ASSIGNMENT REPORT 2: VMWARE KALI MACHINE

CENG 3544, COMPUTER AND NETWORK SECURITY

Ahmet Oral
ahmetoral@posta.mu.edu.tr

Monday 7th June, 2021

Abstract

This lab assignment report contains the steps of download and installation of the Kali Linux machine, examination of the tools in this machine and obtaining information about the services on the "victim" machine running in parallel using Nmap. Kali Linux is installed as virtual machine on Windows OS using Wmvare Workstation which uses virtualization technology and allows running multiple operating systems in a virtual environment. Our victim machine is Ubuntu, which is a Linux OS based on Debian and also created as virtual machine on Vmvare Workstation.

1 Introduction

In this lab assignment, my goal is to learn as much as I can about these operating systems, tools included in it and be able to determine which tools can be used for certain types of tasks and what are the benefits of using Kali Linux machine. Because I am also using a victim machine I will also observe weaknesses and security threats that can be exploited by attackers.

2 Assignments

Lab assignments consists of three main tasks:

- Downloading and Installing Kali Linux Machine on Wmvare
- Examining Tools on Kali Linux
- Gathering Information about Victim Machine Using Nmap

Detailed explanation of how each of these tasks solved and which steps are taken to solve them are shown below.

2.1 Assignment 1 - Installation of Kali Linux Machine on Wmvare

Kali Linux is a Debian-based Linux distribution which is mainly used for advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

Wvmare is a virtualization software that enables users to create and run virtual machines directly on a single Windows or Linux computer. Those machines can run simultaneously with the physical machine. Each machine runs its own OS such as Windows or Linux. In this assignment we will install Kali Linux.

Kali Linux official website has a download option that have Vmvare pre-built images, which allows installing Kali without altering host OS with additional features such as snapshots. Installing this version of Kali is very simple because it's a pre-built image. Installation can be completed by just opening this image on Vmware Workstation. Steps of the installation are;

1)Downlading Vmware pre-built Image of Kali Linux

Kali Linux official website has a download option that have Vmvare pre-built images, which allows installing Kali without altering host OS with additional features such as snapshots. Installing this version of Kali is very simple because it's a pre-built image. Installation can be completed by just opening this image on Vmware Workstation. This pre-built image can be downloaded from website shown in below.

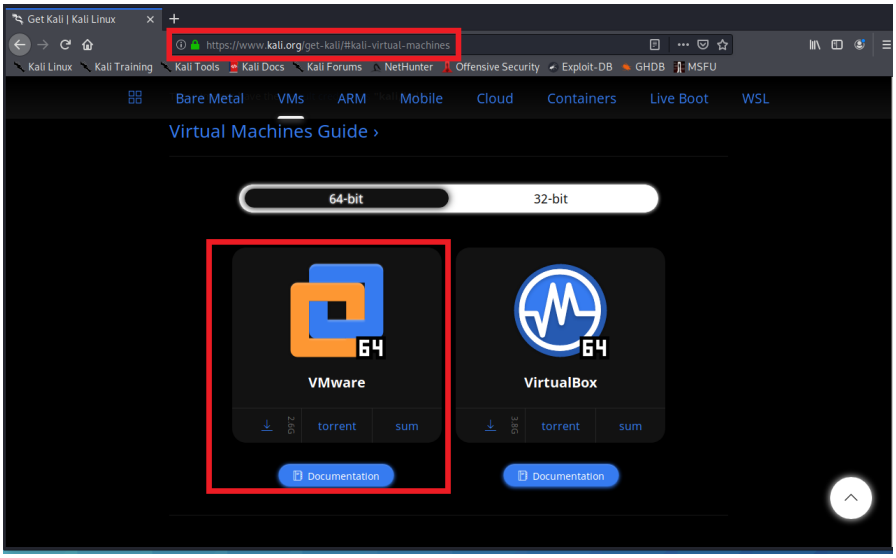
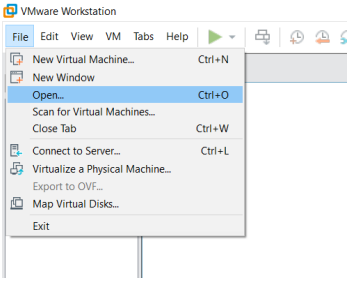
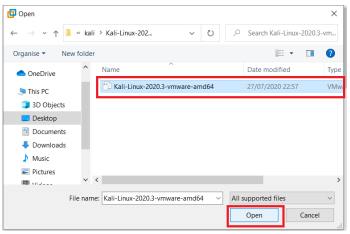


Figure 1: Kali Linux Pre-Built Image File Download

2)Installing Kali Linux Virtual Machine on Wmvare



Open Vmvare Workstation and click open.



Select the configuration file in the folder we downloaded from ”kali.org” .

After clicking open, Kali Linux VM is visible in Vmware Workstation. Settings of the machine can be changed. Amount of memory, cores, wifi connection and all technical system settings can be configured on this page.

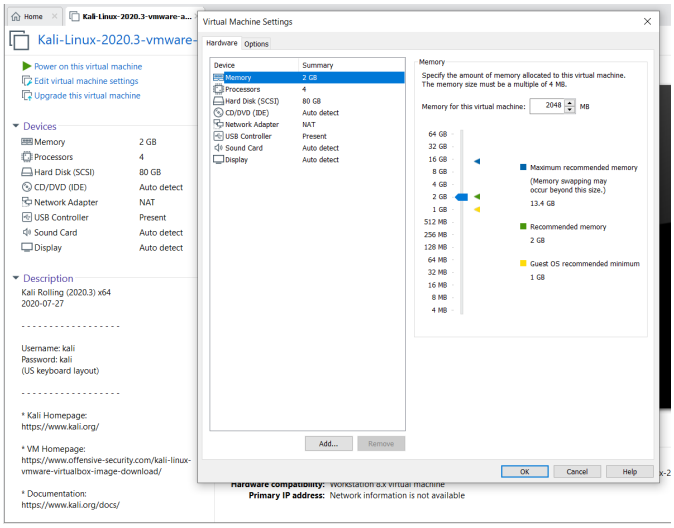


Figure 2: Virtual Machine Settings Configurations

Kali Linux will start after clicking ”Power on this virtual machine”. The default username and password for Kali Linux is ”kali”. After logging into the system Kali Linux is operational and we can use it to complete other tasks in this assignment.

2.2 Assignment 2 - Examining Tools on Kali Linux

Tools are used to automate tasks to achieve efficiency and save time while performing penetration testing or hacking as there could be thousands of conditions and payloads to test and testing them manually is a difficult task. These tools not only saves time but also captures the accurate data and output the specific result.

Kali Linux comes packed with more than 350 tools which could be useful for hacking or penetration testing.There are different types of tools that are present in Kali Linux to perform different operations. Different usage areas for operations and and some of the best tools that can be used to execute these operations are shown below.

Information Gathering

These tools are used to scan, collect and format the data in a form that could further be used. This step is very important because, to perform a successful attack, one must know as many as possible about their target.

Information Gathering Tools:
-Nmap (Most famous one)
-Zenmap
-Stealth Scan

Vulnerability Analysis

Vulnerability is being open to the possibility of being attacked or exploited. These tools are used to check a system or machine for any kind of flow or vulnerability available in them, which could lead to any security breach and data loss. These tools can be also used help in fixing those vulnerabilities by identifying them.

Vulnerability Analysis Tools:
-Bed
-Ohrwurm
-Powerfuzzer
-Sfuzz

Password Attacks

These are basically a collection of tools that could handle the wordlist or password list to be checked on any login credentials through different services and protocols. Some tools are wordlist collectors and some of them are the attacker.

Password Attack Tools:
-Hydra
-Hashcat
-John the Ripper(Most famous one)
-Medusa

Wireless Attacks

These tools are wireless security crackers, like breaking wifi – routers, working and manipulating access points. Wireless attacks are not limited to password cracking these are also used in information gathering and knowing behavior of victims over the internet. For example, the Victim is connected to a compromised access point or a fake access point then it can be used as a Man-in-The-Middle attack.

Wireless Attack Tools:
-Aircrack-ng(Most famous one)
-Fern- wifi –cracker
-Kismet
-Ghost Phisher

Exploitation

These tools are used to exploit different systems like personal computers and mobile phones. They can generate payloads for the vulnerable system and through those payloads information from the devices can be exploited. For example, the Victim's system is compromised using payloads over internet or installing it if physically accessible.

Exploitation Tools:
-Armitage
-Metasploit(Most famous one)
-Searchsploit
-Beef xss framework

Social Engineering

These tools generate similar services that people use in daily life and extract personal information using those fake services. These tools use and manipulate human behavior for information gathering. For example, Phishing is one of the example of social engineering, a similar looking home page of any social platform can be created and login details of the victim using this page can be compromised.

Social Engineering Tools:
-SET(Most famous one)
-Backdoor-f
-U3-pwn
-Ghost Phisher

2.3 Assignment 3 - Gathering Information about Victim Machine Using Nmap

Nmap is an open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyzes the responses in order to produce the desired results. It could even be used for host discovery, operating system detection, or scanning for open ports. It is one of the most popular reconnaissance tools and comes pre-installed with Kali Linux.

The task is to gather information about victim machine. The victim machine is another virtual machine that is co-running with Kali Linux in same host OS. With this information, we can start our analysis.

Step 1- Get the IP Range/Subnet Mask of the Network

We know that our victim machine is on the same network with us. In order to know the devices that are connected to our network, we first need to get the IP range or the subnet mask of our network.
In order to get information about the network our system is connected to, we need to execute command below:

```
$ ip address
```

Result after executing this command is shown in the image below.

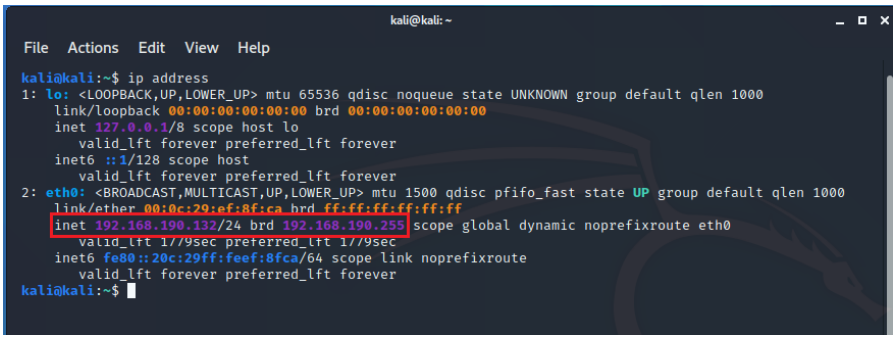


Figure 3: Information of the Network

The Ip within the red rectangle indicates that our system is using 192.168.190.0 subnet mask and the range is 255. Thus our network IP range is from 192.168.190.0 to 192.168.190.255.

Step 2 - Scan network for connected devices

Now that we know the subnet mask Ip, we can use it through the Nmap tool to scan the report of all devices connected to the network. For this operation we will perfom a Ping Only Scan:

```
$ nmap -sP 192.168.190.0/24
```

Result after the executing scan is show in the image below.

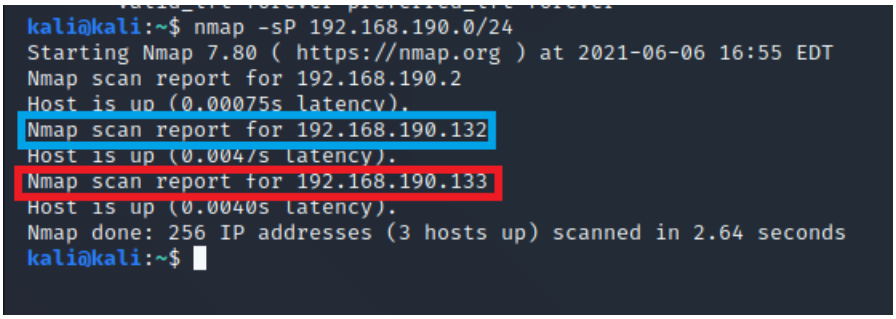


Figure 4: Ping Only Scan Results

The output shows that there are 3 devices connected on the network; one is the router itself, one is the Kali Linux I am using(Inside the blue rectangle), and the third one is our victim machine(Inside the red rectangle). Now that we located the victim machine, we can proceed to the next step.

Step 3 - Gathering Information

First, we want to see if the server is answering to a ping or if the host is up.(From the last step, we already know that our target is online and responsive, but there is no harm checking it before scanning because scan may take in another time of the day or etc.) We will do this by performing a TCP NULL Scan:

```
$ nmap -sN 192.168.56.102
```

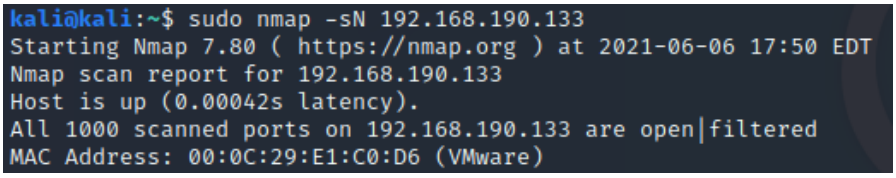


Figure 5: Null Scan Results

We can see that our target is online and we can proceed to the next step. Which is to scan services running in the victim machine. We can do this scan by running Service Version Detection command:

```
$ nmap -sV 192.168.56.102
```

Output will be:

```
kali@kali:~$ sudo nmap -sV 192.168.190.133
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 18:56 EDT
Nmap scan report for 192.168.190.133
Host is up (0.00062s latency).
Not shown: 995 filtered ports
PORT    STATE  SERVICE  VERSION
20/tcp  closed ftp-data
21/tcp  open   ftp      vsftpd 3.0.3
22/tcp  open   ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp  open   http     Apache httpd 2.4.41 ((Ubuntu))
443/tcp closed https
MAC Address: 00:0C:29:E1:C0:D6 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.21 seconds
kali@kali:~$
```

Figure 6: Service Version Detection Results

As seen in the image above, we perfomed an Nmap scan for 192.168.190.133 (Victim machine) and it is successful. We can see that there are 3 open ports; 20/tcp, 21/tcp and 22/tcp, which are ftp, ssh, http services. These are the services we installed in our first lab assigment. We can also see versions of these services. Another information available is the operating system of the target, which is linux, and it's Mac Address.

3 Conclusion

In this lab assignment I examined the tools in Kali Linux and learned usage areas of these tools and what are their purposes. I also learned how to use some of them bu I didn't included it in the report because the report is already too long. I did some experiments between the Kali machine and Ubuntu machine. I observed the weaknesses and exploitable services in linux OS. Lastly I learned to use Nmap and scanned target machine to gather information. I also did some experimenting with Nmap and tried it's other usage areas and different commands, which I think it's really cool.