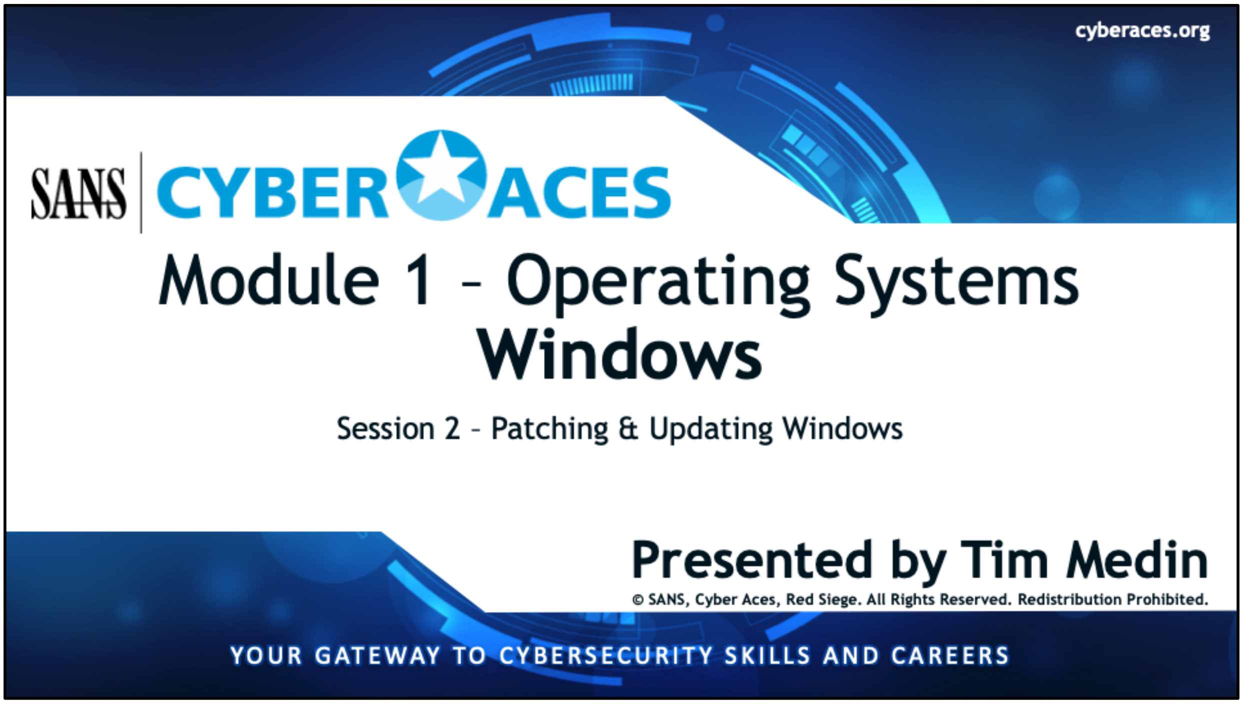


cyberaces.org

SANS | CYBER ACES

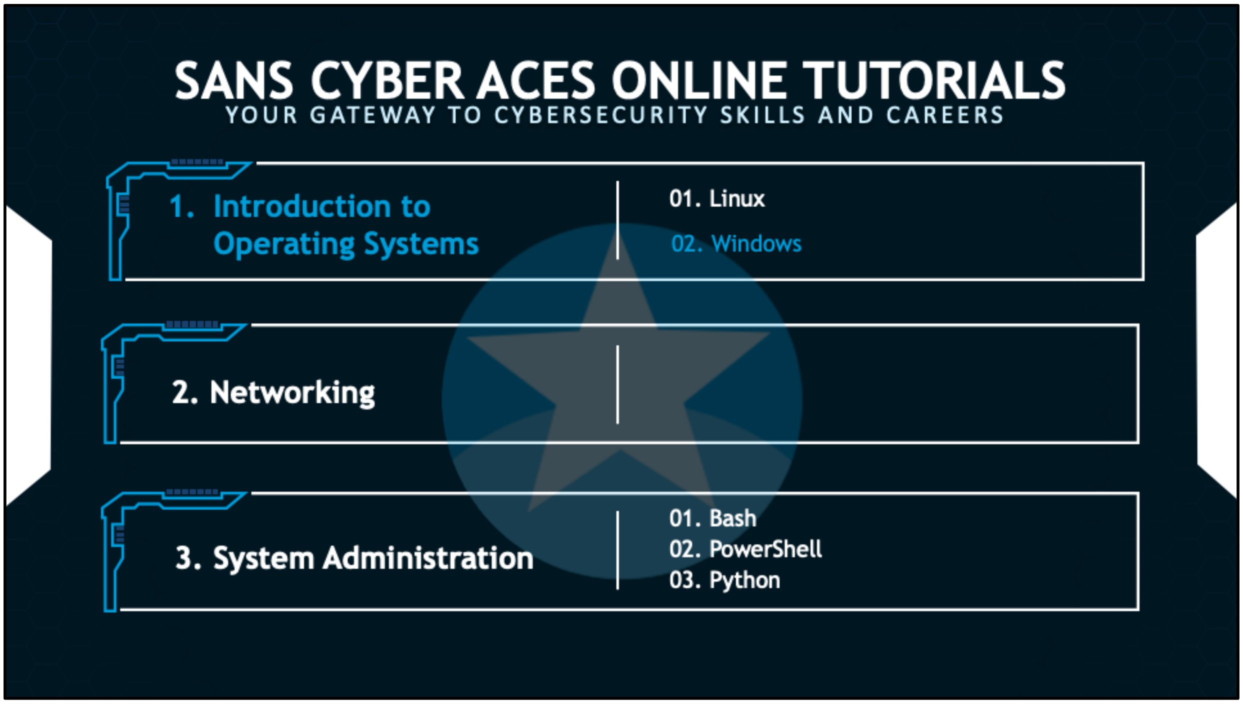
Module 1 – Operating Systems Windows

Session 2 – Patching & Updating Windows

Presented by Tim Medin

YOUR GATEWAY TO CYBERSECURITY SKILLS AND CAREERS

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.



SANS CYBER ACES ONLINE TUTORIALS

YOUR GATEWAY TO CYBERSECURITY SKILLS AND CAREERS

1. Introduction to Operating Systems
   - 01. Linux
   - 02. Windows

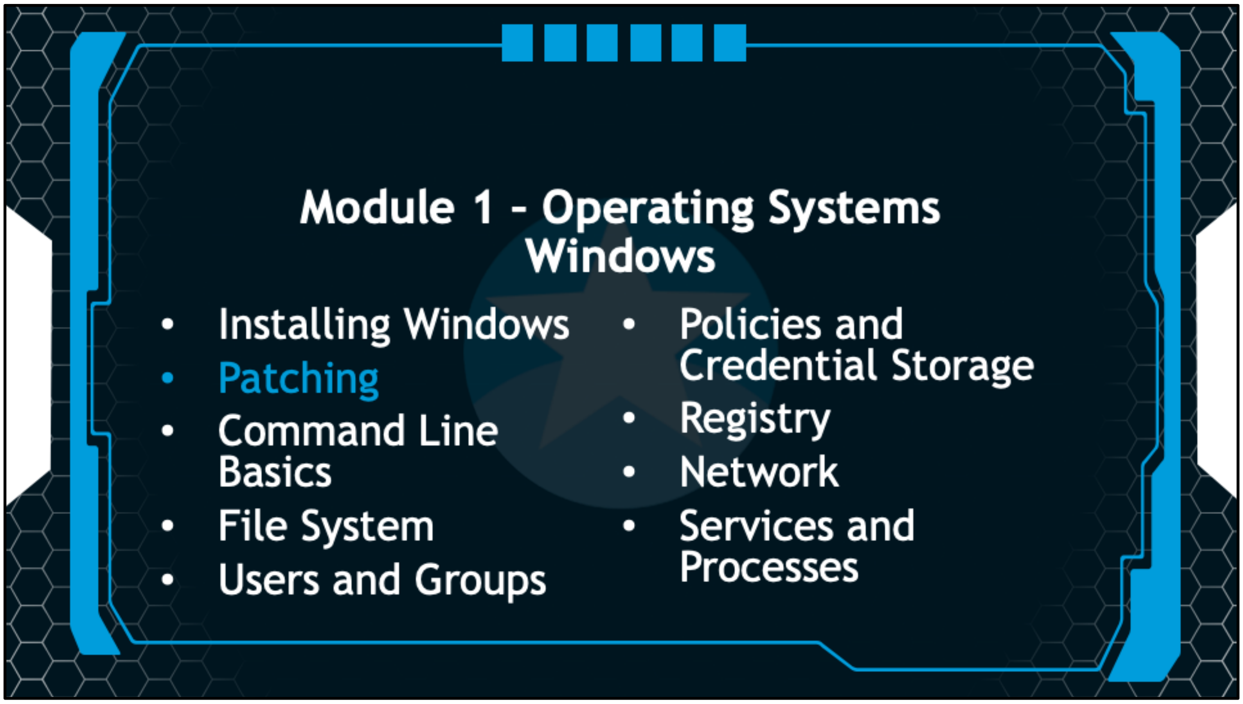
2. Networking

3. System Administration
   - 01. Bash
   - 02. PowerShell
   - 03. Python

This training material was originally developed to help students, teachers, and mentors prepare for the Cyber Aces Online Competition. This module focuses on the basics of what an operating systems is as well as the two predominant OS's, Windows and Linux. This session is part of Module 1, Introduction to Operating Systems. This module is split into two sections, Linux and Windows. In this session, we will continue our examination of Windows.

The three modules of Cyber Aces Online are Operating Systems, Networking, and System Administration.

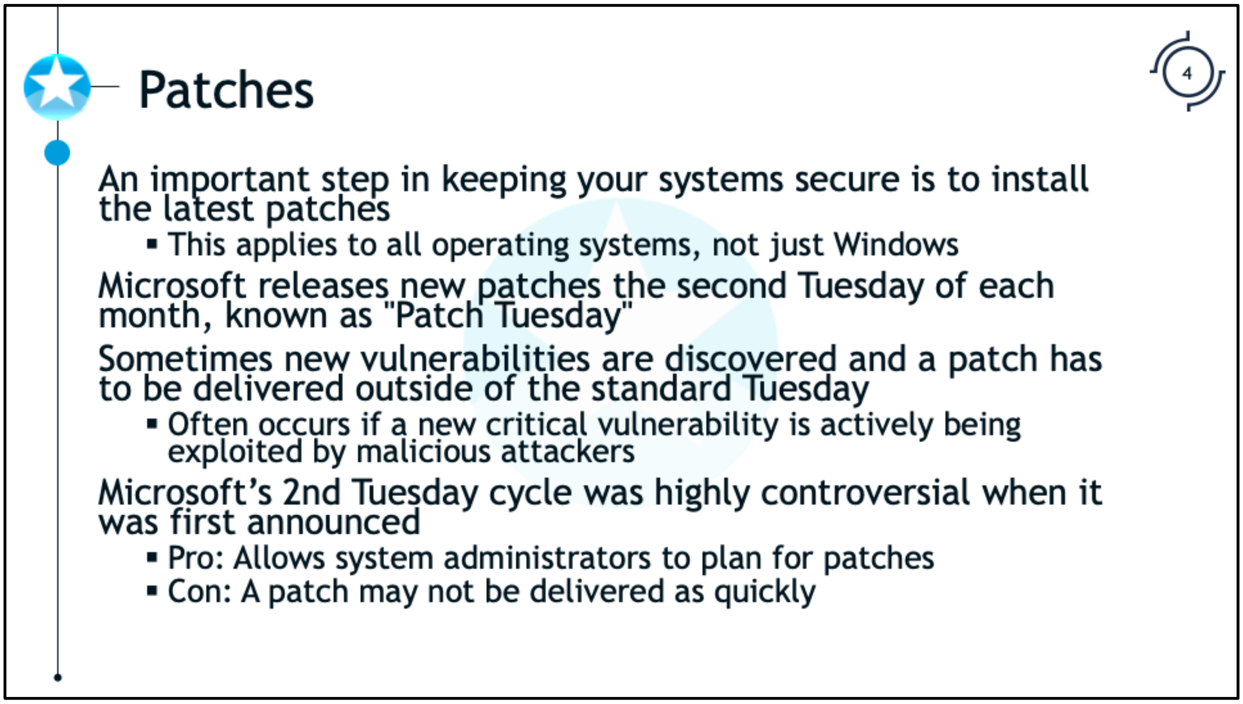
For more information about the Cyber Aces program, please visit the Cyber Aces website at https://CyberAces.org/.



Module 1 - Operating Systems Windows

- Installing Windows
- Patching
- Command Line Basics
- File System
- Users and Groups
- Policies and Credential Storage
- Registry
- Network
- Services and Processes

In this session will will discuss Windows updates and patching.



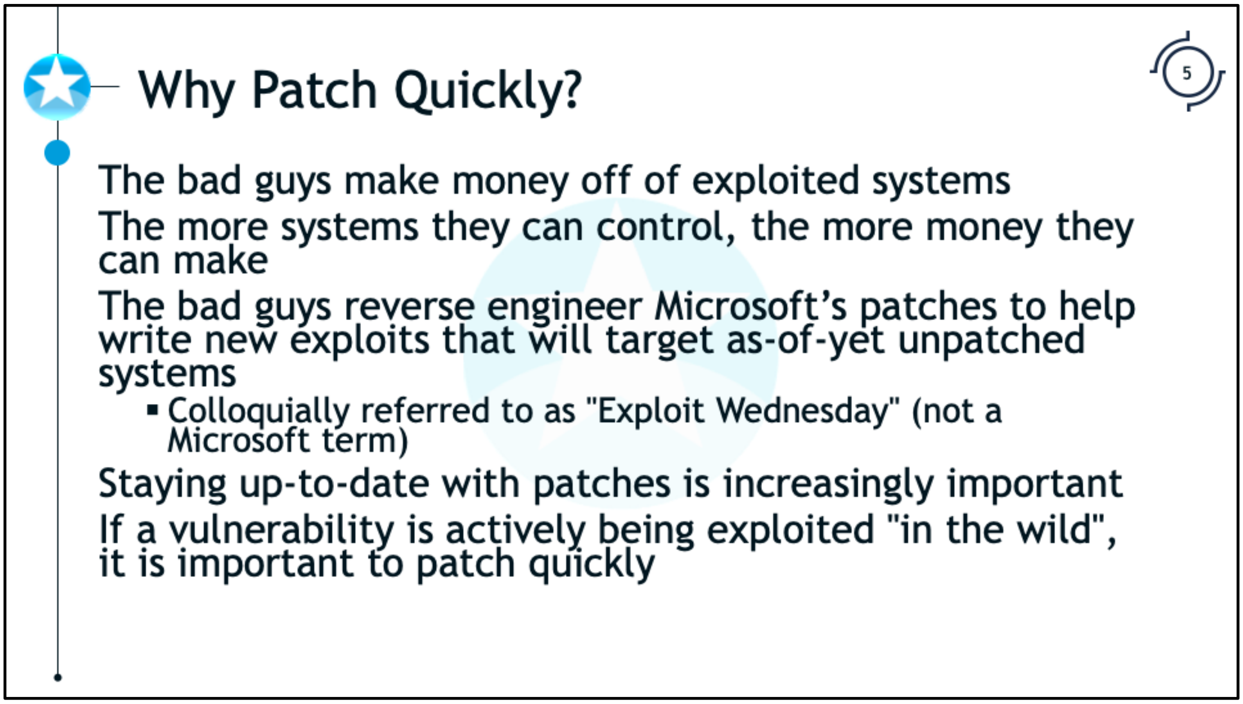
Patches

- 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

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.

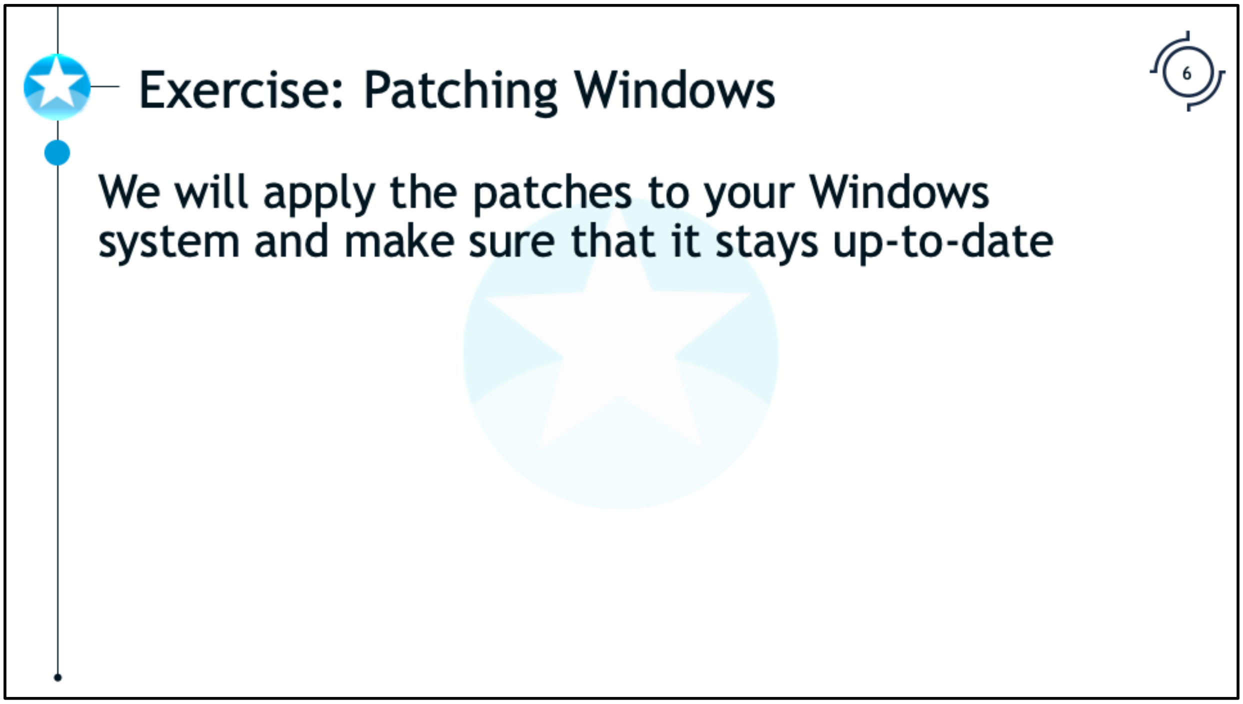


Why Patch Quickly?

- 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

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.



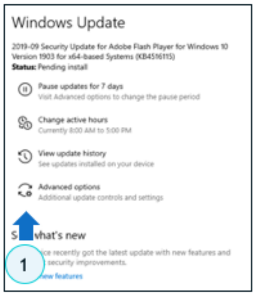
Exercise: Patching Windows

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

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 Update Settings

- Make sure your system is configured to automatically download updates
- The "Receive updates for other Microsoft products when you update Windows" will also download updates for other Microsoft products, such as Microsoft Office



Windows Update

2019-09 Security Update for Adobe Flash Player for Windows 10 Version 1903 for x64-based Systems (KB4516115)
Status: Pending install

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 8:00 AM to 5:00 PM

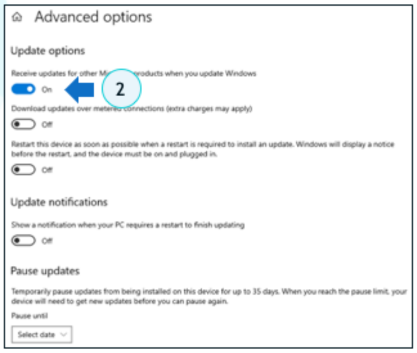
View update history
See updates installed on your device

Advanced options
Additional update controls and settings

S what's new

ice recently got the latest update with new features and security improvements.

ew features



Advanced options

Update options

Receive updates for other Mi roducts when you update Windows
On

Download updates over metered connections (extra charges may apply)
Off

Restart this device as soon as possible when a restart is required to install an update. Windows will display a notice before the restart, and the device must be on and plugged in.
Off

Update notifications

Show a notification when your PC requires a restart to finish updating
Off

Pause updates

Temporarily pause updates from being installed on this device for up to 35 days. When you reach the pause limit, your device will need to get new updates before you can pause again.

Pause until
Select date

Windows 10 will automatically download available updates by default. Most users will want to leave the Windows Update settings as they are set by Microsoft. Users have the option to pause updates temporarily and to disable automatic rebooting after applying updates.

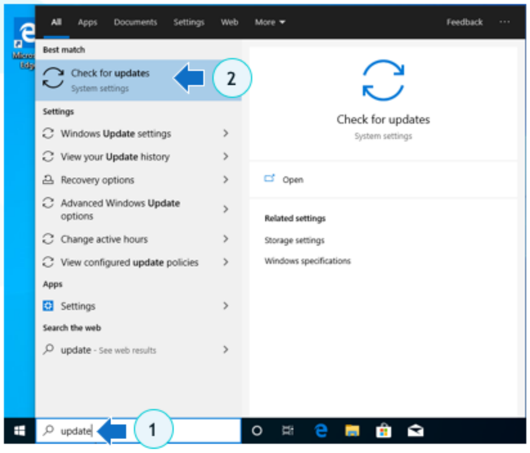
Microsoft also offers a feature to ensure that all Microsoft products (not just the operating system) are updated. Malicious attackers will often target other Microsoft products, such as the nearly ubiquitous Microsoft Office suite, so it is important to keep this software updated.

Apply Updates

Click in the search box next to the Windows button

Start typing “update”

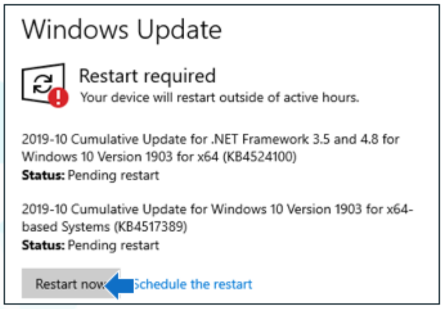
Click “Check for updates”



To view the settings related to Windows Update, open the menu by typing the word “update” in the search box, next to the Windows icon, and click the “Check for updates" option. From there click the "Check for updates" button. Windows 10 will automatically download available updates by default.

Apply Updates & Reboot

Click "Restart now"



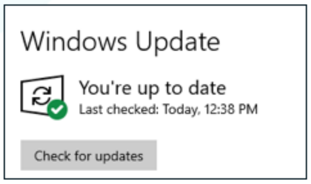
Windows Update

Restart required
Your device will restart outside of active hours.

2019-10 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1903 for x64 (KB4524100)
Status: Pending restart

2019-10 Cumulative Update for Windows 10 Version 1903 for x64-based Systems (KB4517389)
Status: Pending restart

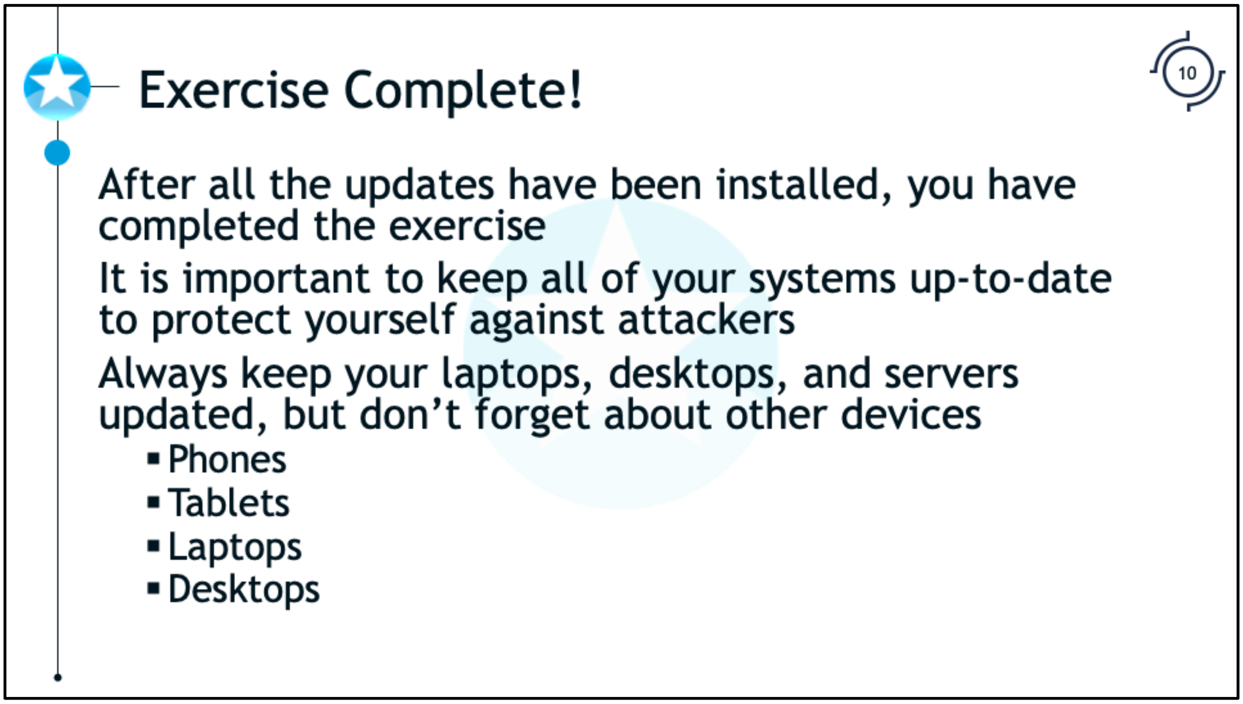
Repeat process after rebooting until no updates remain



Windows Update

You're up to date
Last checked: Today, 12:38 PM

After the updates have been installed, you may be prompted to reboot. Windows may require several reboots to complete patching a new machine.



Exercise Complete!

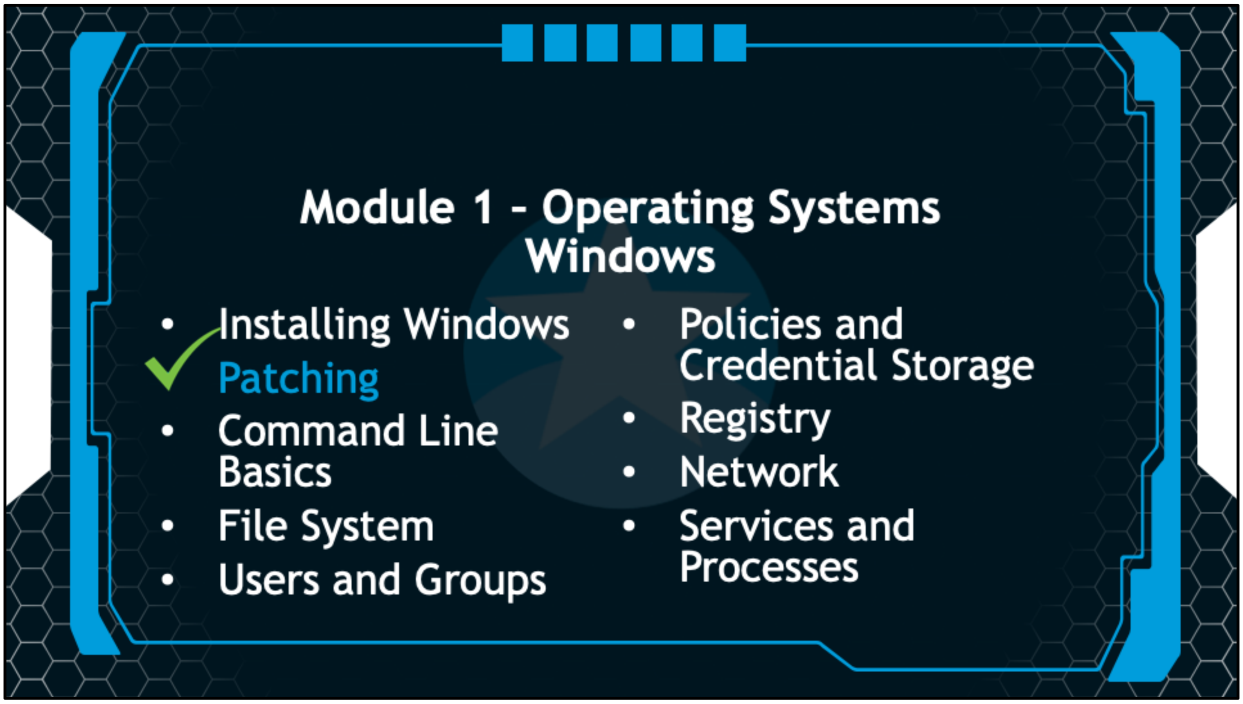
After all the updates have been installed, you have completed the exercise

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

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



Module 1 - Operating Systems Windows

- Installing Windows
- ✓ Patching
- Command Line Basics
- File System
- Users and Groups
- Policies and Credential Storage
- Registry
- Network
- Services and Processes

In the next session, we will discuss the command line basics using CMD.EXE.