Cybersecurity Lab Documentation

1. Overview

This documentation provides a step-by-step breakdown of the setup and configuration of a virtual cybersecurity lab used to simulate a real-world security environment. It includes the creation of two virtual machines (Kali Linux and Windows 10), internal networking setup, and connectivity testing.

2. Virtualization Tool Used

Tool: Oracle VM VirtualBox

Host OS: Windows 10 Pro

Version: 7.1

3. Virtual Machines Setup

a. Kali Linux VM

- OS: Kali Linux
- Base Memory (RAM): 3 GB
- Processors: 2
- Video Memory: 128 MB
- Storage: 20 GB (Virtual Disk)
- Network Adapter: Internal Network

SCREENSHOTS ATTACHED

b. Windows 10 VM

- OS: Windows 10 (64-bit)
- Base Memory (RAM): 3 GB
- Processors: 2
- Video Memory: 128 MB
- Storage: 25 GB (Virtual Disk)
- Network Adapter: Internal Network

SCREENSHOTS ATTACHED

4. Network Configuration

Both VMs were configured to use an Internal Network to ensure isolated communication within the lab environment. IP addresses were automatically assigned or set manually.

Find attached copies of screenshots

5. Connectivity Test

Using the terminal and command prompt, ping tests were run to verify network communication:

- Kali to Windows:
  ping 192.168.74.3

- Windows to Kali:
  ping 192.168.74.4

SCREENSHOTS ATTACHED

6. Shared Folders (Optional)

Shared folders were configured to allow file transfers between host and virtual machines.

7. Guest Additions Installation

VirtualBox Guest Additions were installed to enable features such as clipboard sharing and improved resolution.

SCREENSHOTS ATTACHED

8. Issues Encountered and Resolutions

- Issue: VirtualBox not opening initially
  Solution: Updated Windows OS to latest version.

- Issue: Blank screen during Windows ISO setup
  Solution: Disabled unattended installation and restarted setup manually.

9. Conclusion

The virtual cybersecurity lab was successfully configured with both attacker (Kali) and victim (Windows) environments communicating over an isolated internal network. This setup provides a controlled environment for penetration testing, digital forensics, and network analysis exercises.