Lab 1 part 1: Malware Analysis Virtual Machine(2%)

What You Need for This Project

- A computer with an Internet connection.

Install a Hypervisor

Download and install one of these products:

For Windows: **VMware Player**
For Mac: **VMware Fusion**
For all platforms: **VirtualBox**

Install Archive Software

You need software that can unzip a 7-Zip archive. Download and install the appropriate software for your operating system from the list below.

For Windows: **7-Zip**
For Mac: **The Unarchiver**
For Linux: Use **7z**, which is included in Kali. To add it to Ubuntu, or other Debian-based systems, use

```
apt install 7z
```

The next steps depend on your hypervisor.

VMware Users

Download the Virtual Machine

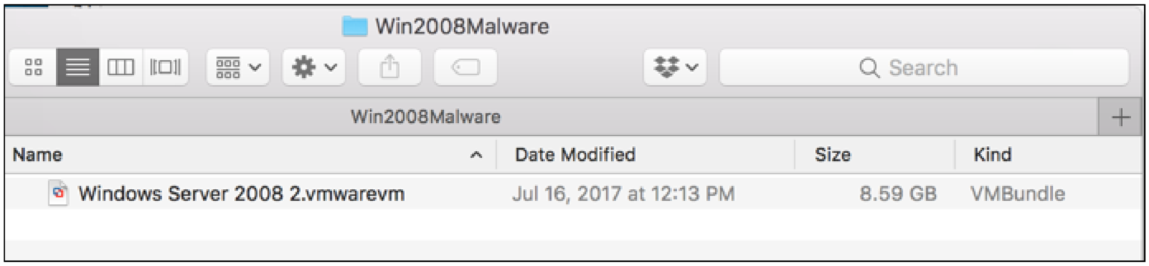
Download the VM file, as shown below.

For VMware: **Win2008Malware.7z**
Size: 2,073,173,278 bytes
SHA-256: c2d59bb80d71cb73350fe436d2658eeb46c869edce66c950ce97268e2a2fa25a

Unzip the Virtual Machine

After extracting the VM, a folder appears with several files in it, as shown below.

(On the Mac, it appears as a single file unless you right-click it and click "Show Package Contents", which you don't have to do.)

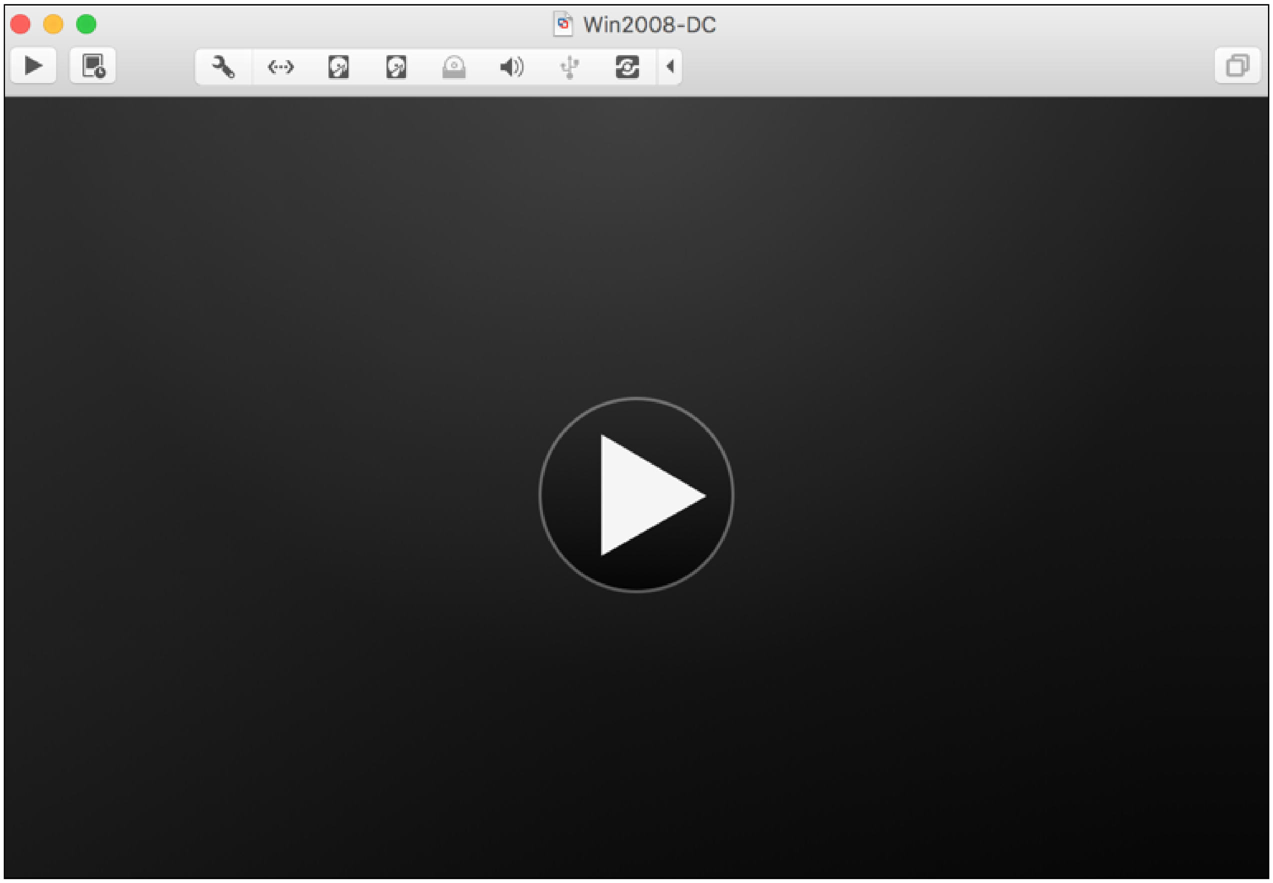


Name	Date Modified	Size	Kind
Windows Server 2008 2.vmwarevm	Jul 16, 2017 at 12:13 PM	8.59 GB	VMBundle

Opening the VM

Launch your hypervisor software. Click **File**, **Open**. Navigate to the folder containing the extracted files and double-click it. If more folders appear, double-click them until you find a file, then double-click that.

The VM opens, as shown below. Click the big rightward-pointing triangle to start it. If a box pops up asking you whether you moved or copied it, click "**I copied it**".



VirtualBox Users

Download the Virtual Machine

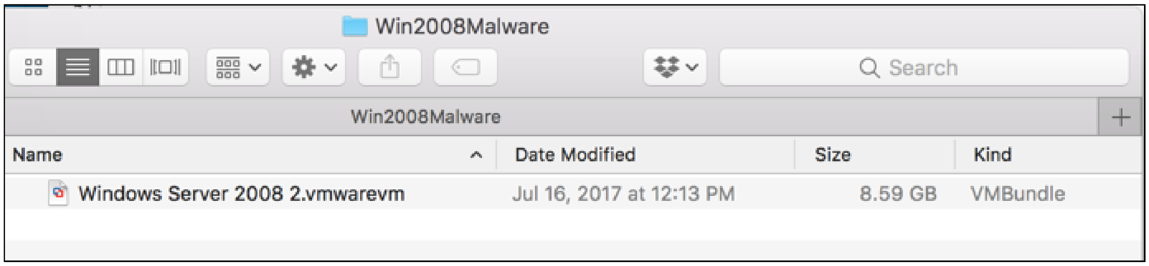
Download the VM file, as shown below.

For VirtualBox: **[Win2008MalwareVB.7z]**
Size: 3,754,472,442 bytes
SHA-256: 879584a72752a3a22843b21e02992e6aa78ad4b73aed5536a44c91613d813113

Unzipping the Virtual Machine

After extracting the VM, a folder appears with several files in it, as shown below.

(On the Mac, it appears as a single file unless you right-click it and click "Show Package Contents", which you don't have to do.)



Name	Date Modified	Size	Kind
Windows Server 2008 2.vmwarevm	Jul 16, 2017 at 12:13 PM	8.59 GB	VMBundle

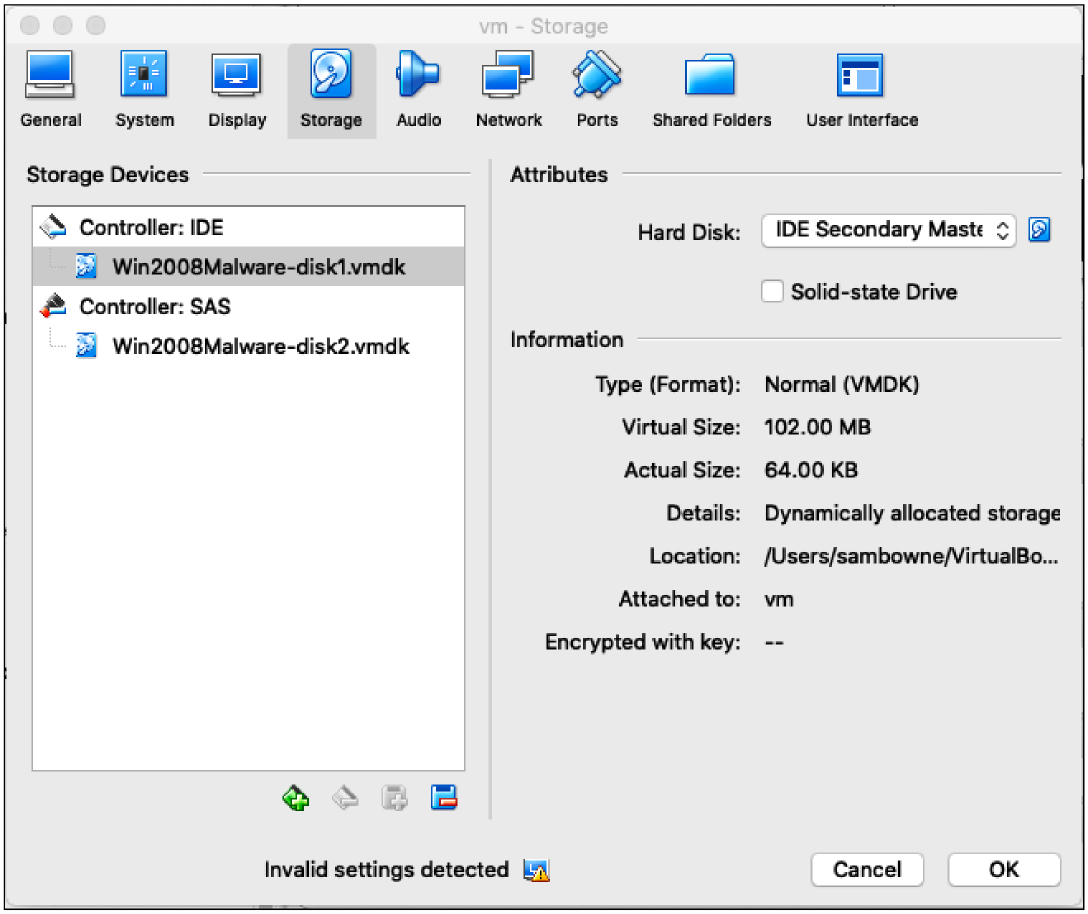
Importing the VM

Launch VirtualBox. Click **File**, "**Import Appliance**". Navigate to the folder containing the extracted files and double-click the **Win2008Malware.ovf** file. Click **Continue**. Click **Import**.

Removing the Small Disk

In the "Oracle Vm VirtualBox Manager" window, a new virtual machine appears, named **vm**. Right-click it and click **Settings**.

There are two virtual disks, as shown below. Find the one that has a size of 102 MB. Right-click that disk click "**Remove Attachment**".



Storage Devices

- Controller: IDE
  - Win2008Malware-disk1.vmdk
- Controller: SAS
  - Win2008Malware-disk2.vmdk

Attributes

Hard Disk: IDE Secondary Maste

□ Solid-state Drive

Information

Type (Format): Normal (VMDK)
Virtual Size: 102.00 MB
Actual Size: 64.00 KB
Details: Dynamically allocated storage
Location: /Users/sambowne/VirtualBo...
Attached to: vm
Encrypted with key: --

Invalid settings detected

Click **OK**.

Opening the VM

Click the green **Start** button to launch the virtual machine.

Hyper-V Users

Download the Virtual Machine

Download the VM file, as shown below.

For Hyper-V: Svr8Vm12.7z
Size: 2.21 GB

Unzip the Virtual Machine

After extracting the VM, a folder appears with several files in it.

Opening the VM

Launch the VM in Hyper-V. I don't have step-by-step instructions for that process.

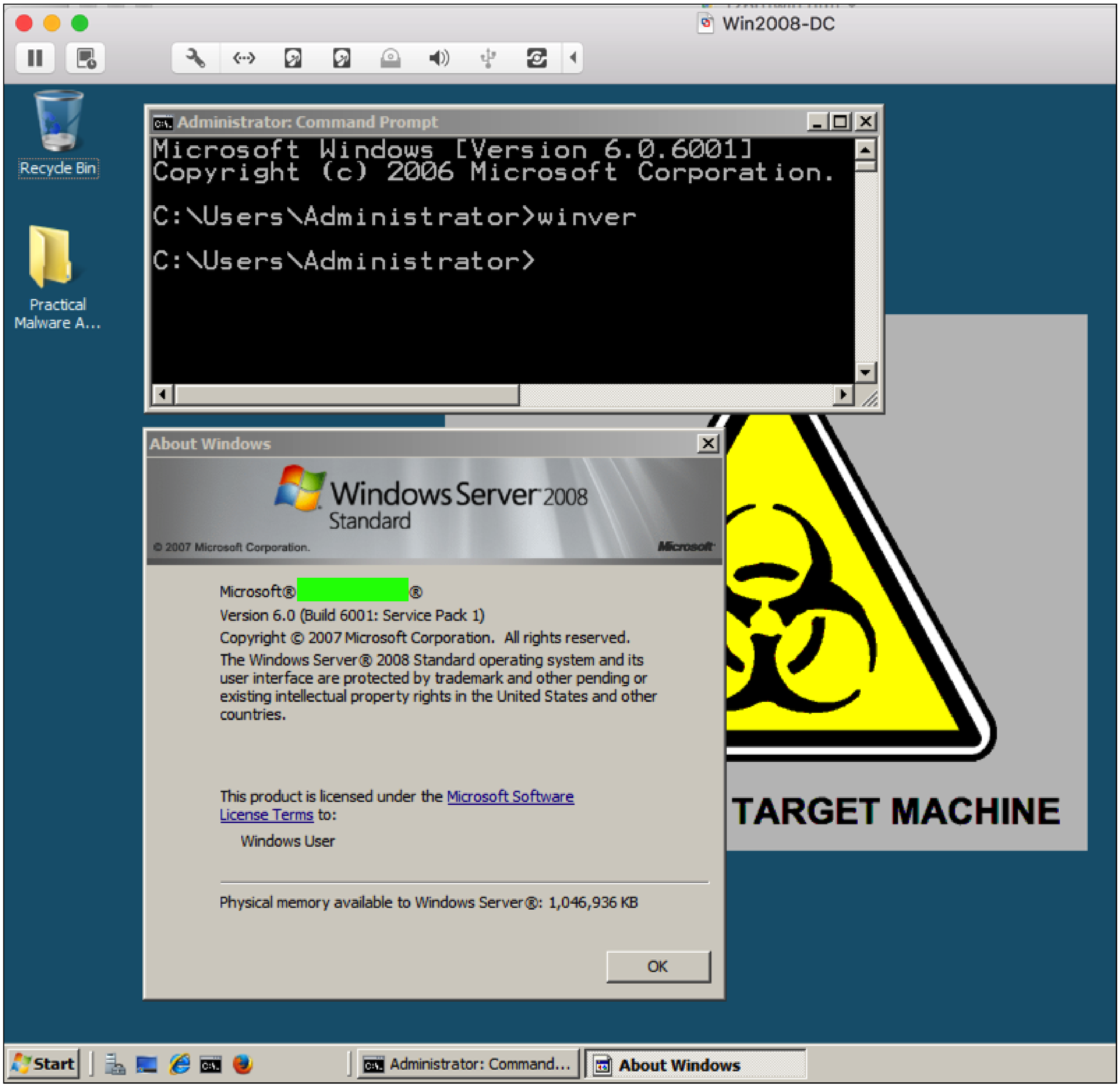
Viewing the Windows Version

Flag PMA 20: Windows Version (10 pts)

When the desktop appears, as shown below, open a Command Prompt and execute this command:

```
winver
```

An "About Windows" box pops up, as shown below. Find the words that are covered by the green box in the image below. They are the flag.



Administrator: Command Prompt

```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.

C:\Users\Administrator>winver

C:\Users\Administrator>
```

About Windows

Windows Server 2008 Standard

© 2007 Microsoft Corporation.

Microsoft

Microsoft® [redacted] ®

Version 6.0 (Build 6001: Service Pack 1)

Copyright © 2007 Microsoft Corporation. All rights reserved.

The Windows Server® 2008 Standard operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries.

This product is licensed under the Microsoft Software License Terms to:

Windows User

Physical memory available to Windows Server®: 1,046,936 KB

OK

Renumbered and put in flag format 8-14-19
Updated with better VirtualBox instructions 8-25-2020