**Final Project**

Angelica Y. Meza

Department of Professional and Continuing Education, University of San Diego

CSOL 570: Network Visual/ Vulnerability

Dr. Michelle Moore

August 16, 2021

**Table of Contents**

1. Introduction …………………………………………………………………………………….3

2.Trade Studies…………………………………………………………………………………...3

3. Virtualized Test Lab Architecture……………………………………………………………...7

4. Security Toolkit and Surveillance and Reconnaissance Processes …………………………….7

5. Lessons Learned and Final Thoughts…………………………………………………………13

References………………………………………………………………………………………..15

**Final Project**

**1. Introduction**

Often cybersecurity professionals lack of hands-on experience that could help them succeed in this ever-changing field. Every ethical hacker must have a place to practice and explore so beginners could understand how the theoretical knowledge of responding to a threat fit into a penetration test's grand scheme. According to Thomas (2014), most seasoned security professionals accomplished hands-on experience by getting exposure to real-life situations by creating a personal "hacking lab." The purpose of this assignment is to create a hacking lab to sharpen my skills when using different scanning tools, network visualization tools within a virtual machine. This hacking lab will provide a free environment to explore different tools and techniques without fearing an actual attack on the network.

**2. Trade Studies**

Setting up a hacking lab is vital as it is one of the most effective ways to learn and master the basics of penetration testing. In this test lab I used an Oracle Virtual Box which is a free open-source hosted hypervisor that allowed me to download the following Virtual Machines:

**Kali Linux Virtual Machine:** Kali Linux a security-testing platform. Kali Linux runs separate from the host, which allowed me to interact with other virtual machines on the network. Kali comes with several tools for penetration testing. Some of the tools that I used were Wireshark Kismet and Nmap.

Text

Description automatically generated

**Metasploitable Virtual Machine:** Metasploitable is an intentionally vulnerable Linux virtual machine. The Metasploit framework is a powerful tool that cybercriminals and ethical hackers can use to probe systematic vulnerabilities on networks and servers (Petters, 2020). Metasploit could be used in most operating systems due to its open-source framework, and it is considered the leading and most used pen-testing tool.

This is how I used Metasploit:

Launching Metasploit

Text

Description automatically generated

Searching for vulnerabilities: search name: microsoft type: exploit- The search command cold be run with a keyword to search for a specific author, an OSVDB ID or a platform.

Graphical user interface, text

Description automatically generated

show payloads: The use of this command allowed me to return a list of compatible payloads for the exploit.

Text

Description automatically generated

show all exploits of the metasploit framework- The show options command showed the available parameters for an exploit if used when the command line is in exploit context. Graphical user interface, text

Description automatically generated

When all the required options have been set for the exploit, the exploit can be executed by using two commands: run and exploit. Just type run or exploit in the msfconsole and the exploit will run.

**OWASP Webgoat Virtual Machine:** WebGoat is an insecure application that allows developers to test vulnerabilities located in Java-based applications that use open-source components. I found this VM a bit more difficult to learn.

**3. Virtualized Test Lab Architecture**

Virtual machines emulate real computers. By using a virtual machine, I was able to emulate different computers with different OS’s on a physical computer. In this case I was running a Linux OS on a Windows PC.

Diagram

Description automatically generated

**4. Security Toolkit and Surveillance and Reconnaissance Processes**

**NMAP:** Nmap is a free and open-source network scanner that I used to discover hosts and services on a computer network by sending packets and analyzing the responses (Nmap, 2010). Some of its features includes probing computer networks, and service and operating system detection.

How did I use Nmap?

I ran NMAP and began scanning the Metasploitable VM to identify open ports on the machine. I noticed that some of the ports were open:

21/tcp, 22/tcp, 23/tcp, 25/tcp, 80/tcp, 111/tcp, 139/tcp, 445/tcp, 512/tcp, 513/tcp, 514/tcp, 1099/tcp, 1524/tcp, 2049/tcp, 2121/tcp, 3306/tcp, 5432/tcp, 5900/tcp, 6000/tcp, and 6667/tcp.

**Grafana:** Grafana is a visualization tool that allows the user to see and analyze all the metrics in one unified dashboard. Usually, organizations use Grafana when (Campion, 2020):

Need annotated graphs.

Have multiple logs and need to see them in one place.

Need to share the dashboards across the organization.

Need to reorganize information based on specific team needs.

Need an easy-to-use query builder.

Need alerting for events.

I visited <https://www.itpanther.com/> for a quick tutorial on how to install Grafana.

On my Kali Linux terminal emulator, I typed the following commands:

I had to run: sudo apt-get install -y adduser libfontconfig1 to be able to install Grafana.

After that, I ran: wget <https://dl.grafana.com/oss/release/grafana_6.7.3_amd64.deb>

Text

Description automatically generated

To start Grafana, I typed the following command:sudo systemctl start grafana-server.service

Right after that, I typed the IP address and the default port number, which is 3000.

**Nagios:** Nagios is a software for server, network, and log monitoring. Nagios can monitor applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Nagios also offers capacity planning and snapshot configurations. Nagios is used when organizations (Campion, 2020):

Want to monitor servers

Want to monitor networks

Want to monitor applications

Need Windows or Linux monitoring

Need log monitoring

I did not install Nagios in my VM because I chose to work with Grafana instead. However, I did my research and seems to be a good option for selecting a Network Visualization tool.

**Wireshark**: Wireshark is a network protocol analyzer or an application that captures packets from a network connection from any home, office computer, or internet (CompTia, 2021). I used Wireshark to test the network and achieve the following:

Packet Capture: Wireshark can listen to a real-time network connection and capture the entire traffic stream.

Filtering: Wireshark can sort out all random live data received by using filters.

Visualization: Wireshark allows to visualize conversations and network streams.

After configuring the network adapter, I proceeded to download and launch Wireshark by using the following sequence:

$ sudo apt-get install wireshark

$ sudo dpkg-reconfigure wireshark-common

$ sudo usermod -a -G wireshark $USER

$ newgrp wireshark

IP Packets Captured:I selected my network interface as WiFi, and then I pressed the start button to begin to capture packets. Once I captured the packets I wanted, I pressed the stop button. Now I have created a static packet to investigate.

Graphical user interface, text, application, email

Description automatically generated

Capturing TCP Packets. Wireshark allows capturing traffic on the selected IP addressed or any selected port.

Graphical user interface, application, table

Description automatically generated

There are not many tools available for Security Engineers and IT professionals that incorporate a complete network packet capture tool. Wireshark capabilities to capture network packets and break them down in real-time or filter for offline analysis are extremely helpful. Security Engineers could use this tool to inspect and filter the network’s traffic and zoom into the root of the problem by assisting security professionals with advanced network analysis and network security. To get the most benefit out of Wireshark, a security professional should have basic understandings of several protocols such as TCP, UDO, DHCP, and ICMP.

**Nessus:** Nessus is a software for vulnerability assessment. Nessus performs inspections that aid security professionals in identifying vulnerabilities such as missing patches, malware, and misconfigurations (Capterra, 2018).

Pros

Free version and a product trial.

On point-in-time assessments to help identify vulnerabilities, such as software flaws, missing patches, malware, and misconfigurations.

Low price and affordable for organizations. The initial purchase is $1,500.

Customizable and flexible reporting.

Vulnerability scanning of network including IPv4 network and IPv6 network.

Capable of scanning all network devices connected.

Easy to find patching solutions.

Cons

Nessus is available for free, but the free version has some restrictions. The free version does not allow to perform internal/external PCI scan policies and configure audits.

The Nessus professional version is pricy and cannot be afforded by anyone.

Nessus does not display the scan status while the scan is ongoing.

The Nessus Pro version is limited to one user.

Nessus does not support scans for machines with 2-factor authentication implemented on it.

The final scan result showed several vulnerabilities by severity. I was able to use the Exploit DB tool on the Kali Linux VM. I searched for vulnerability MS08-067. Exploit DB showed me the code for that vulnerability. I also googled the vulnerability mentioned above, and Rapid7's site gave a good explanation of the meaning of that particular vulnerability.

A picture containing Word

Description automatically generated

**Kismet**: Kismet is an open-source tool for wireless sniffing. Kismet supports wireless network scanning and intrusion detection. Kismet can monitor traffic by displaying all the packets it captures.

Launching Kismet by: Logging into Kali Linux>Wireless Attacks>Launch Kismet>Type Kismet

Text

Description automatically generated

I got a message saying that Kismet could not capture data until a capture interface is added. After that I added the interface -wlan0. I started the server and immediately started seeing traffic detected and the mac addresses-names for the interfaces.

Graphical user interface

Description automatically generated

I was able to see the wireless card connected, the packets received and which channel they are connected to.

I researched Google to find other valuable commands and to learn how to better navigate Kismet. I went to <https://tools.kali.org/wireless-attacks/kismet> and <https://www.shorttutorials.com/apt-get-commands/man-kismet.html> where I learned more about Kismet capabilities and their commands. I do see the importance of learning how to use this tool. Throughout my research, I learned that there are three common paths to using Kismet: MAC address spoofing, packet injection and wireless encryption protection (WEP) cracking.

**5. Lessons Learned and Final Thoughts**

Technology is rapidly advancing, and more vulnerabilities are being exposed and exploited by malicious criminals. I learned that wireless network must be secured with WPA2 encryption, channel control and a strong, non-default password. Security professionals must familiarize themselves with valuable pen testing tools such as Kismet, Nessus or Wireshark. These tools are robust pen testing tools capable of performing an extensive array of tasks. A basic understanding of any visualization tool or network scanning could help cybersecurity professional understanding network vulnerabilities and watch if any attacker has any malicious intension as

running a vulnerability scan will show the network’s issues so the system administrator can quickly patch and adjust the system's vulnerabilities to improve security.

**References**

Campion, N. (2020). *Grafana vs. Nagios | MetricFire Blog*. Metricfire.com. Retrieved 13 August

2021, from <https://www.metricfire.com/blog/grafana-vs-nagios/>.

Capterra. (2018). Retrieved 14 August 2021, from

<https://www.capterra.com/p/130577/Nessus/reviews/>.

CompTia. (2021). *What Is Wireshark and How to Use It | Cybersecurity | CompTIA*. Default.

Retrieved 13 August 2021, from <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>.

GVS, C. (2020). *Things to Consider While Choosing The Right Vulnerability Assessment Tool*.

Appknox.com. Retrieved 14 August 2021, from <https://www.appknox.com/blog/choosing-the-right-vulnerability-assessment-tool>.

G2. (2020). Retrieved 14 August 2021, from

<https://www.g2.com/categories/vulnerability-scanner>.

Nessus. (2021). *Nessus Product Family*. Tenable®. Retrieved 13 August 2021, from

<https://www.tenable.com/products/nessus>.

Infosec Aphorisms. (2018). *Discover Wireless Networks with Kismet*. Youtube.com. Retrieved

13 August 2021, from <https://www.youtube.com/watch?v=IBzUIgTwuYE>.

ITPanther. (2020). *Installing Grafana on Linux - Step by Step With Example*. IT Panther.

Retrieved 14 August 2021, from <https://www.itpanther.com/installing-grafana-on-linux/>.

Kali Linux. (2021). Retrieved 14 August 2021, from <https://www.kali.org/get-kali/>.

Kershaw, M. (2021). Tools.kali.org. Retrieved 13 August 2021, from

<https://tools.kali.org/wireless-attacks/kismet>.

Kioptrix. (2010). *Kioptrix: Level 1 (#1)*. Vulnhub.com. Retrieved 13 August 2021, from

<https://www.vulnhub.com/entry/kioptrix-level-1-1,22/>.

Mallory, P. (2020). *Ethical hacking: Wireless hacking with Kismet - Infosec Resources*. Infosec

Resources. Retrieved 15 August 2021, from <https://resources.infosecinstitute.com/topic/ethical-hacking-wireless-hacking-with-kismet/>.

Metasploitable 2. (2021). *Metasploitable 2 | Metasploit Documentation*. Docs.rapid7.com.

Retrieved 14 August 2021, from <https://docs.rapid7.com/metasploit/metasploitable-2/>.

Nmap. (2010). *Chapter 9. Nmap Scripting Engine | Nmap Network Scanning*. Nmap.org.

Retrieved 13 August 2021, from <https://nmap.org/book/nse.html>.

OpenManiak. (2008). *Kismet - The Easy Tutorial - Installation*. Openmaniak.com. Retrieved 13

August 2021, from <https://openmaniak.com/kismet_install.php>.

Oracle. (2013). *6.4. Installing the VirtualBox Guest Additions*. Docs.oracle.com. Retrieved 13

August 2021, from <https://docs.oracle.com/cd/E36500_01/E36502/html/qs-guest-additions.html>.

OWASP Broken Web Applications Project Download. (2021). *OWASP Broken Web*

*Applications Project*. SourceForge. Retrieved 14 August 2021, from <https://sourceforge.net/projects/owaspbwa/>.

Petters, J. (2021). *How to Use Wireshark: Comprehensive Tutorial + Tips | Varonis*. Inside Out

Security. Retrieved 14 August 2021, from <https://www.varonis.com/blog/how-to-use-wireshark/>.

Petters, J. (2020). *What is Metasploit? The Beginner's Guide - Varonis*. Inside Out Security.

Retrieved 13 August 2021, from <https://www.varonis.com/blog/what-is-metasploit/>.

Rapid7. (2021). *Cybersecurity & Compliance Solutions & Services | Rapid7*. Rapid7. Retrieved

14 August 2021, from <https://www.rapid7.com/>.

Rapid7. (2021). *Metasploitable 2 Exploitability Guide | Metasploit Documentation*.

Docs.rapid7.com. Retrieved 14 August 2021, from <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide>.

Shapiro, J. (2020). *What Is Vulnerability Scanning And Why Is It Important?*.

Blogs.iuvotech.com. Retrieved 14 August 2021, from <https://blogs.iuvotech.com/what-is-vulnerability-scanning-and-why-is-it-important>.

Shorttutorials.com. (2016). Retrieved 14 August 2021, from <https://www.shorttutorials.com/apt->

get-commands/man-kismet.html.

Skedler. (2021). *Everything you need to know about Grafana - Skedler*. Skedler. Retrieved 14

August 2021, from <https://www.skedler.com/what-is-grafana-why-use-it-everything-you-should-know/>.

Stackshare. (2021). *Grafana vs Nagios | What are the differences?*. StackShare. Retrieved 14

August 2021, from <https://stackshare.io/stackups/grafana-vs-nagios>.

Thomas, V. (2014). *Ethical Hacker - an overview | ScienceDirect Topics*. Sciencedirect.com.

Retrieved 12 August 2021, from <https://www.sciencedirect.com/topics/computer-science/ethical-hacker>.

TechSpertise TV. (2018). *How To attach USB WIFI ADAPTER in virtualbox, with KALI LINUX*

*| VB2*. Youtube.com. Retrieved 14 August 2021, from <https://www.youtube.com/watch?v=UdWm4DhwuaY>.

VirtualBox. (2021). *Oracle VM VirtualBox*. Virtualbox.org. Retrieved 14 August 2021, from

<https://www.virtualbox.org/>.

Walsh, E. (2014). *Connect USB Wireless Adapter to Kali Linux in Virtualbox*. Youtube.com.

Retrieved 15 August 2021, from <https://www.youtube.com/watch?v=K1ETBeRQBs4>.

Wireshark. (2021). *Wireshark · Go Deep.*. Wireshark.org. Retrieved 15 August 2021, from

<https://www.wireshark.org/>.

YouTube. (2021). *How to Install Nessus in Kali Linux* [Video]. Retrieved 14 August 2021, from

<https://www.youtube.com/watch?v=2Pnr_UAgrqg>.