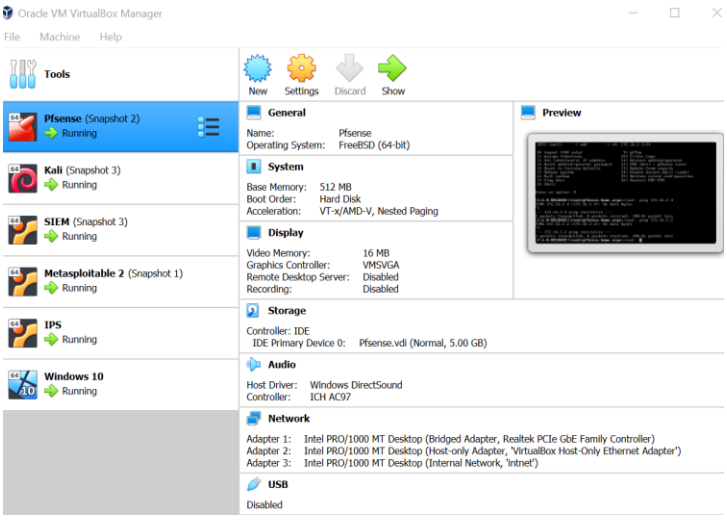
3.1- Splunk activity logs (Jobs page):



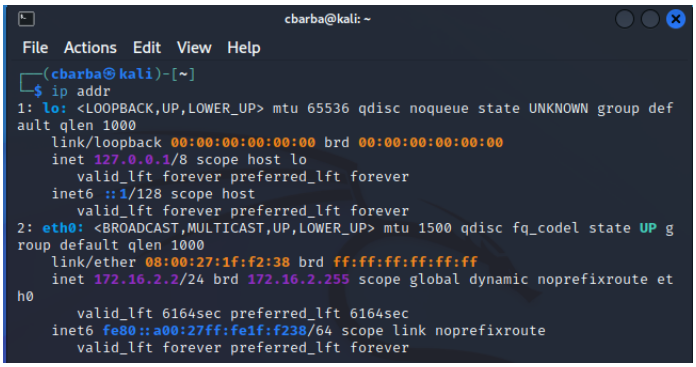
3.2- Splunk alert page:



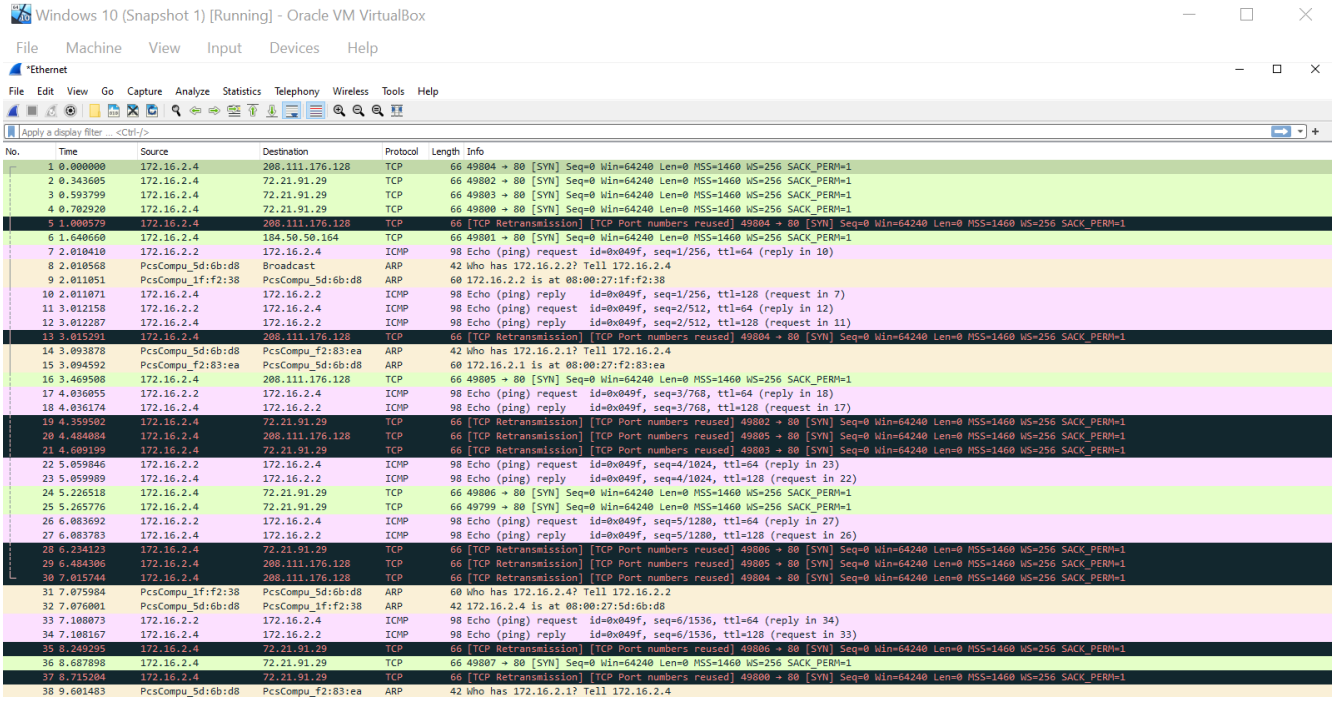
4.1- List of all VMs working on the host computer:



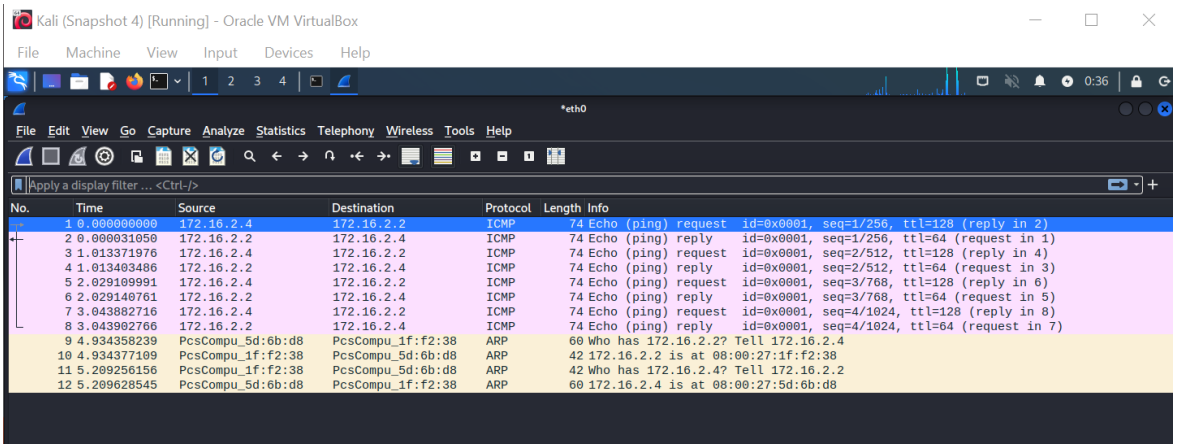
5.1- Kali Linux IP address configurations.



5.2- Windows Wireshark results:



5.3- Kali Wireshark results:



Works Cited

"HTTP and DNS Load Balancer Detection." *Packt*, https://subscription.packtpub.com/book/networking-and-servers/9781783982165/5/ch05lvl1sec50/http-and-dns-load-balancer-detection.

mohdshariq. "Identification of Web Application Firewall Using WAFW00F in Kali Linux." *GeeksforGeeks*, 30 June 2021, https://www.geeksforgeeks.org/identification-of-web-application-firewall-using-wafw00f-in-kali-linux/.

"Netmask: Kali Linux Tools." *Kali Linux*, 5 Aug. 2022, https://www.kali.org/tools/netmask/.

"Nmap Commands in Kali Linux - Javatpoint." *Www.javatpoint.com*, https://www.javatpoint.com/nmap-commands-in-kali-linux.