README.md

Cybersecurity Virtual Lab Environment

This repository details the construction and utilization of a personal cybersecurity virtual lab environment. Designed for hands-on experience, this isolated setup facilitates the practice of ethical hacking techniques, vulnerability assessments, and the implementation of defensive strategies without impacting the host system or external networks.

This project serves as a practical demonstration of proficiency in virtualization, network configuration, Linux administration, and fundamental cybersecurity methodologies.

Lab Components

The virtual lab environment comprises the following key components:

- **Virtualization Software: Oracle VM VirtualBox** is employed as the virtualization platform. Its robust, free, and open-source nature makes it an ideal choice for creating isolated lab environments.
- **Attacker Machine: Kali Linux** serves as the primary offensive platform. This Debian-based distribution is pre-loaded with an extensive suite of penetration testing and security auditing tools, enabling realistic attack simulations.
- **Vulnerable Target: Metasploitable 2** functions as the intentionally vulnerable target system. This Linux VM is specifically designed with numerous known vulnerabilities, providing a controlled environment for ethical exploitation exercises.

Network Architecture

All virtual machines within this lab are interconnected via a dedicated **NAT Network** configured in VirtualBox, named CyberLabNet. This network architecture is critical for several operational and security reasons:

- **Isolation:** All lab VMs operate within a self-contained network segment, ensuring complete isolation from the host machine's operating system and the external local area network. This containment is essential for safely conducting security experiments and simulated attacks.
- **Inter-VM Communication:** The configuration allows Kali Linux and Metasploitable 2 to communicate seamlessly within this isolated network, which is prerequisite for realistic attack scenario execution.
- **Controlled Internet Access:** While isolated from the local network, VMs within CyberLabNet can be configured to access the internet (via the host machine's

connection) for necessary updates or tool downloads, maintaining internal isolation while allowing external connectivity as required.

Setup Process Overview

The construction of this virtual lab involved the following key steps:

1. **VirtualBox and Extension Pack Installation:** Oracle VM VirtualBox and its corresponding Extension Pack were installed on the host operating system.
2. **VM Image Acquisition:** Official ISO images for Kali Linux (installer version) and the Metasploitable 2 VMDK (virtual disk image) were securely downloaded from their authorized distribution sources.
3. **Kali Linux VM Creation:** A new virtual machine for Kali Linux was configured with 4GB of RAM, 2 CPU cores, and a 30GB dynamically allocated virtual disk. Its network adapter was assigned to the custom NAT Network: CyberLabNet. A standard graphical installation of Kali Linux was then performed.
4. **Metasploitable 2 VM Preparation:** For Metasploitable 2, 1GB of RAM and 1 CPU core were allocated, and the downloaded .vmdk file was attached as the virtual disk. Critically, its network adapter was also configured to the *same* NAT Network: CyberLabNet to facilitate communication with the Kali VM. The default login credentials (msfadmin/msfadmin) were noted.
5. **Network Connectivity Verification:** Post-setup, basic ping tests were executed between the Kali Linux VM and Metasploitable 2 VM to confirm seamless network communication within the isolated lab environment.

Demonstrated Skills

This hands-on project has provided the opportunity to develop and showcase the following essential cybersecurity and technical skills:

- **Virtualization Management:** Proficiency in deploying, configuring, and managing virtual machines using industry-standard virtualization software (Oracle VM VirtualBox).
- **Network Configuration & Segmentation:** Practical understanding and implementation of basic network topologies, including isolated NAT networks and IP addressing schemes.
- **Linux OS Administration:** Demonstrated familiarity with command-line operations, file system navigation, and fundamental system management on both Kali Linux (for offensive tasks) and vulnerable Linux targets.
- **Vulnerability Assessment Fundamentals:** Gaining practical insight into identifying system weaknesses and methods for conducting initial vulnerability discovery.
- **Reconnaissance & Scanning:** Hands-on experience with network scanning

tools, such as Nmap, to enumerate open ports, services, and potential attack surfaces.
- **Ethical Exploitation:** Practical application of controlled exploitation techniques using frameworks like Metasploit against intentionally vulnerable systems, understanding the attack lifecycle.
- **System Hardening Basics:** Fundamental knowledge of securing operating systems and services to mitigate common threats and enhance system resilience.

Future Expansion Plans

My commitment to continuous learning drives the planned expansion and refinement of this lab:

- Integration of a **Windows Server VM** to practice Active Directory enumeration, privilege escalation, and domain security attacks and defenses.
- Implementation of a **Security Information and Event Management (SIEM) tool** (e.g., Splunk Free or Wazuh) to centralize log collection, monitor for suspicious activities, and analyze security events comprehensively.
- Simulation of more complex **incident response scenarios** (e.g., ransomware, data exfiltration) with thorough documentation of the detection, containment, eradication, and recovery phases.
- Ongoing development and refinement of **custom Python/Bash scripts** for automating various reconnaissance, exploitation, or defensive tasks within the lab environment.