PMA 20: Malware Analysis Virtual Machine (15 pts)

What You Need for This Project

- A computer with an Internet connection. Virtualization software: VMware, VirtualBox, or Hyper-V
- The instructions below assume you are using Windows and VMware Player. You can use VMware on the Mac and other operating systems, but the steps may be somewhat different.

Install a Hypervisor

Download and install one of these products:

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

Download the Virtual Machine

Download the appropriate VM file, as shown below.

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

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

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

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.

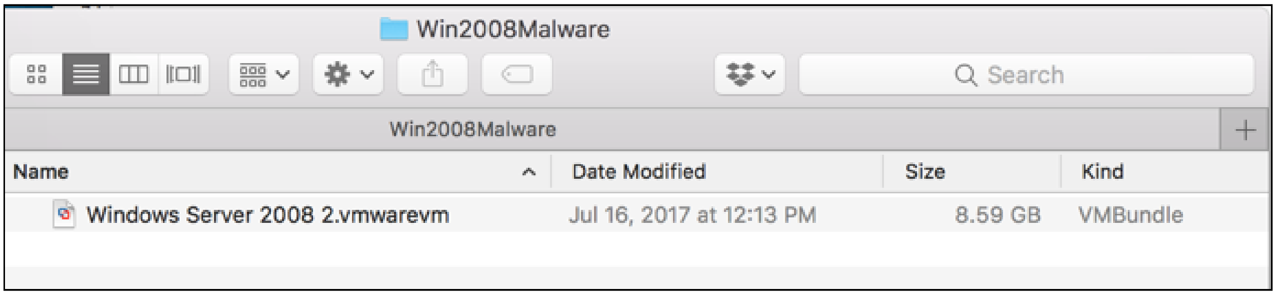
For Windows: [7-Zip]
For Mac: [The Unarchiver]
For Linux: Use **7z**, which is included in Kali. To add it to Ubuntu, or other Debian-based systems, use

```
    apt install 7z
```

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.)

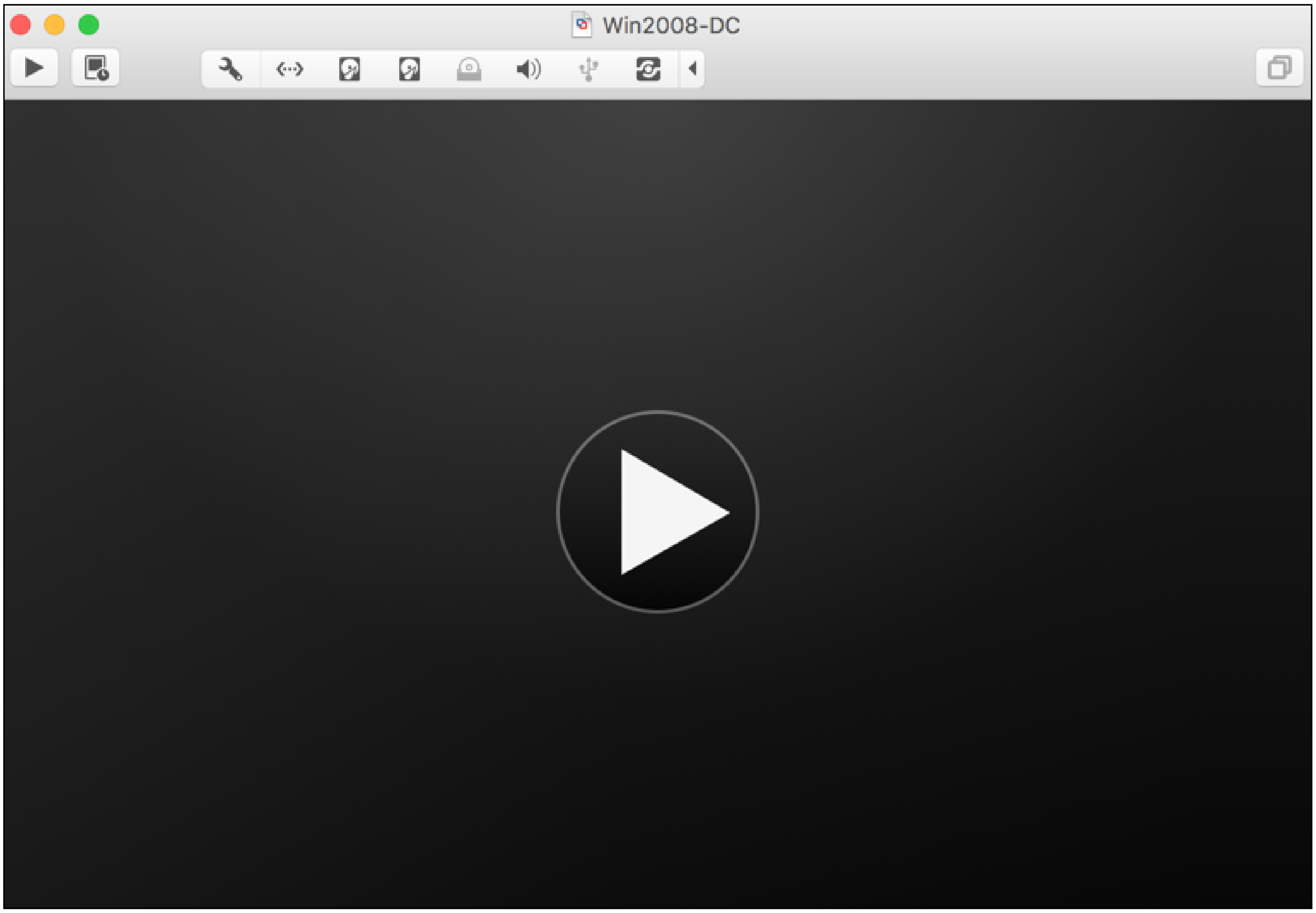


Name	Date Modified	Size	Kind
Windows Server 2008 2.vmwarevm	Jul 16, 2017 at 12:13 PM	8.59 GB	VMBundle

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**".

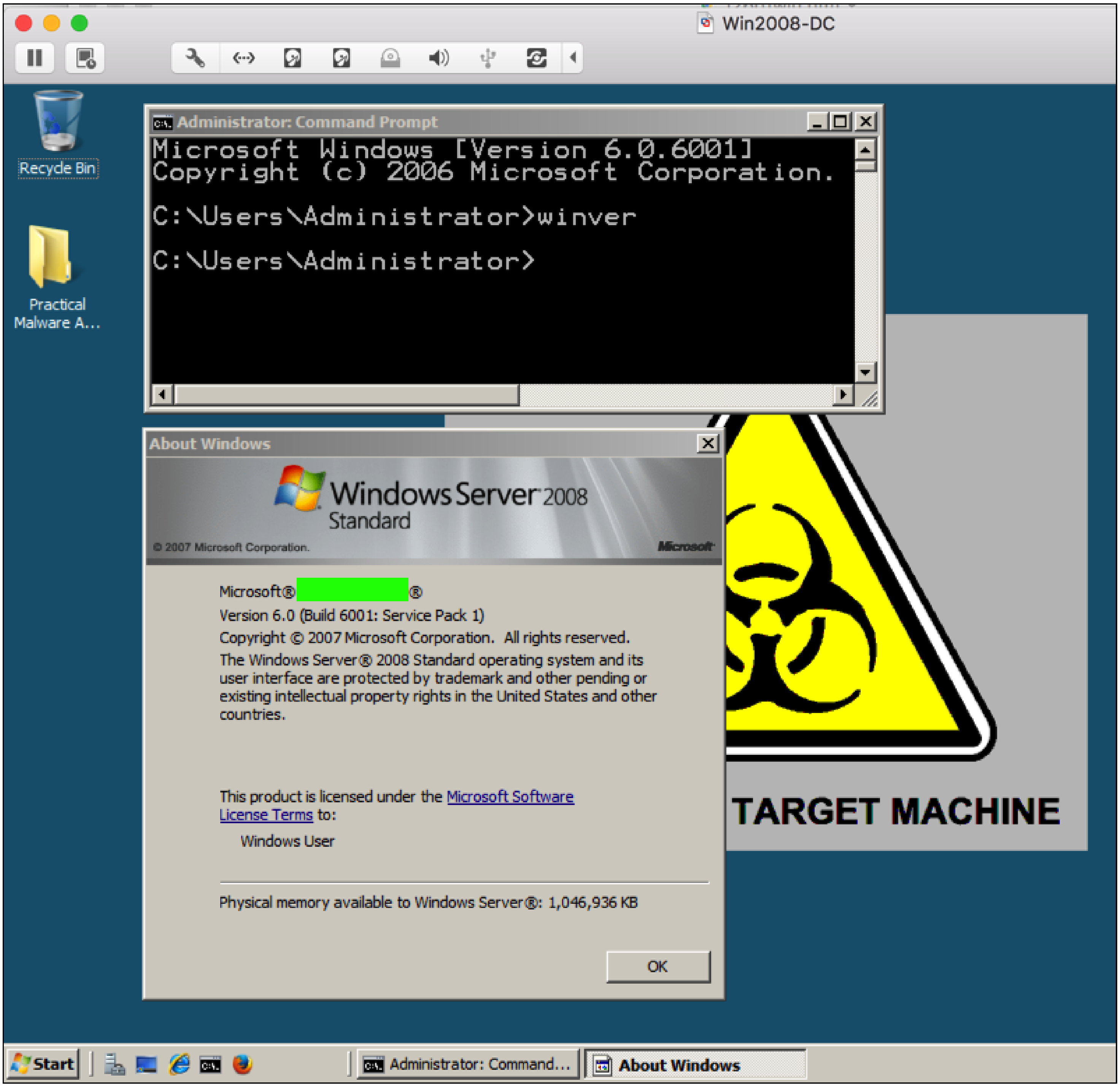


Viewing the Windows Version

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.



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

C:\Users\Administrator>winver

C:\Users\Administrator>
```

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

Renumbered and put in flag format 8-14-19