Malware Analysis Lab

Introduction

The goal of this document is to provide a detailed guide for setting up a Malware Analysis Lab. This lab will serve as a controlled environment for examining, understanding, and mitigating the impact of malicious software. The lab supports both static analysis (examining malware without execution) and dynamic analysis (observing malware behavior during execution). Proper isolation and security measures will be emphasized to ensure the host system remains unaffected.

Objectives and Scope

- **Purpose:** Create a secure environment for analyzing malware samples without risking the integrity of the host system.
- **Scope:** Support multiple operating systems and tools to analyze a wide variety of malware types, including ransomware, trojans, and viruses.
- **Capabilities:** Enable both static and dynamic analysis using industry-standard tools and techniques.

Hardware and Software Requirements

Hardware Requirements

- **Processor:** Multi-core CPU (quad-core or higher recommended).
- **Memory:** Minimum 16 GB RAM to support multiple virtual machines (VMs).
- **Storage:** SSD with at least 500 GB capacity to accommodate OS images, snapshots, and analysis tools.
- **Network:** Dedicated network interface for isolated lab connectivity.

Software Requirements

- **Host Operating System:** A stable OS such as Windows 10, macOS, or a Linux distribution.
- **Virtualization Platform:** VMware Workstation/Fusion, Oracle VirtualBox, or Microsoft Hyper-V.
- **Guest Operating Systems:** Windows 7, Windows 10, and a Linux distribution (e.g., Ubuntu) for diverse malware analysis.
- **Analysis Tools:** Flare VM, INetSim, Sysinternals Suite, Wireshark, and Ghidra.

Setting Up the Virtual Environment

Step 1: Install Virtualization Software

- Download and install your chosen virtualization platform (e.g., VMware Workstation or VirtualBox).
- Enable hardware virtualization (VT-x/AMD-V) in your system's BIOS/UEFI settings.

Step 2: Create Virtual Machines

1. **Set Up Windows VM:**
    - Allocate 4 GB of RAM, 2 CPU cores, and 60 GB of storage.
    - Install Windows 10 or Windows 7 from an ISO file.
2. **Set Up Linux VM:**
    - Allocate 2 GB of RAM, 1 CPU core, and 40 GB of storage.
    - Install a Linux distribution (e.g., Ubuntu).
3. **Network Configuration:**
    - Configure the network to use an internal network adapter for isolated connectivity.
    - Optionally, set up a NAT network for controlled internet access.

Step 3: Install Guest Additions/Tools

- Install VirtualBox Guest Additions or VMware Tools for improved performance and shared folder support.

Installing and Configuring Analysis Tools

Flare VM Installation

1. Download the Flare VM repository from GitHub.
2. Extract the ZIP file to a directory on the Windows VM (e.g., `C:\FlareVM`).
3. Open PowerShell as Administrator and set the execution policy:

   ```
   Set-ExecutionPolicy unrestricted
   ```

4. Navigate to the extracted directory and run the installation script:

   ```
   .\install.ps1
   ```

5. Confirm prompts and wait for the installation to complete (1-3 hours).

Additional Tools

- **INetSim:** Simulates network services for analyzing malware network behavior.
- **Wireshark:** Captures and analyzes network traffic.
- **Sysinternals Suite:** Includes tools like Process Explorer and Autoruns for detailed system analysis.
- **Ghidra:** A reverse engineering tool for static analysis of malware binaries.

Best Practices for Lab Usage

- **Isolation:** Ensure all VMs are isolated from the host system and external networks unless necessary.
- **Snapshots:** Take snapshots of clean VM states to quickly revert after each analysis.
- **Resource Monitoring:** Regularly monitor resource usage to avoid performance bottlenecks.
- **Security Updates:** Keep all tools and operating systems updated to mitigate vulnerabilities.

Conclusion

By following this guide, you can set up a comprehensive malware analysis lab to safely and effectively examine malicious software. Proper isolation, robust tools, and adherence to best practices will ensure the lab remains secure and functional for diverse analysis tasks.