Name Click here to enter name ID Click here to enter id

Blue Team Cookbook Choice

Exercise 9.4

# Instructions

Unlike previous exercises, you will compose and upload your own tutorial document as your homework submission.

*Recommendation*: use the same outline format as your exercises. Start with an Introduction, Overview, and any Setup requirements. End with a Wrap-up (if necessary) and expected Deliverable. Your exercises so far have asked you to provide answers in text fields like this: Click or tap here to enter text. You’re welcome to use such input fields in your tutorial if you choose, but it’s not required. Your tutorial could instead ask for a screenshot or two, as evidence that the learner successfully completed the tasks in your tutorial.

# Overview

Chapter 9 shows several “blue team cookbook” procedures using PowerShell. ***Choose one*** of the following sections in Chapter 9. Write a new tutorial for one of your classmates to follow on their non-domain-joined Windows Server VM, BO-BOBO-*<number>*, to learn how to accomplish your chosen blue-team tasks. *Note*: most of the example commands given in the cookbook are generic. The example commands or scenarios you write in *your* walkthrough must be *specific*, or otherwise *substantially different*, than the cookbook recipes in the textbook. (Don’t plagiarize!)

* Choice: **Reviewing the PowerShell history of all users** and **Inspecting the event log of a remote host** (pp 379-381):
  + Use the bastion VM, HORACE, for your history walkthrough, and use your non-domain-joined server as a base to remotely inspect HORACE’s and SLAYGORE’s event logs.
* Choice: **Monitoring to bypass powershell.exe** (pp 381-382):
  + As part of your tutorial, walk your learner through steps to download and transfer the Sysmon software to their BO-BOBO-*<number>* VM and install it there.
* Choice: **Getting specific firewall rules**, **Allowing PowerShell communication only for private IP address ranges**, and **Isolating a compromised system** (pp 383-355):
  + Do not actually isolate your system! Also don’t modify the firewall settings on HORACE! Your learner should only modify firewall rules on their BO-BOBO-*<ncumber>* VM.
  + Include instructions for rolling back firewall changes made on their BO-BOBO-*<number>* VM.
* Choice: **Check the digital signature of a file or a script** (pp 356-358) and chapter 11’s **Preventing unauthorized script execution with code signing** (pp 436-443):
  + You might find it helpful to referemce PowerShell’s about\_Signing help topic.
* Choice **Checking file permissions of files and folders** through **Enabling a local account** (pp 388-390):
  + As part of your tutorial, find a couple of *benign* services and processes that aren’t running by default. Ask your learner to start those services or launch those processes, so that they can later stop them. Also, walk your learner through creation of a new local user account, so that they can later disable/enable that account.
* Choice: **Checking whether a specific port is open** and **Showing TCP/UDP connections and their initiating processes** (pp 392-393):
  + As part of your tutorial, walk your learner through an investigation of the discovered ports and connections, and making judgments about whether their associated services are necessary or optional.
* Choice: **Searching for downgrade attacks using the Windows event log** and **Preventing downgrade attacks** (pp 393-394):
  + As part of your tutorial, walk your learner through an actual downgrade attack as shown in Chatper 4 (pp 163-164), so that there will be an audit trail of at least one downgrade attack they can detect, and they can verify the efficacy of their prevention attempt.

# Deliverable

Upload your tutorial document to I-Learn Canvas.