Lab 1.2: Setting Up Your Lab Environment

Introduction

Fundamentally, emulating adversary TTPs means executing real cyber-attacks. We need a controlled lab environment in which to develop and test our emulated TTPs before applying them in a production network. Otherwise, we risk executing attacks against unintended systems which can result in serious trouble.

This lab will walk you through setting up an environment suitable for completing hands-on-keyboard labs throughout this course.

Objectives

1. Setup a lab environment in which to emulate adversary TTPs in a controlled manner.

Estimated Completion Time

- 1 - 2 hours

Requirements

1. Internet Access
2. Elevated privileges to install hypervisor software, such as VirtualBox
3. This lab requires sufficient resources to run Kali Linux and Windows Server 2019 virtual machines concurrently. The following minimum hardware specifications are recommended:
    - 8 GB RAM
    - 75 GB free disk space
    - 4 core 2 GHz CPU

Malware Warning

Fundamentally, this course entails executing publicly known adversary TTPs so that we can assess and improve cybersecurity. As a result, many of our tools and resources will likely be flagged malicious by security products. We make every effort to ensure that our adversary emulation content is trusted and safe for the purpose of offensive security testing.

As a precaution, you should not perform these labs on any system that contains sensitive data. Additionally, you should never use capabilities and/or techniques taught in this course without first obtaining explicit written permission from the system/network owner(s).

Walkthrough

Step 1: Download and Install a Hypervisor

A hypervisor is software that can create and run Virtual Machines. Virtual machines enable you to run guest operating systems on your host computer.

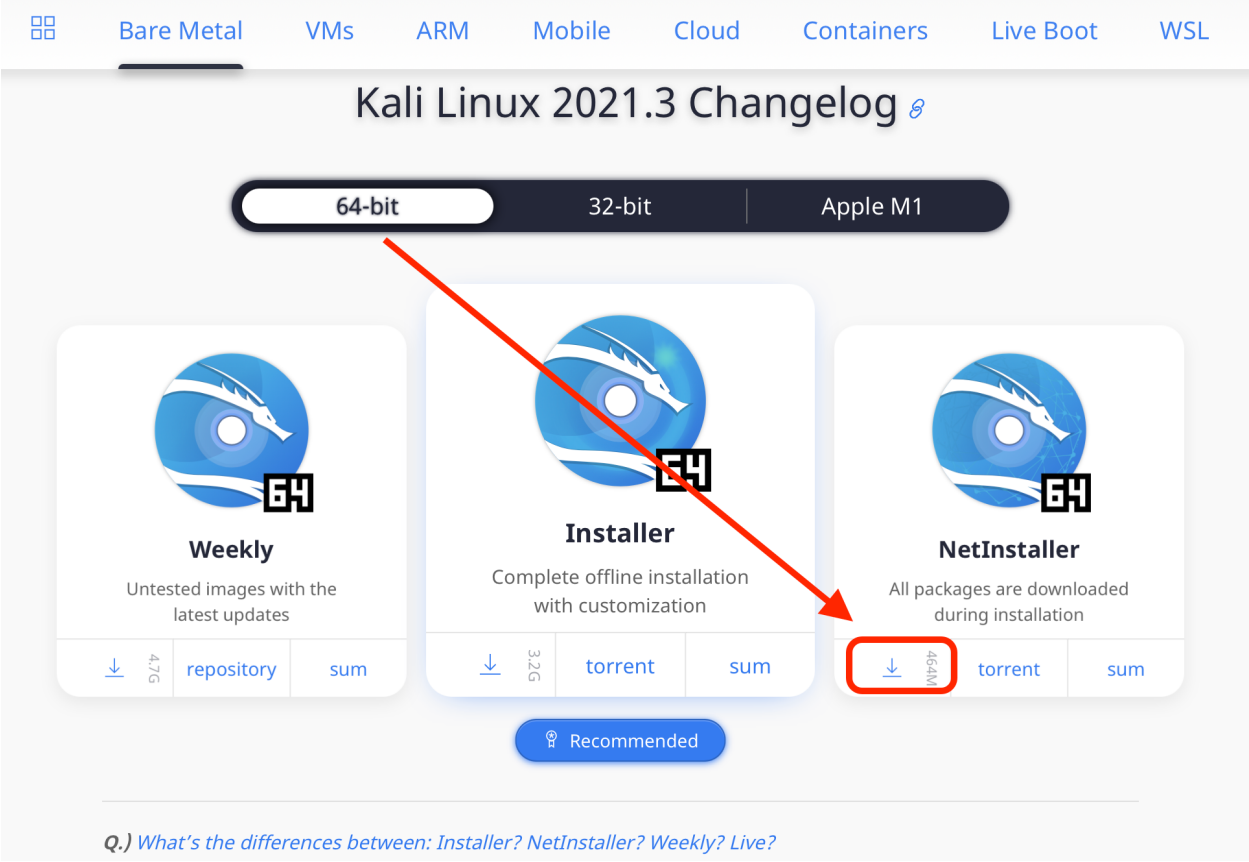
We will use a hypervisor in order to run virtual machines running Kali Linux and Windows Server 2019.

1. Download and install the hypervisor of your choice; The video walkthroughs will utilize VirtualBox, as it is freely available and supported on most operating systems (Windows, Mac, and Linux).
    a. https://www.virtualbox.org

Step 2: Download and Install Kali Linux

Kali is a free Linux distribution that contains tools and configurations needed for offensive cybersecurity activities. This course uses Kali as our platform from which to execute emulated TTPs.

1. Download Kali Linux
    a. https://www.kali.org
    b. This course uses the *Bare Metal > NetInstaller 64-bit* option



2. Install Kali Linux in your hypervisor
    a. If using VirtualBox, follow along with the lab walkthrough video. Otherwise, consult your hypervisor documentation.

3. Optional – install extensions for your hypervisor
    a. Hypervisors such as VMWare and VirtualBox have tools/extensions that enable niceties such as drag and drop files between host and VMs, shared clipboard, etc.
    b. This course will install VirtualBox extensions for this purpose.

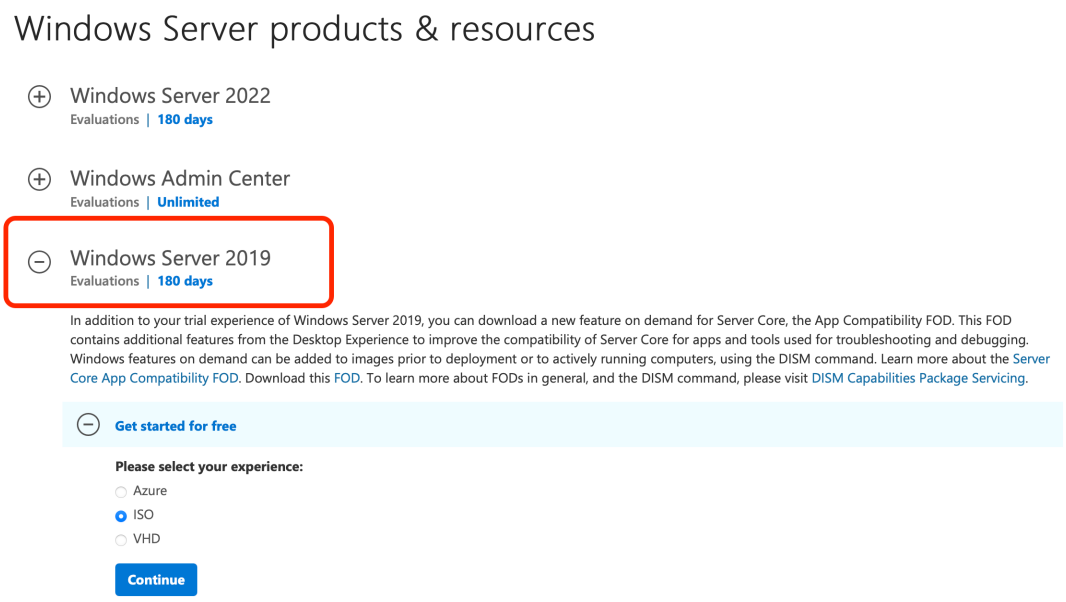
4. Take a baseline snapshot after OS installation
    a. Snapshots will enable you to revert your VM to a clean state; this is very useful if you execute TTPs that make undesirable changes or leave spurious artifacts.

Step 3: Download and Install Windows Server 2019 (Trial)

This course uses a Windows Server 2019 VM to deploy attacks against. Windows Server 2019 was selected in order to emulate Active Directory attacks. While Windows Server 2019 is a commercial product, it can be obtained for free in a trial capacity from Microsoft.

1. Download Windows Server 2019
    a. https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019
    b. This course uses the ISO version
    c. Make sure you download **Windows Server 2019** and not an alternate version such as *Window Server 2019 Essentials*

Make sure that you download Windows Server 2019, and not one of the variations such as *Windows Server 2019 Essentials.*



2. Install Windows Server 2019 in your hypervisor

3. Optional – install extensions for your hypervisor

4. Take a baseline snapshot after OS installation

Step 4: Download and Execute Lab Setup Scripts

This course provides automated setup scripts to streamline configuration of your lab environment.

1. Download the MITRE ATT&CK Defender Adversary Emulation repository from GitHub.
    a. https://github.com/maddev-engenuity/AdversaryEmulation/releases
    b. Select the latest release available and download the source code.
    c. Transfer the repository folder to both your Kali and Windows Server 2019 VMs.

2. From the Kali VM, execute the setup script:

    ```
    cd AdversaryEmulation/vm_setup_scripts/kali
    sudo ./setup-kali-vm.sh
    ```

    When the setup process completes, a new user will have been created with the following credentials:

    ```
    Username: attacker
    Password: ATT&CK
    ```

3. From the Windows Server 2019 VM, open an Administrator PowerShell session and execute the setup script:

    ```
    cd AdversaryEmulation\vm_setup_scripts\windows_server\
    .\setup-dc.ps1
    ```

    When the setup process completes, a new user will have been created with the following credentials:

    ```
    Username: MAD\madAdmin
    Password: ATT&CK
    ```

4. Take snapshots of both VMs to preserve this configuration.

Lab Summary

During this lab we setup a small range environment in which to complete course labs and practice adversary emulation activity.

Setting up a lab and installing operating systems may seem mundane, but it is an essential skill for cybersecurity practitioners.

In our next lab, we'll put this environment to use by executing the FIN6 adversary emulation plan.