

Cyber Aces Online

Module 1 – Operating Systems

Updating Windows

By Tim Medin
Presented by Tim Medin
V15Q1

This tutorial is licensed for personal use exclusively for students and teachers to prepare for the Cyber Aces Online competition. You may not use any part of it in any printed or electronic form for other purposes, nor are you allowed to redistribute it without prior written consent from the SANS Institute.

Cyber Aces Online Module 1- ©2015 The SANS Institute. Redistribution Prohibited.

1

Welcome to Cyber Aces Online, Module 1! A firm understanding of operating systems is essential to being able to secure or attack one. This module dives in to the Microsoft Windows Operating System. In this module we will be updating your Windows Virtual Machine.

Patches

- An important step in keeping your systems secure is to install the latest patches
 - This applies to all operating systems, not just Windows
- Microsoft releases new patches the second Tuesday of each month, known as "Patch Tuesday"
- Sometimes new vulnerabilities are discovered and a patch has to be delivered outside of the standard Tuesday
 - Often occurs if a new critical vulnerability is actively being exploited by malicious attackers
- Microsoft's 2nd Tuesday cycle was highly controversial when it was first announced
 - Pro: Allows system administrators to plan for patches
 - Con: A patch may not be delivered as quickly

Patches

All systems, including Windows systems, need to be updated regularly to help protect them. In 2003, Microsoft changed the way they delivered patches. Instead of delivering patches as soon as they were completed, the patches were all released on the same day, the second Tuesday of the month. Releasing the patches on a regular schedule allows systems administrators to plan for the patch deployment and work them into a standard set of processes to get the patches deployed. This day became known as "Patch Tuesday".

When this plan was initially revealed it was controversial, and some people still do not like the process. They contend that patches should be released as soon as they are ready to help protect the systems. The counterpoint is that systems administrators can't plan to deploy the patches and the systems will not be properly patched. However, if a critical vulnerability is being actively exploited by malicious attackers Microsoft will release an out-of-cycle patch to resolve the issue.

Another important thing to note is that Microsoft now splits feature updates and security updates. This means that the security patches are less likely to affect functionality and interrupt existing business processes. Other software vendors (notably Apple) do not have such a strong delineation between security and feature updates.

Why Patch Quickly?

- The bad guys make money off of exploited systems
- The more systems they can control, the more money they can make
- The bad guys reverse engineer Microsoft's patches to help write new exploits that will target as-of-yet unpatched systems
 - Colloquially referred to as "Exploit Wednesday" (not a Microsoft term)
- Staying up-to-date with patches is increasingly important
- If a vulnerability is actively being exploited "in the wild", it is important to patch quickly

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

3

Why Patch Quickly?

Malicious attackers make money off the systems they compromise. Typically, the more machines they control, the more money they can make. They work very hard to compromise new systems and there is a race to exploit the systems before another attacker can take control.

These attackers will take the patches released by Microsoft and reverse engineer them to determine the original flaw. They will then take advantage of the vulnerability on systems that are not yet patched. The speed at which they can create a working exploit given the patch is increasing, and in many times can occur in less than a day or two. The speed of exploit development leads to "Exploit Wednesday", where these new exploits are released against unsuspecting users. Another reason that releasing all the patches at the same time (as with Patch Tuesday) is that it allows administrators to schedule the patches for quicker deployment, thereby limiting the exposure due to Exploit Wednesday.

Exercise: Patching Windows

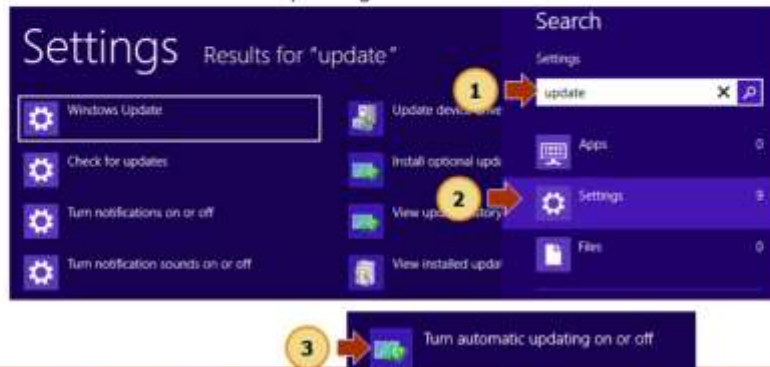
- We will apply the patches to your Windows system and make sure that it stays up-to-date

Exercise: Patching Windows

In this exercise, your Windows VM will be patched. It is likely that your system has already been updated, or is in the process of updated. The "express" settings option you selected earlier will automatically download and apply the updates, but it is always good to check. You may have nothing to do here other than to verify the settings.

Verify Automatic Updates are Enabled

- Press the Windows Key to open the menu
- Start typing "Update"
- Click "Settings"
- Select "Turn automatic updating on or off"



Cyber Aces Online Module 1 - ©2015 the SANS Institute. Acquisition 2/2015/2016

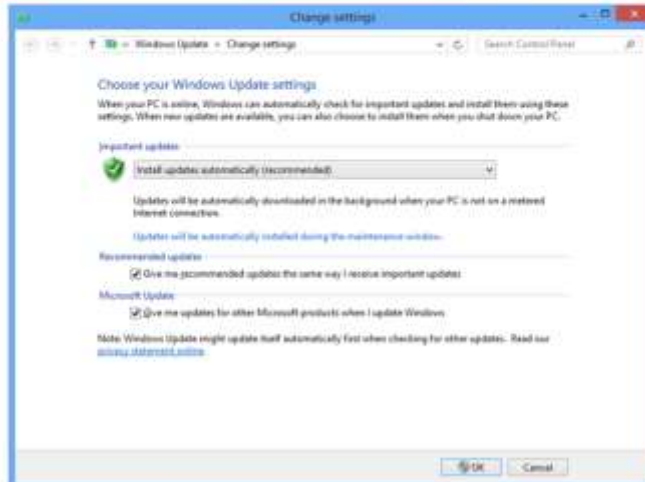
5

Verify Automatic Updates are Enabled

To view the settings related to Windows Update, open the menu by pressing the Windows Key or moving your cursor to the corner. Then type the word "update" and click the "Settings" option. From there you will see the "Turn automatic updates on or off". Click on it to open the interface to change the update options.

Update Settings

- Make sure your system is configured to automatically download updates
- Most home users should use the "Install updates automatically" option
- The "Give me updates for other Microsoft products when I update Windows" will also download updates for other Microsoft products, such as Microsoft Office



Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

6

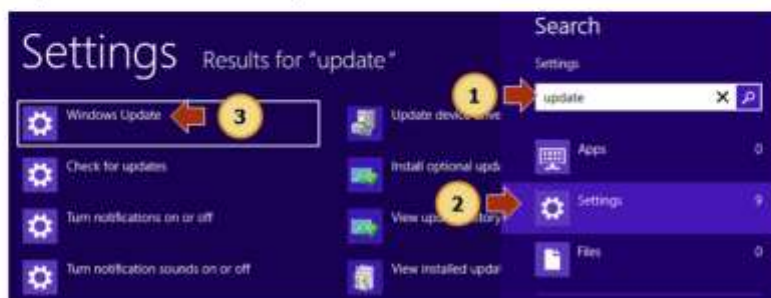
Updates Settings

Most users will want to select "Install updates automatically" to ensure they are always up-to-date. If you want to be a little more cautious about installing updates use the "Download updates but let me choose whether to install them". With this settings the updates will be downloaded and you will be prompted to install them instead of the updates being installed automatically. If you use this option, you need to make sure that you do install the most important updates to keep your system secure.

Microsoft also offers a feature to ensure that all Microsoft products (not just the operating system) are updated. Malicious attackers will often target other Microsoft products, such as the nearly ubiquitous Microsoft Office suite, so it is important to keep this software updated.

Run Windows Update

- Press the Windows Key to open the menu
- Start typing "Update"
- Click "Settings"
- Open Windows Update



Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

7

Run Windows Update

The Windows Update tool on Windows will manage and apply the patches on our system. To get to Windows Update first hit the Windows Key or move your mouse to one of the corners. Next, type "update" and click on Settings. Finally, click on the "Windows Update" program.

Check for Updates

- Your VM is brand new and likely doesn't yet have patches applied
 - But, the "express" configuration option selected during install will enable automatic updates, so your system may have already installed updates
- Click "Check for updates now"
 - This may take a while

Windows Update

You're set to automatically install updates

Never checked for updates

Check for updates now

Windows Update

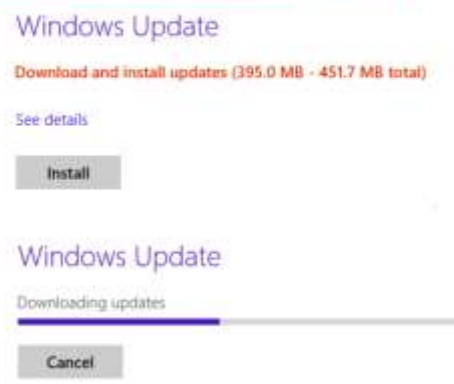
Checking for updates

Check for Updates

If your VM has not yet checked for the updates you will need to click the "Check for updates now" button to start the update process. Windows will then check with the update servers to check if there are any patches that need to be applied.

Apply Updates

- Click "Install" to apply the updates
- Wait for the updates to be installed



The screenshot displays the Windows Update window. The top section, titled 'Windows Update', shows the status 'Download and install updates (395.0 MB - 451.7 MB total)' in orange text. Below this is a blue link 'See details' and a grey 'Install' button. The bottom section, also titled 'Windows Update', shows the status 'Downloading updates' in blue text, accompanied by a progress bar that is approximately one-third full. Below the progress bar is a grey 'Cancel' button.

Cyber Aces Online Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 9

Apply Updates

Once the update server has been contacted and updates have been found, you will be prompted to install the patches. Click "Install" to install the updates. The process can take a while as the updates need to be downloaded and installed. After the updates have been installed, you may be prompted to reboot.

Exercise Complete!

- After all the updates have been installed, you have completed the exercise
- It is important to keep all of your systems up-to-date to protect yourself against attackers
- Always keep your laptops, desktops, and servers updated, but don't forget about other devices
 - Phones
 - Tablets
 - Laptops
 - Desktops

Exercise Complete!

You have updated your Windows system. Congratulations, you are done with this exercise!