

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | Lab 1: Cyber Range Configuration & Network Topology | | | | |  | |
|  |  | | | | | | |  |
|  | | | |  |  | | | |
|  | | | | Cesar Munguia |  | | | |
|  | | | | 09/11/2023—IS-3523-004—Ian Burres |  | | | |
|  | | |  | | |  | | |



|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  | | |  |
|  | INSTRUCTIONS | | | | | | |  |
|  |  | | |  |  | | |  |
|  |  | |  | | |  | |  |
|  |  |  | This lab involves two sections. The **first section** helps you set up and configure the cyber range that you will be using for the remainder of the semester. The **second section** asks you to write a 4-page, double-spaced MLA format paper, discussing all the networked elements in the cyber range. You will also provide a network diagram showing me how the virtual network is configured. | | |  |  |  |
|  | | | | |
|  |  |  |  |
|  |  |

# Section 1: Cyber Range Configuration

1. I accessed my Cyber Range instance with the information provided to me by  
   the administrator (currently Jerod Ryan).
2. Inside of the Windows 11 VM, I saw the Desktop and a folder (likely  
   with my last name). That folder contained the HomeIRLab.ova
3. I right-clicked the VirtualBox icon and ran as admin (used the admin username  
   and password Jerod gave you).
4. I imported the appliances, I made sure to choose “import all MAC addresses”  
   from the dropdown box. I DID NOT create new ones.
5. I started up Pfsense.
6. I navigated the browser and made sure I could access 172.16.1.1 (Pfsense  
   GUI)
7. Now I started the IPS and checked to make sure it had the correct IP.
8. I started the SIEM and checked its IP. I waited about 3 minutes after it started before  
   I moved on to step 9.
9. I logged into Splunk using the browser: <https://172.16.1.3:8000>
10. I started up the rest of the VMs and checked their IP and connectivity.

# Section 2: Network Analysis and Network Topology

The main purpose of this second section of the lab is to describe and explain the major components of the network I previously set up in section one. There are exactly five virtual machines that are being used in this network in which those are: 1) Pfsense, 2) IPS, 3) SIEM, 4) Kali, and 5) Metasploitable 2.

The network was made intentionally with some logic behind it. The first component that one would encounter in this network would be Pfsense. Pfsense is essential the firewall that protects all the traffic that goes in and out of the network. In order for this network to be compromise, the hacker would have to bypass the firewall first and then it would access to it. Another thing to mention is that once the intruder has made its way into the network there is no possible way that the firewall (Pfsense) can do something about it to stop or to prevent the intruder from doing malicious things because that is not its main task. There is a particular VM that does what I’ve previously stated and that is the IPS which stands for Intrusion Prevention System. In brief words an IPS is a particular system within a network that its main task is to look for any suspicious activities that might be in the look for specific vulnerabilities and to also prevent those activities from happening in the first place. At the same time that it’s preventing these activities from happening it is also storing and reporting all the information given for future references. The next virtual machine works together with the IPS and that is the SIEM. The SIEM, which stands for Security Information and Event Management, is a system that functions a little similar to an Intrusion Prevention System. Rather than controlling and preventing a threat just like the IPS does, its main task is to utilize the IPS’s information to create a better overall picture/image of the security aspects of the network. It can also find some vulnerabilities and threats that might be unknown, out of the sight, and/or hidden in the network so that they could be potentially fixed in the future for a more secure network. The next VM is the target machine, which is the Metasploitable 2 machine. This is essentially a virtual machine that is designed intentionally to be vulnerable so one can do penetration testing, exploit testing, and other practices. These vulnerabilities are more operating system-and-network-based rather than application vulnerabilities. This is an excellent place where us the students can learn and practice aspects about intrusion detection and prevention. The last component that is to be considered in this lab is the Kali virtual machine. This is basically the machine that is responsible to break into the network, or in other words, the intruder itself. This is how the network is logically arranged. Next, I will be talking about the networks inside the network.

To leave things clear I will be stating the IP address of each virtual machine so that it’s better visualized and understood.

1. Pfsense: **172.16.2.1**
2. IPS: **192.168.56.101**
3. SIEM: **192.168.56.102**
4. Kali: **172.16.2.2**
5. Metasploitable 2: **172.16.2.3**

Within this network there are two additional networks, or communication of some sort between two or more VMs. The first network within our main network is composed of the Pfsense VM, the Kali VM, and the Metasploitable 2 VM. Their subnet mask is 255.255.255.0. The second network is composed of the IPS and the SIEM, their subnet mask is 255.255.255.0.

There are another two extra components that need to be mention that play important roles and those are the Pfsense GUI and the SIEM Splunk and their IP addresses are **172.16.1.1** and **172.16.1.3**, respectively. The Pfsense GUI is just similar to the regular Pfsense, however, this one is a little more friendly because information is organization and visualization is much better. They are both within the same network meaning that they could technically communicate with each other. They share the same subnet mask which is 255.255.255.0.

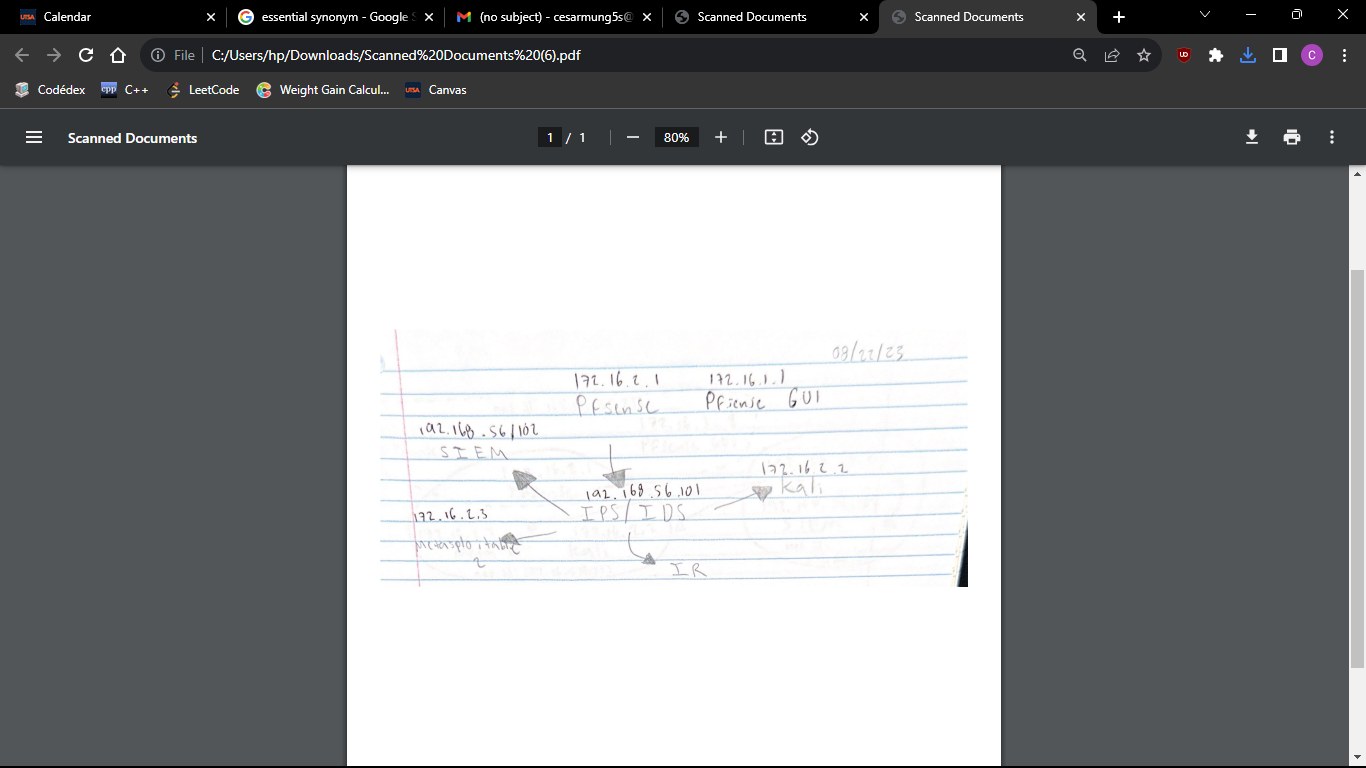
Logically, before the intruder tries to attack or invade the network it has to deal with its firewall first which it’s the first step to take. Kali (or the intruder) is able to contact the firewall software because it’s technically reachable in the network. As I played around with the network and the VMs for a few minutes I was able to find the firewall rules in the Pfsense GUI and these were my findings for OPT1: 1) Metasploitable 2 is not able to establish any type of connection from its end (outbound connection), 2) DNS packets are allowed to come in to the gateway, 3) NTP packets are allowed, 4) proxy traffic allowed, 5) can’t send HTTP packets out, and finally 6) can’t send FTP packets out. OPT1 is basically a port that help us create networks separated from the others, in other words, isolated networks. I saw that only a couple of rules had a green checkmark meaning that those rules are enabled and the other ones are disabled. There are currently four enabled firewall rules in which three of them have source IP 172.16.2.0/24 and destination IP 172.16.2.1 which is the Pfsense VM. The firewall rules for LAN are as follow: 1) anti-lockout rule, 2) better anti-lockout rule, 3) allow DNS traffic to gateway, 4) allow NTP traffic to gateway, 5) allow squid proxy traffic to gateway, 6) allow SSH access from hypervisor host to Kali Linux, and 7) allow HTTPS outbound. Out of the ten firewall rules only 8 are enabled, the rest are disabled. Most of the rules have source IP 172.16.1.0/24 and destination IP 172.16.1.1. It seems like the OPT1 rules are made specifically for the Pfsense VM and information circulating in its own network only. In the other hand, the LAN rules are made for the Pfsense GUI and information circulating in its own network only. Coming back to my very first statement, if a hacker wanted to access the network, he/she would have to bypass all of the rules that I’ve stated before.

Once the intruder has made its way into the network the next thing that it will come up with is the IPS (intrusion prevention system). There is a very particular aspect about this next “step” which is to re-emphasize that this IPS works together with SIEM (Security Information and Event Management). They both combat the intruder into preventing any further damage or exploitation. The IPS and SIEM VMs work with the Suricata software and the Splunk software respectively. Another important thing to re-iterate is that they are, obviously, in the same network (192.168.56.0/24).

Out of all the tools that Suricata offers there is one that is considered to be used in the future and that is the AF\_PACKET. It is essentially a tool that “establishes a software bridge between two interfaces by copying packet from one interface to another (and reverse)” as the Mirantis stated in its webpage (IPS Mode using AF\_PACKET). This tool would have to be set up manually by the user, for instance, one could set a bridge between two interfaces like eth0 and eth1 but it all depends on the interface that one is working with and the data as well. Moving on, the SIEM Splunk is somewhat similar to the Pfsense GUI and we are actually accessing in the browser for the same reason that we were using Pfsense too in the beginning. It offers us better visualization and data is better organized, at least to the human eye.

The “final destination” of the intruder is then reached, which is the vulnerable machine Metaspolitable 2. Our main job during the semester is to “keep an eye” of what is being happening in the network and for that we would be using another virtual machine which we will not be using until later. This is essentially how the network is set up and to know and understand all this is crucial for being successful in the class.

Here is a diagram that I drew myself to show a visual representation of our network:



# Works Cited

“IPS Mode Using AF\_PACKET¶.” *Mirantis Documentation: IPS Mode Using AF\_PACKET*, docs.mirantis.com/mcp/q4-18/mcp-security-best-practices/use-cases/idps-vnf/ips-mode/afpacket.html. Accessed 8 Sept. 2023.