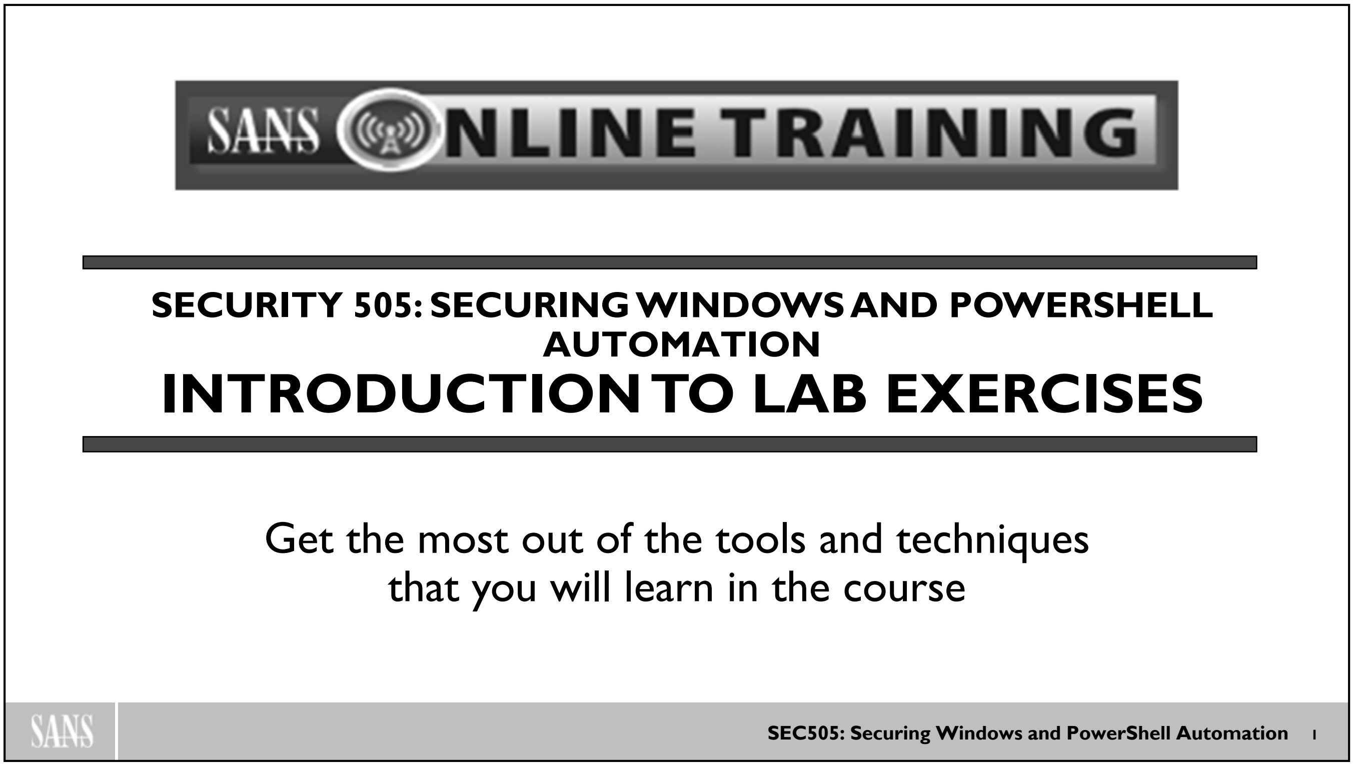


SANS ONLINE TRAINING

SECURITY 505: SECURING WINDOWS AND POWERSHELL AUTOMATION

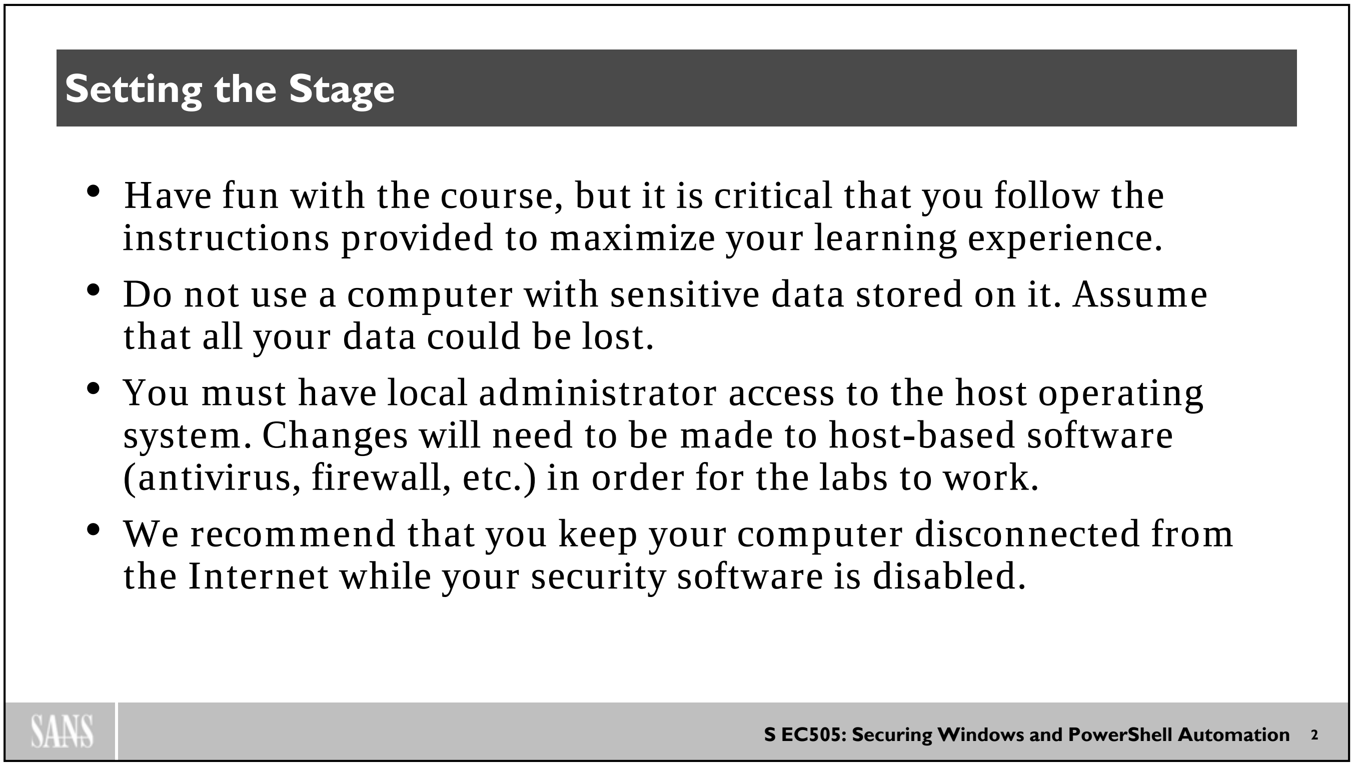
INTRODUCTION TO LAB EXERCISES

Get the most out of the tools and techniques
that you will learn in the course

SANS

SEC505: Securing Windows and PowerShell Automation 1

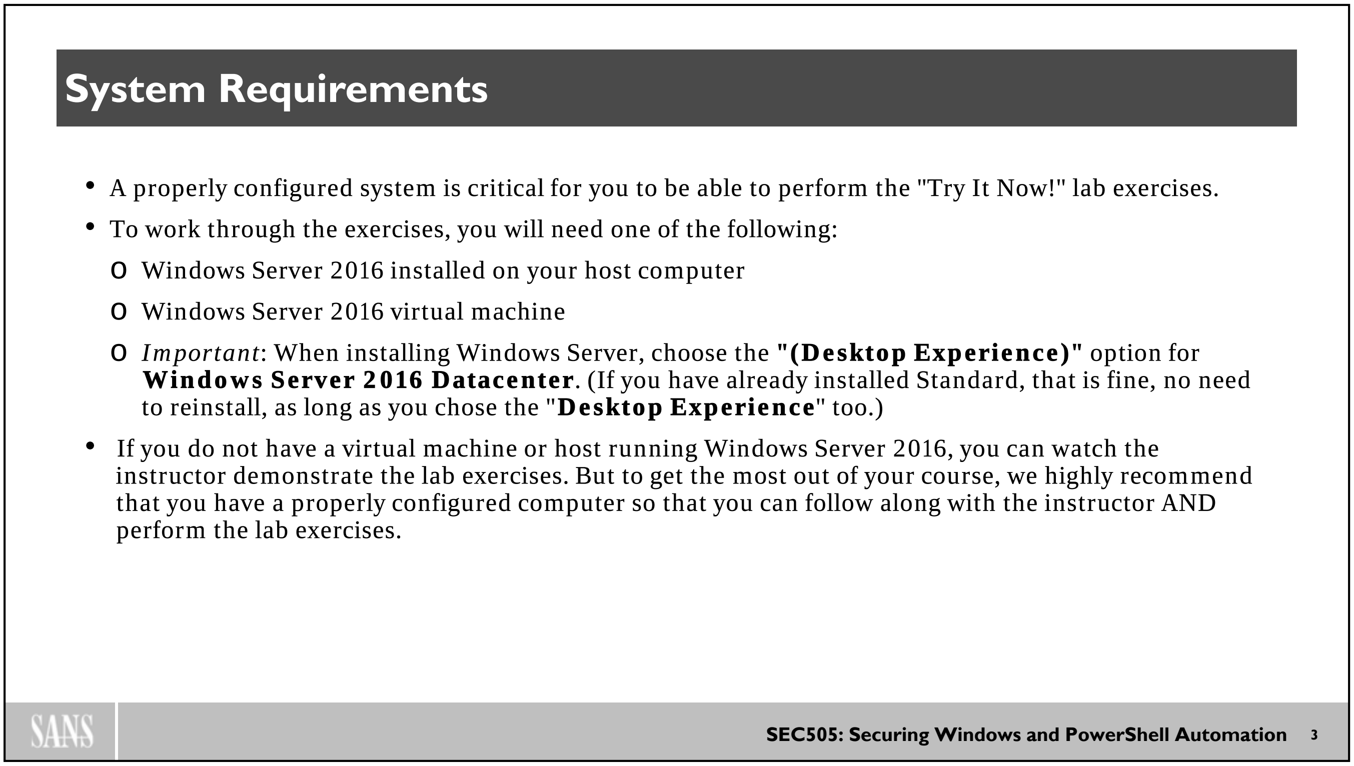
If you have any questions while working through your labs, please do not hesitate to contact our online Subject Matter Experts (SMEs) by sending an e-mail to online-sme@sans.org.



Setting the Stage

- Have fun with the course, but it is critical that you follow the instructions provided to maximize your learning experience.
- Do not use a computer with sensitive data stored on it. Assume that all your data could be lost.
- You must have local administrator access to the host operating system. Changes will need to be made to host-based software (antivirus, firewall, etc.) in order for the labs to work.
- We recommend that you keep your computer disconnected from the Internet while your security software is disabled.

This section is intentionally left blank.



System Requirements

- A properly configured system is critical for you to be able to perform the "Try It Now!" lab exercises.
- To work through the exercises, you will need one of the following:
  - Windows Server 2016 installed on your host computer
  - Windows Server 2016 virtual machine
  - *Important*: When installing Windows Server, choose the **"(Desktop Experience)"** option for **Windows Server 2016 Datacenter**. (If you have already installed Standard, that is fine, no need to reinstall, as long as you chose the "**Desktop Experience**" too.)
- If you do not have a virtual machine or host running Windows Server 2016, you can watch the instructor demonstrate the lab exercises. But to get the most out of your course, we highly recommend that you have a properly configured computer so that you can follow along with the instructor AND perform the lab exercises.

Windows Server 2016 R2

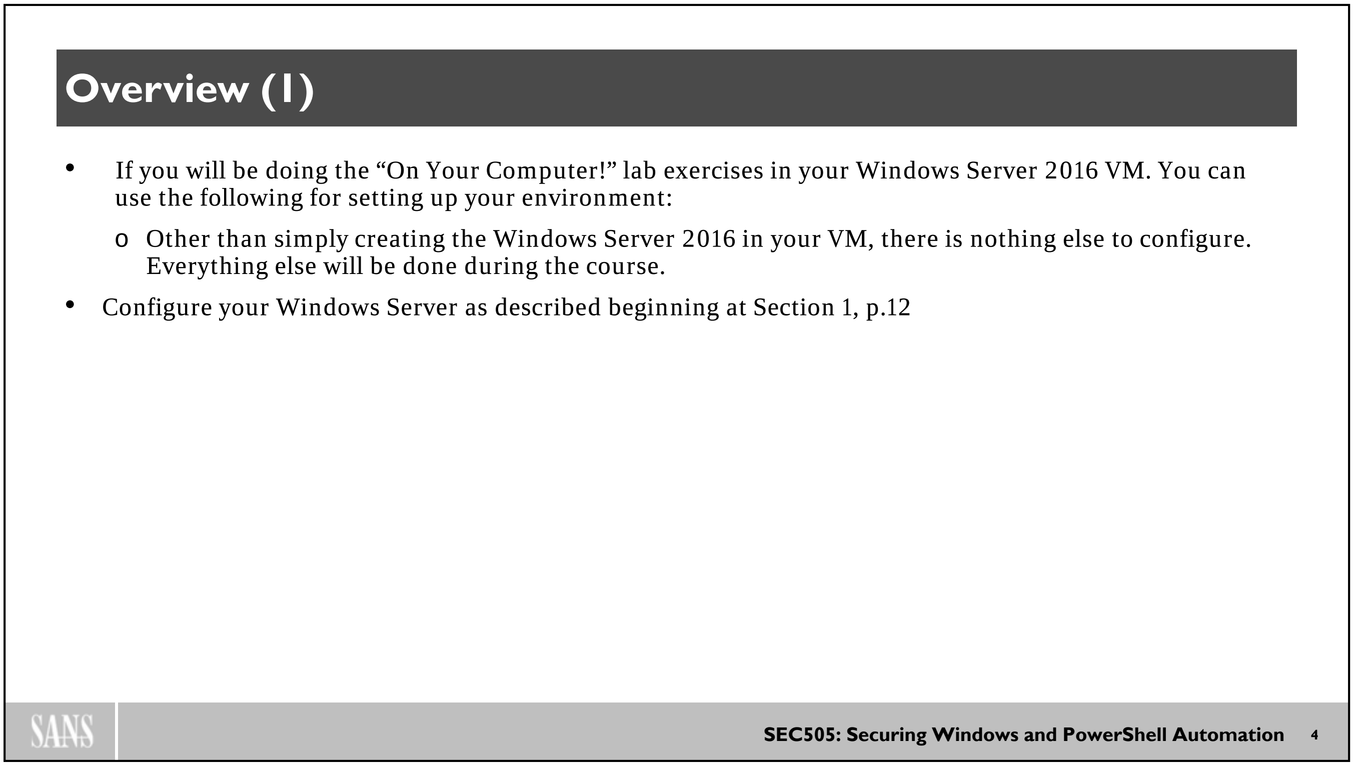
- *Important*: When installing Windows Server, choose the **"(Desktop Experience)"** option for **Windows Server 2016 Datacenter**. (If you have already installed Standard, that is fine, no need to reinstall, as long as you chose the "Desktop Experience" too.)
- If necessary, you can download a free trial version of **Windows Server 2016** from Microsoft as an ISO image file (an ISO file is an exported copy of a CD/DVD disk). You should already have this ISO before attending the course. If necessary, do an Internet search on "site:microsoft.com windows server trial eval" to find the download link to the ISO file on Microsoft's web site.

VMware Software

- SANS provides software licenses to VMware with your course.
- Directions for obtaining your software can be obtained from the **VMware Software License Handout**

URL References

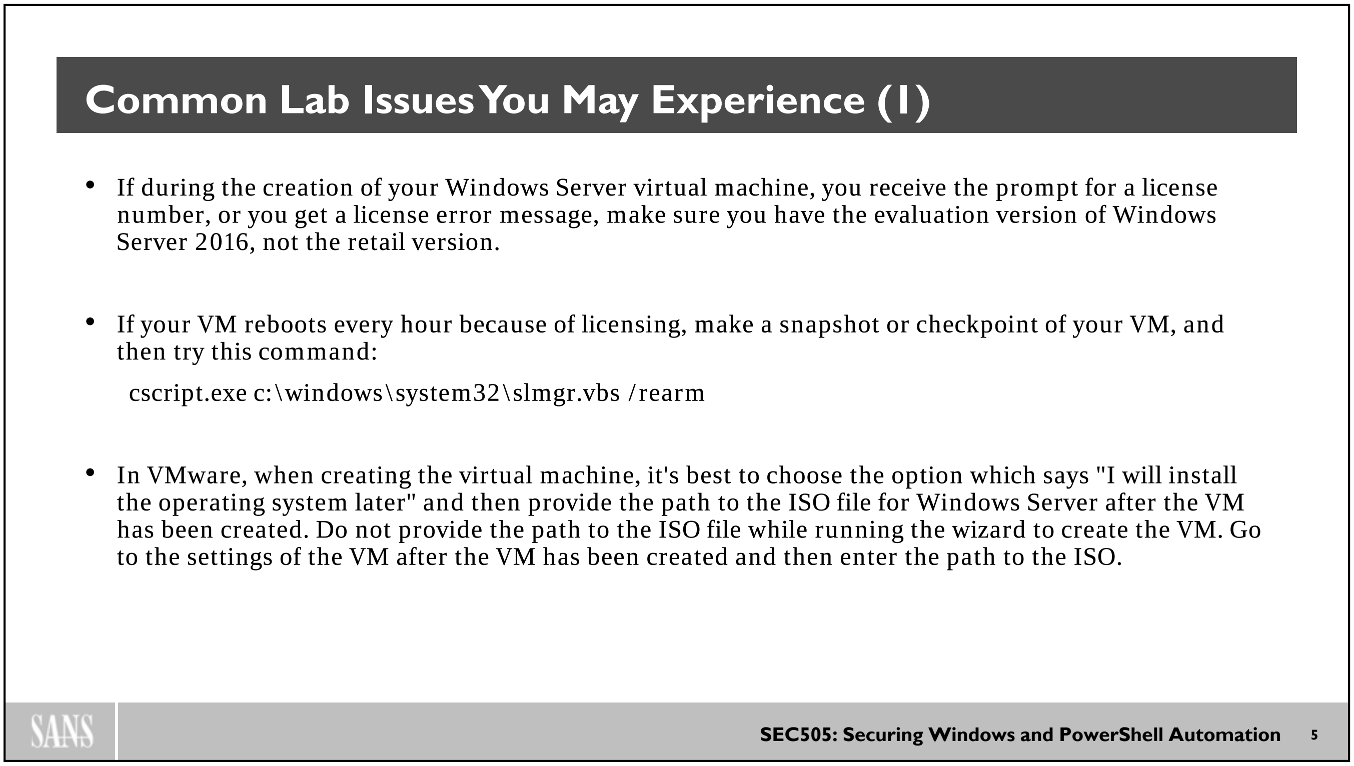
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016



Overview (1)

- If you will be doing the “On Your Computer!” lab exercises in your Windows Server 2016 VM. You can use the following for setting up your environment:
  - Other than simply creating the Windows Server 2016 in your VM, there is nothing else to configure. Everything else will be done during the course.
- Configure your Windows Server as described beginning at Section 1, p.12

This section is intentionally left blank.



Common Lab Issues You May Experience (1)

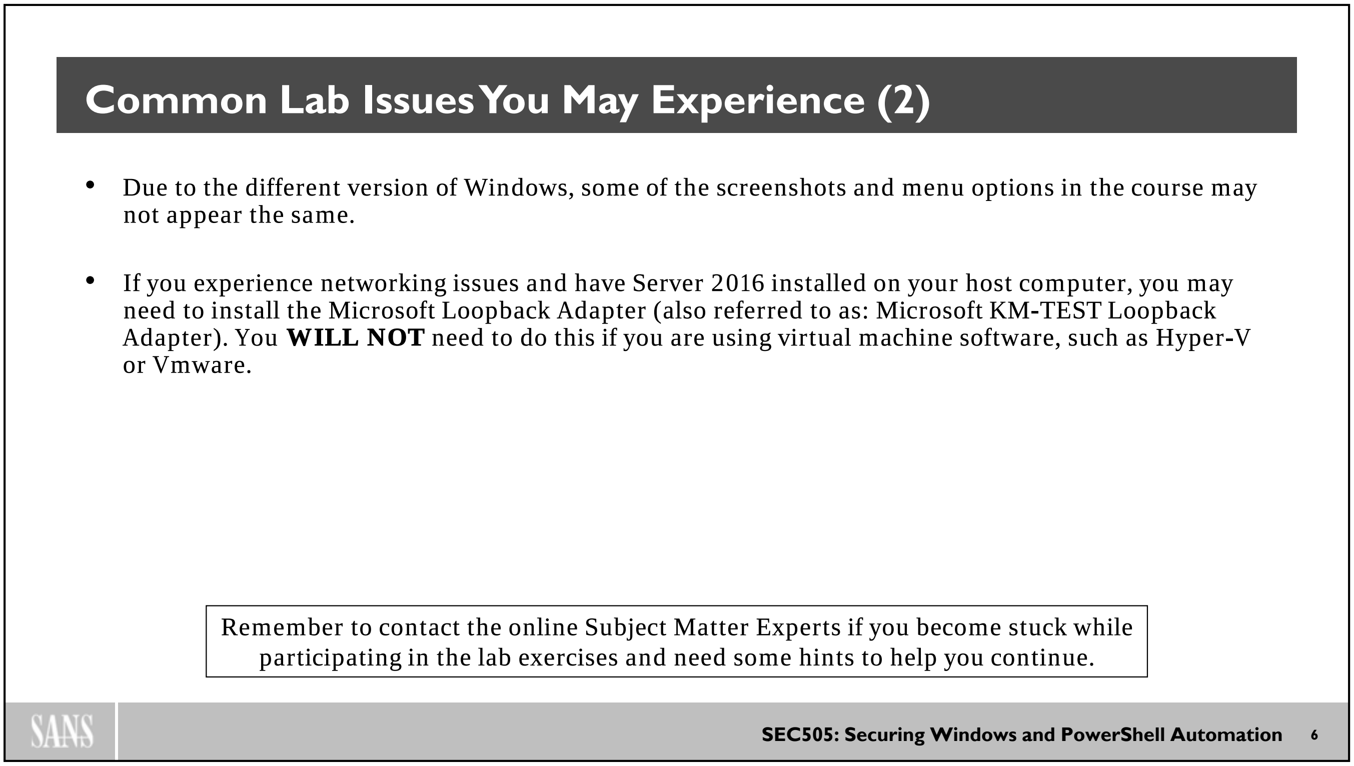
- If during the creation of your Windows Server virtual machine, you receive the prompt for a license number, or you get a license error message, make sure you have the evaluation version of Windows Server 2016, not the retail version.

- If your VM reboots every hour because of licensing, make a snapshot or checkpoint of your VM, and then try this command:

  ```
  cscript.exe c:\windows\system32\slmgr.vbs /rearm
  ```

- In VMware, when creating the virtual machine, it's best to choose the option which says "I will install the operating system later" and then provide the path to the ISO file for Windows Server after the VM has been created. Do not provide the path to the ISO file while running the wizard to create the VM. Go to the settings of the VM after the VM has been created and then enter the path to the ISO.

This section is intentionally left blank.



Common Lab Issues You May Experience (2)

- Due to the different version of Windows, some of the screenshots and menu options in the course may not appear the same.
- If you experience networking issues and have Server 2016 installed on your host computer, you may need to install the Microsoft Loopback Adapter (also referred to as: Microsoft KM-TEST Loopback Adapter). You **WILL NOT** need to do this if you are using virtual machine software, such as Hyper-V or Vmware.

Remember to contact the online Subject Matter Experts if you become stuck while participating in the lab exercises and need some hints to help you continue.

This section is intentionally left blank.