**Final Project Recap**

 Jose Flores

CSOL-570-03-SP23: Network Visual/Vulnerability

Dr. McCready

February 27, 2023

**Trade Studies**

Performing trade studies are essential to help decide which platforms are more beneficial to the organization. Trade studies depend on the factors the organization considers ranging from cost, customizability, usability, and paramount circumstances. Performing a trade study to identify which network visualization and vulnerability scanning tool are best for an organization was challenging because of the different circumstances.

**Network Visualization Tools**

A network visualization tool provides a visual aid for data flows between network entities. Due to having trouble with the virtual box at the beginning of the course, I could not install and explore different network visualization tools. Instead, I had the privilege of using SolarWinds and Splunk on an enterprise level with my organization. The criteria I chose to compare these two network visualization tools were: cost, customizability, security, visual aids, features, and useability. Another criterion I should have added to this trade study is the organization’s reputation because a reliable and trustworthy application is vital.

Conducting the trade study was different because I did not install the applications and did not get to change the interface as I would have liked to. I explored and created customized visual aids to represent the traffic flow for both applications. These visual aids ranged from maps, graphs, and bar charts, and I could choose the color, size, and font to my liking. Both interfaces were user-friendly and easy to navigate through without taking extra steps. The cost factor between network visualization tools differs and depends on the organization’s size and traffic flow. Splunk’s cost depends on the daily data flow; it would cost more if the organization had a heavy traffic flow (Splunk, n.d.). SolarWinds’s cost depends on the devices connected to the application; the more devices the organization has, the more it will cost (SolarWinds, n.d.). The organization's traffic flow and devices will depend on the cost-efficient application. Between the two network visualization tools, I have concluded that I would go with Splunk because of its reputation. Splunk has an excellent reputation compared to SolarWinds because of its recent attack in 2020. SolarWinds supply chain attack impacted government departments and companies such as Homeland Security, State, Intel, and Microsoft (Kerner & Oladimeji, 2022).

**Vulnerability Scanning**

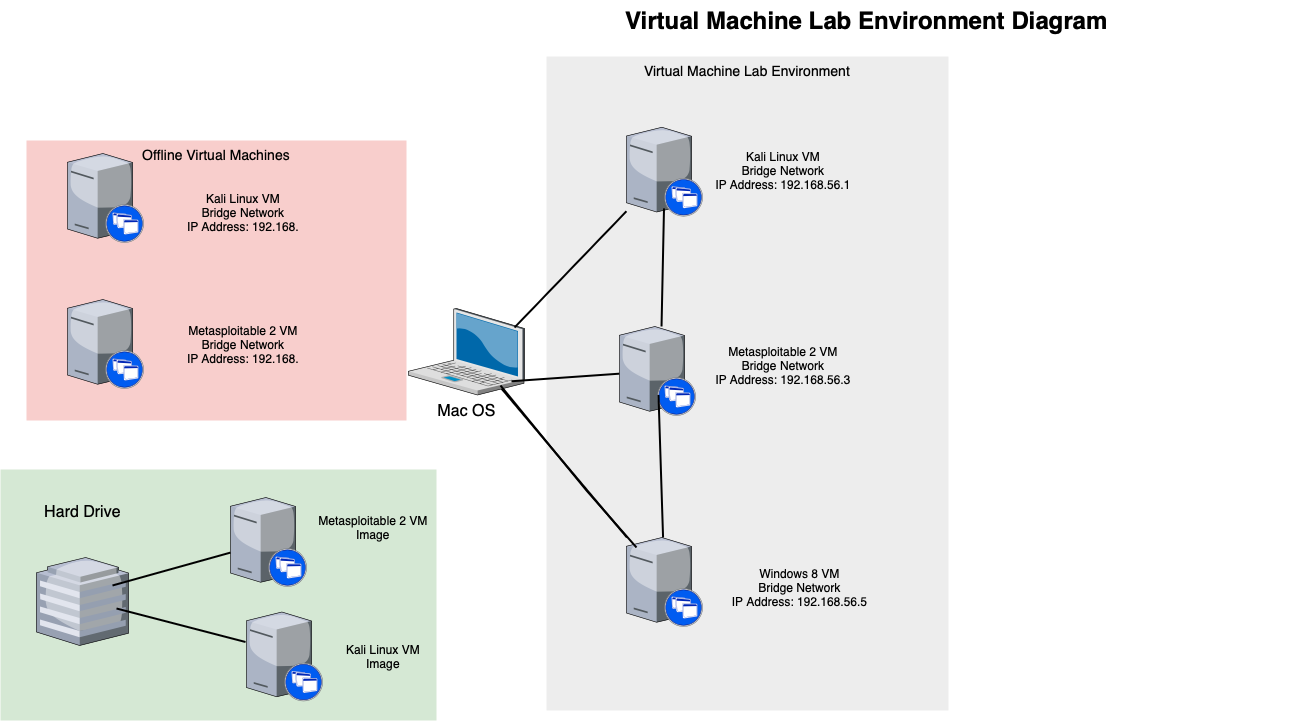
A vulnerability scanning tool aims to find and correct the system’s weaknesses before a malicious hacker finds them. The application can save the organization time and money by actively protecting its systems and correcting errors. Some errors are easily fixable by updating or fixing a misconfiguration on a system. The criteria used to determine which vulnerability scanner is more effective were: features, complexity, support, cost, operating specifications, and CVE compatibility.

The two vulnerability scanning tools compared were Nessus and OpenVAS. Nessus is flexible on multiple operating systems, but OpenVAS is only available on Linux. The complexity of installing Nessus was straightforward as downloading the packages. The Nessus website automatically detects which operating system you are running and which version is compatible with the specification of your system. If there was any complication while downloading the packages, Nessus has a breakdown on installing the file and provide customer service through a chat box. OpenVAS does not have a customer service section but a community forum where users may ask specific questions. Nessus and OpenVAS are compatible with common vulnerabilities and exposures (CVE) databases and have user-friendly web interfaces. The Nessus dashboard is more advanced than OpenVAS, and it is easier to start a scan on the system. OpenVAS required extra steps to start a scan, and navigating through the different pop-ups was complicated. The main difference between the two applications where the cost. OpenVAS is free to any user with a Linux system. Nessus cost, at a minimum for any version, is about $3000 (Tenable, 2023).

Of the two vulnerability scanning tools, Nessus is much more powerful than OpenVAS. If an organization has the funds to spend on Nessus, I would prefer Nessus due to the additional features and operating system flexibility. However, OpenVAS is an excellent alternative for Nessus if the operating systems are Linux. The most critical

**Virtualized Test Lab Architecture**

Setting up the virtualized test lab in a MacOS is difficult due to the hardware limitations, but it is possible with additional software. The purpose of having a virtual test lab is to experiment with different tools in a controlled environment. These tools are powerful enough to misconfigure, destroy, or harm the system if misused. After extensive research and networking with colleagues, Parallels Desktop is the best option for running a MacOS. Parallels Desktop allows the user to run Windows operating systems and Linux virtual machines. Downloading VirtualBox into a MacOS limits its capability because the virtual machine will crash or be unresponsive. Although the latest VirtualBox supports Apple Silicon M1/M2 chips, the virtual machine will continuously crash.

Using the Parallels Desktop on a MacOS was easier because the virtual machine would not crash while running multiple virtual machines simultaneously. My virtual test lab environment consisted of two Kali Linux, a Windows 8, and two Metasploitable 2 virtual machines. The purpose of having two Kali Linux and Metasploitable 2 virtual machines is in case I misuse the tools and misconfigure, destroy, or harm my system. I kept a Kali Linux and Metasploitable 2 virtual machine offline and images of them on my hard drive. The purpose of the Kali Linux virtual machine was to explore vulnerability scanning, network sniffing, information gathering, exploitation, and other vital tools. These tools are compelling, and I experienced firsthand how powerful they are by misconfiguring my Kali Linux when looking for exploitation on my Metasploitable2 virtual machine. The Metasploitable 2 virtual machine is the Linux system I use to test security tools. Instead of downgrading an operating system or leaving ports open, Metasploitable 2 is designed to have vulnerabilities and practice using the tools in Kali Linux. The Windows 8 virtual machine was used in case I could not do any of the assignments with my MacOS and needed to go on a Windows operating system. The VM was configured as a bridge network with a DHCP server configured with a pool of IP addresses it may use. 

**Security Tool**

Kali Linux virtual machine has unique security tools that can be used to protect or attack a system. The tools to protect a system are actively looking for vulnerabilities or unusual traffic flow so it may be fixed or corrected. The tools used to attack a system are actively looking for vulnerabilities and want to exploit them.

**Wireshark**

Wireshark is a network protocol analysis and packet sniffer software. This tool lets the user see and read captured packet data. Security engineers can detect suspicious activity in real-time or offline analysis by filtering the captures to see if the three-way handshake was completed (CompTIA, n.d). Wireshark ability to see network traffic is vital to investigating a Distributed Denial of Service (DDoS) attack because it captures the IP addresses, time, and altitude of packets. Although Wireshark can not stop malicious activity, it is essential software that can improve network defenses by examining network security and patterns. With Wireshark, I can see all my traffic flow in my virtual environment. For example, the traffic flow is heavier when streaming videos online than web surfing.

**Nessus and OpenVAS**

Nessus is a paid, well-known vulnerability scanner used by large corporations. The software is compatible with CVE baseline and various operating systems. OpenVAS is a free, open-source vulnerability scanner compatible with the CVE database and only available on a Linux operating system. A vulnerability scanner looks for potential security vulnerabilities in a system by cross-referencing the CVE database. Using these tools, I can see my system's weaknesses and take action to correct or fix them before they are exploited.

**Kismet**

Kismet is a sniffer tool that detects wireless networks and devices nearby. The application can be installed on MacOS or Linux operating systems. Kismet's web interface displays the wireless access points (WAP), service set identifiers (SSID), Media Access Control (MAC) addresses, manufacturer, and encryption protocols. Knowing this information, a malicious hacker can MAC spoof and exploit known vulnerabilities by the manufacturer or their encryption protocol. Kismet allowed me to see every WAP and SSID nearby me and tell me what channel they are using. This is helpful to malicious hackers who want to develop an evil twin access point and let new users connect to the SSID.

**Metasploit**

Metasploit is an application that provides security vulnerabilities and helps penetration testers look for system weaknesses. With commands such as Nmap, Metasploit was able to list all the ports that were open and corresponding services. Additional commands such as “-sV” and Metasploit display the version each port is on. From there, the malicious hacker or penetration tester can use the auxiliary database and tailor their attacks to the version the ports are on. Metasploit can help me determine what vulnerabilities I may have in my system by trial and error. I would first use Nessus to correct all my vulnerabilities and then use Metasploit to see if I can enter my system.

**Splunk and SolarWinds**

Splunk and SolarWinds were not directly added to my virtual lab environment, but they were tools I used at an enterprise level in this course. These two network visualization applications help me monitor extensive data throughout the network and create visual aids such as graphs, charts, and trendlines. These security tools can play a role in my virtual environment by using Security Information and Event Management (SIEM) to analyze network or log recordings.

**Surveillance and Reconnaissance Process**

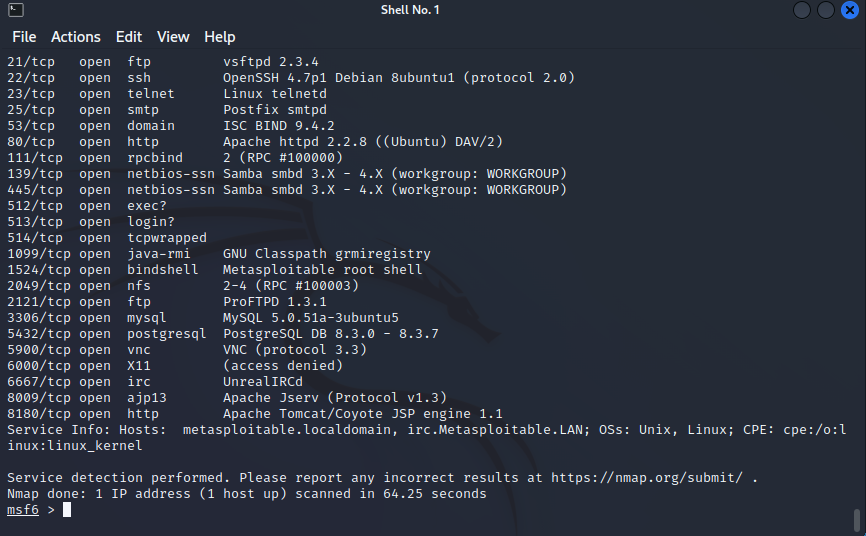
**Network Scanning**

The command to network scan a host and determine the operating system is “Nmap.” You first must know the IP address of the host you are scanning. This is where additional tools, such as Kismet, are useful for wireless attacks. Nmap can do a ping sweep on an IP range on a network. Since I used Nmap in my virtual lab environment, I knew the IP address.



**Launching an Exploit Payload**

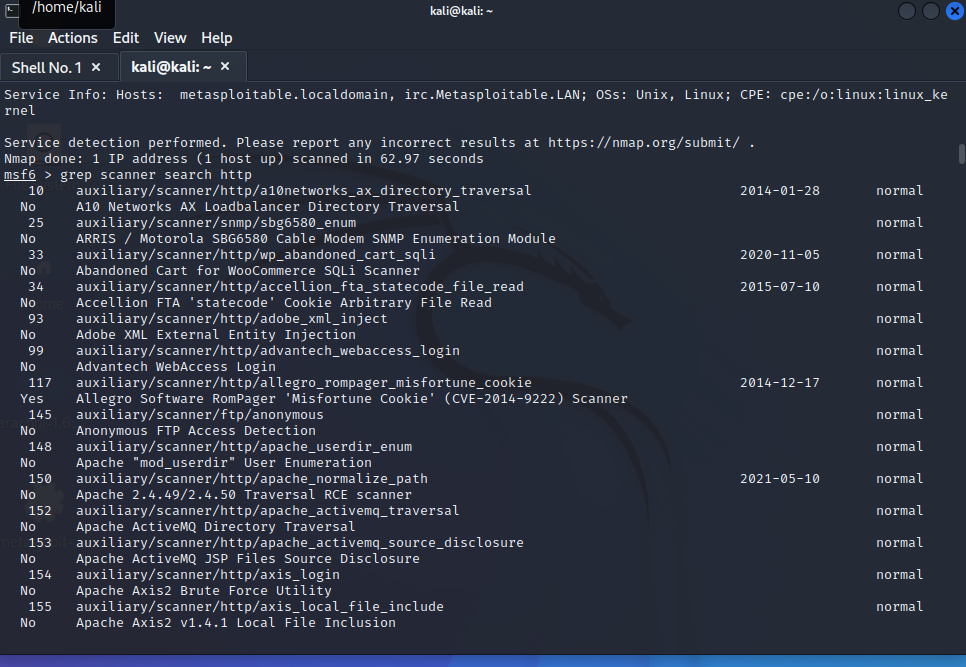
While using the Metasploit application, I could launch exploit payloads to the target host. I started by using the “Nmap -Pn -sV” command to discover the open ports' versions on my target IP address.



Once the ports are discovered with their corresponding versions, you may choose which one to attack.

The command “grep” is an acronym for global regular expression print. This command allows me to search and match patterns in a chosen text file.

The following screenshot expresses “grep scanner search http.”

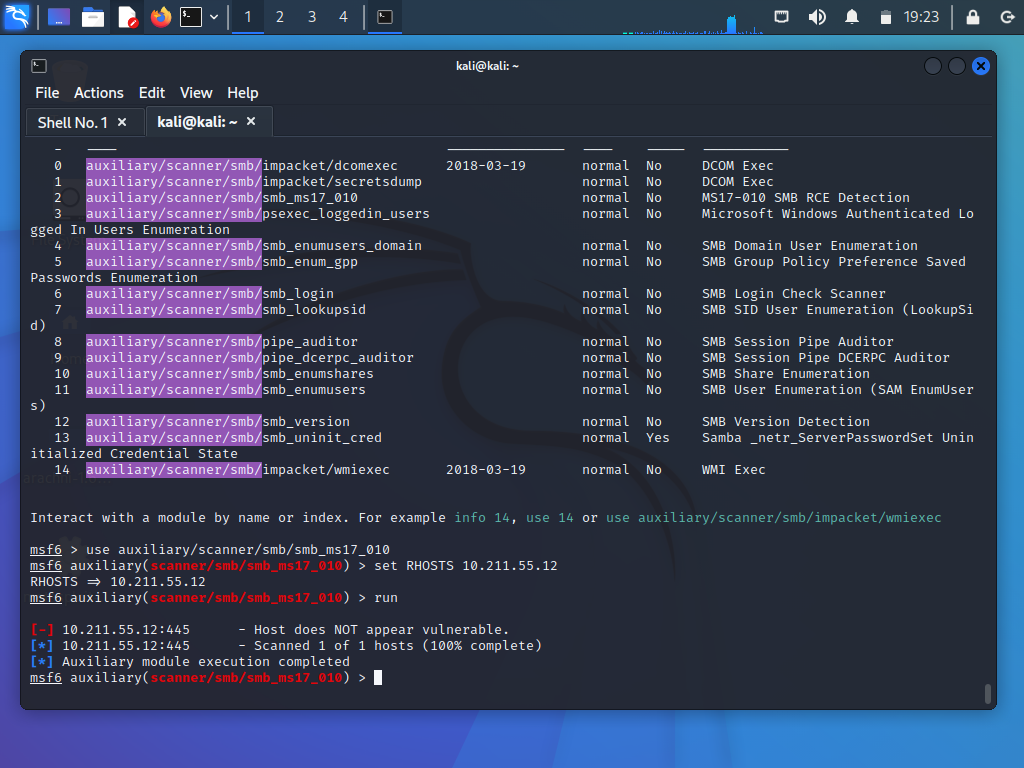


The “grep scanner search http” results will display, and you can choose from any of these databases.

Once the payload has been identified, you execute the command by setting the RHOST.

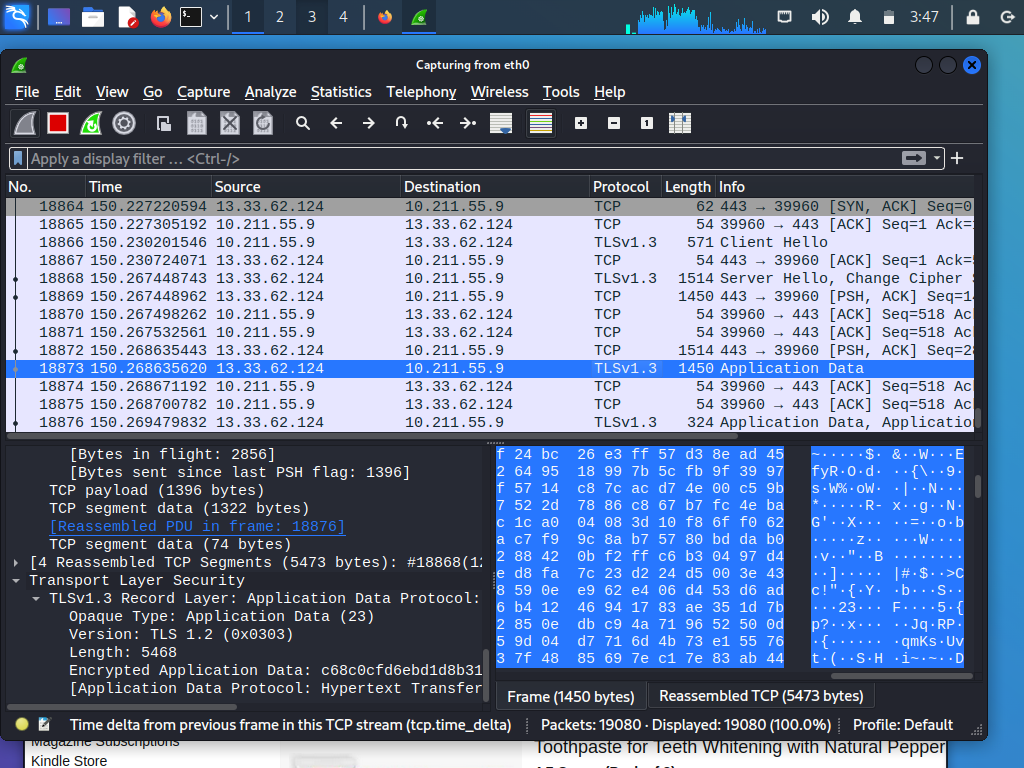
RHOST is the target IP you would like to attack with the payload.

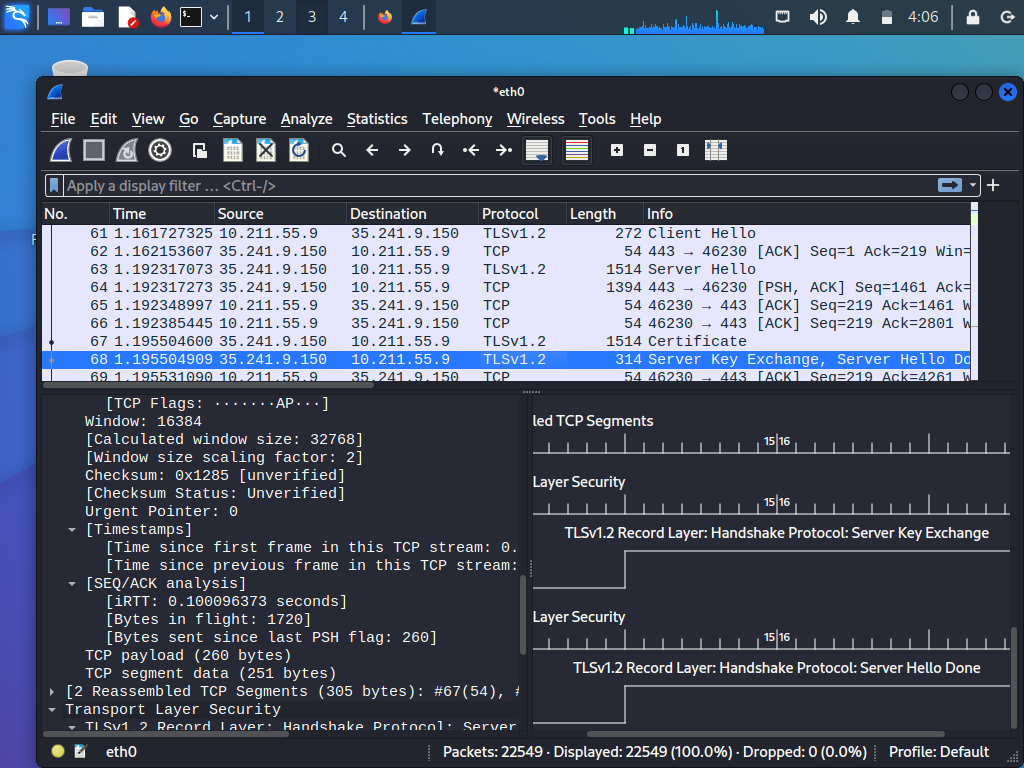
Once the RHOST is set, the command to execute the payload is “run.”



**Port Listening and Eavesdropping**

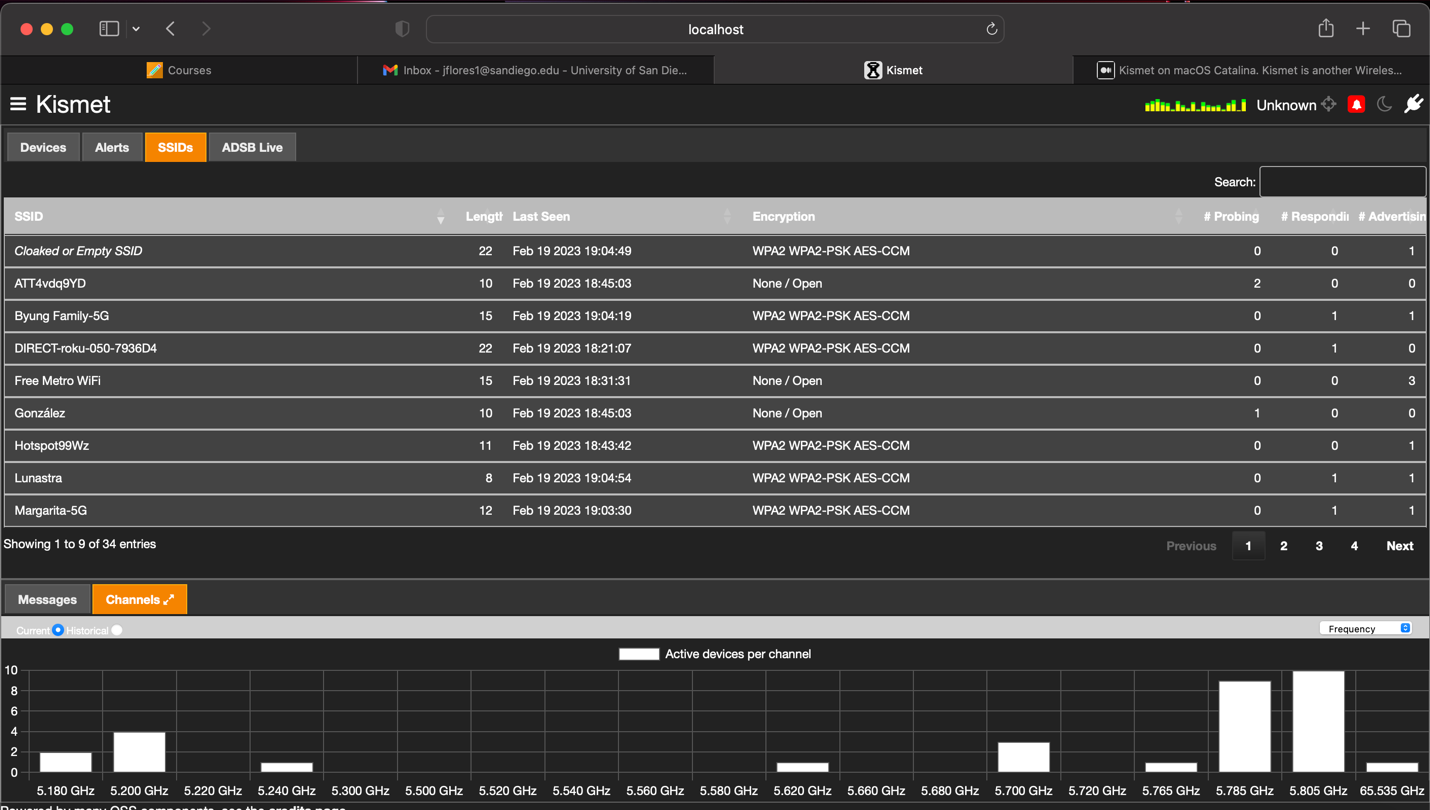
The command to listen to ports is “netstat,” but Wireshark also gives you the resources to listen. Wireshark has a web interface with a search filter that allows you to place what ports you want to see and analyze the packets being traded. The exchanged messages will come encrypted if the communication has a secured protocol. Eavesdropping between the two hosts was possible, but they could not understand the exchange due to the encryption.





**Active SSID**

The Kismet web interface displayed all the SSID nearby. No command was needed to display the SSID because the web interface has a tab that displays all the SSID locally and provides the encryption protocol.



**Lesson Learned**

The virtual lab environment is critical when learning to use new tools, explore new settings, or practice what has been learned. After the fifth week, I learned to implement redundancy best practices because a couple of times, my virtual machine would crash or stop working because I misconfigured the system by trying to install the applications or exploit my system. I now understand the reasoning behind launching new software in a Sandbox virtual setting because it can ruin settings and destroy files within the platform. Setting up the virtual lab environment was a learning experience because I explored imaging, configuring networks, and security tools.

The security tools I explored in these lab environments are powerful in their unique ways. Combining these tools can create a strong defense or penetration toolkit, depending on the role. As a penetration tester, I can exploit a wireless device with SolarWinds, Kismet, and Metasploit applications. SolarWinds will allow me to see the discovered WAP and its corresponding IP address. Kismet finds the local devices with their MAC address and the manufacturer. Knowing the manufacturer and the IP address, I can use Metasploit to look for vulnerabilities in that manufacturer and send a payload. Other attack methods I can use are Wireshark and Kismet. Knowing the SSID of the local devices, I can either do an evil twin method or a MAC spoof. I can inspect the packets using Wireshark, and because they are using my access point, I can remove the encryption protocol.

These tools can improve the system's defense by using them individually or together. SolarWinds can provide a visual aid for unusual traffic on a network. Combining it with Wireshark, I can see what packets are being sent and where they are coming from while creating a visual aid. Nessus or OpenVAS provides a list of vulnerabilities in the system by comparing it to the CVE database. These vulnerabilities are as simple as outdated software, unusual configuration, or missed patches. Running either application and then using Metasploit to exploit that vulnerability will increase the system's defenses by checking if it is still vulnerable.

As a Chief Information Security Officer (CISO), I can develop and implement security policies and procedures after learning about exploitation in our systems and networks. These policies and procedures can improve an organization's incident response and disaster recovery planning by utilizing the tools learned in the labs. Daily vulnerability scans with Nessus/OpenVAS can ensure we are up to standard with the latest CVE database. SolarWinds/Splunks can create a visual aid I may present to the board of directors to explain the network activity in the organization. Lastly, using Wireshark, I can use to investigate an incident by examining the traffic surges or packets exchange.

Depending on the duties, these security tools can be used in an offensive, defense, or executive role. The offensive role can utilize the appropriate tools to exploit the weaknesses or flaws in the system. The defensive position can use the tools to correct or examine vulnerabilities before a malicious hacker exploits them. The executive role can approve these tools for incident response, disaster recovery, and offensive or defensive positions in the organization.

**References**

CompTIA. (n.d.). *What is Wireshark and how to use it: Cybersecurity: Comptia*. CompTIA. Retrieved February 26, 2023, from https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it

Kerner, S. M., & Oladimeji, S. (2022). *Solarwinds Hack explained: Everything you need to know*. TechTarget. Retrieved February 25, 2023, from https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

SolarWinds. (n.d.). *Network performance monitor - onsite & remote monitoring*. SolarWinds. Retrieved February 25, 2023, from https://www.solarwinds.com/network-performance-monitor

Splunk. (n.d.). *Pricing FAQ*. Splunk. Retrieved February 25, 2023, from https://www.splunk.com/en\_us/products/pricing/faqs.html

Tenable. (2023). *Tenable Homepage*. Tenable®. Retrieved February 26, 2023, from https://www.tenable.com/products/nessus