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

Red Team Cookbook Choice

Exercise 8.4

# 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 8 shows several “red team cookbook” attack procedures using PowerShell. ***Choose one*** of the following sections in Chapter 8. Write a new tutorial for one of your classmates to follow on their non-domain-joined VMs, BO-BOBO-*<number>* or DONPATCH-*<number>*, to learn how to accomplish your chosen red-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: **Script Execution** (pp 344-345):
  + *Evading execution policies*, and
  + *Opening a PowerShell command line to execute a command* (without opening a new shell), and
  + *Avoid loading settings from the PowerShell user profile*.
* Choice: **Downloading files** (pp 346-350):
  + *Dowloading a* [script] *file using PowerShell cmdlets* (Invoke-WebReqest, Invoke-RestMethod, Start-BitsTransfer), and
  + *Downloading a* [script] *file and executing it in memory*, and
  + *Downloading and executing a* [script] *file using .NET classes*.
* Choice: **Persistence** (pp 351-355):
  + *Establishing persistence using the registry*, and
  + *Establishing persistence using the startup folder*, and
  + *Establishing persistence using the PowerShell profile*, and.
  + *Establishing persistence using WMI*.
* Choice: **Defense evasion** (stealth tactics, pp 356-358):
  + *Avoiding creating a window on the desktop*, and
  + *Executing a Base64-encoded command using powershell.exe*, and
  + *Converting a string into a Base64 string*, and
  + *Converting a Base64 string into a human-readable string*.
* Choice **Defense evasion** (invasive tactics, pp 359-360):
  + *Performing a downgrade attack*, and
  + *Disabling Microsoft Defender*, and
  + *Clearing logs*.
* Choice: **Discovery** (pp 361-365):
  + *Enumerating users and groups* (local and domain), and
  + *Retrieving information about the current system*, and
  + *Enumerating network-related information*, and
  + *Enumerating domain information*.
* Choice: **Command and Control (C2)** (pp 366-368):
  + *Opening a reverse shell*. (*Note*: use the bastion VM, HORACE, as the C2 listener.)
* Choice: **Exfiltration** (pp 368-369):
  + First, walk through installing and running a web server on one of your non-domain machines, either your Windows Server (BO-BOBO-<number>) or Linux (DONPATCH-<number>). Provision an upload subfolder in your web server’s “document root” folder.
  + *Exfiltrating a file and uploading it to a web server*.
  + (In your walkthrough, after you exfiltrate a file, remember to show how to decode it.)

# Deliverable

Upload your tutorial document to I-Learn Canvas.