ASSESSEMENT 02 (CONFIGURE HACKER LAB USING VIRTUAL BOX)

Prepared by: Dhilipan Kumar P

Date: 03/03/2024

Executive Summary:

This report outlines the process of configuring Kali Linux and Metasploitable 2 virtual machines using VirtualBox, utilizing the NAT (Network Address Translation) tool for network connectivity. The setup allows for the creation of a secure testing environment for educational and penetration testing purposes.

Introduction:

VirtualBox is a widely-used virtualization software that enables users to run multiple operating systems simultaneously on a single physical machine. In this configuration, we aim to deploy Kali Linux, a powerful penetration testing platform, alongside Metasploitable 2, a purposely vulnerable virtual machine, within VirtualBox. The utilization of the NAT tool facilitates network communication between the virtual machines and the host system.

Procedure:

Step 1

VirtualBox Installation:

- Download and install VirtualBox from the official website, ensuring compatibility with the host operating system.

Step 2

Download Kali Linux and Metasploitable 2:

- Obtain the necessary virtual machine images for Kali Linux and Metasploitable 2 from reputable sources. Ensure the integrity of the downloaded files.

Step 3

Import Virtual Machines:

- Launch VirtualBox and import the downloaded virtual machine files.
- For each VM, go to "File" > "Import Appliance," then select the respective VM file and follow the import wizard.

Step 4

Configure Network Settings:

- Select each virtual machine from the VirtualBox manager.
- Navigate to "Settings" > "Network" and choose "NAT" as the network adapter.

- NAT enables the virtual machines to communicate with each other and the host system while remaining isolated from external networks.

Step 5

Adjust System Resources (Optional):

- Allocate appropriate CPU cores, RAM, and disk space to each virtual machine based on performance requirements.

Step 6

Start Virtual Machines:

- Select the Kali Linux and Metasploitable 2 virtual machines from the VirtualBox manager.
- Click on the "Start" button to boot up the virtual machines.

Step 7

Accessing Virtual Machines:

- Once booted, obtain the IP addresses assigned to each virtual machine.
- In Kali Linux, use tools such as nmap or ifconfig to identify the IP addresses.
- Note down the IP addresses for further interaction between the virtual machines.

Step 8

Testing and Exploration:

- Utilize Kali Linux tools to conduct penetration tests and security assessments on Metasploitable 2.
- Experiment with various exploits and vulnerabilities present in Metasploitable 2 to enhance understanding of security concepts.

Step 9

Conclusion:

The configuration of Kali Linux and Metasploitable 2 using VirtualBox with NAT provides a safe and controlled environment for learning and practicing penetration testing techniques. By leveraging the capabilities of VirtualBox and the NAT tool, users can explore cybersecurity concepts without compromising the integrity of their host systems or external networks.

Recommendations:

Regularly update the virtual machines and associated tools to ensure the latest security patches and enhancements.

Exercise caution while performing penetration tests to avoid unintended consequences and potential legal implications.

Continuously expand knowledge and skills in cybersecurity through hands-on experimentation and study.

Acknowledgments:

We extend our gratitude to the developers of VirtualBox, Kali Linux, and Metasploitable 2 for providing valuable tools for educational and security purposes.

VirtualBox Documentation: Oracle VM VirtualBox

Kali Linux Official Website: Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution

Metasploitable 2 GitHub Repository: Metasploitable - Browse /Metasploitable2 at SourceForge.net

Dhilipan Kumar P

Cyber Security Analyst

h1k0r