Home

Welcome to the SANS SEC504 Lab Wiki!

This wiki is your guide to lab exercises in SANS SEC504. In order to keep labs current, to make them more accessible (cut and paste!), and to present the steps in color with rich context, we present the material here in HTML format. You will also will get a hard copy of the printed materials to keep as an heirloom (and to bring into an exam center when you take the GIAC exam).

> *This lab wiki is a work in progress, and is frequently revised by the course authors. This is beneficial to all, since you continue to get updates to lab material as we improve the quality of the exercises, correct typos, and add new exercises.*

Accessing the Digital Edition of the Lab Wiki

To access the digital edition of the lab wiki from the Slingshot Linux VM, open the Firefox browser. The home page will display this text, and allow you to navigate to the course lab exercises.

Similarly, you can access the digital edition of the lab wiki from the class Windows 10 VM as well. Open the Chrome browser and the home page will display this text.

Updating the Lab Wiki – Linux

To update the lab wiki on the Linux VM, make sure your Slingshot Linux VM distributed with the class material is connected to the internet. See the Connecting to the Network (Connecting-to-the-Network.html) guide for instructions.

Once connected, open a terminal prompt and run the following command:

```
sec504@slingshot:~$ update-wiki
```

That's it! With this one step you will always have the most current lab materials.

Updating the Lab Wiki – Windows

To update the lab wiki on the Windows 10 VM, make sure your Windows 10 VM distributed with the class material is connected to the internet. See the Connecting to the Network (Connecting-to-the-Network.html) guide for instructions.

Once connected, open a PowerShell Prompt as an Administrator and run the following command:

```
PS C:\WINDOWS\system32> update-wiki.ps1
```

> *Note: You must open a PowerShell Prompt as an Administrator to update the wiki content, not a Command Prompt!*

That's it! With this one step you will always have the most current lab materials.

Conventions

The following typographical conventions are used throughout the labs:

- *Italic*
  - Indicates new terms and items of emphasis.
- `Constant width`
  - Used for terminal output and within paragraphs to refer to tools or other elements such as variables, function names, statements, keywords, etc.
- | (vertical bar)
  - The vertical bar is used to indicate steps necessary for navigating through menus (Edit | Paste)

Code blocks are used to denote output from tools. Content that is bold represents commands you type. For example:

```
# run_this_command
output from the tool
```

In some cases, the commands you type will call for information that you supply (e.g., that we don't know). In these cases, the content that you supply is noted in italics: `yourinput`. Replace *yourinput* with the information you supply as described in the exercise.

> *This icon signifies a tip, suggestion, warning, or a general note.*

Video Walkthrough

Watch the accompanying video instructions (/videos/000%20Accessing%20the%20Lab%20Wiki/) for additional information.

SANS SEC504

Accessing the Lab Wiki

Joshua Wright
josh@willhackforsushi.com

(/videos/000%20Accessing%20the%20Lab%20Wiki/)

Course and Lab Feedback

We are always excited to hear your feedback on the course materials. Is there a bug we need to squash? Do you have a suggestion for a new awesome tool that we just ***have*** to see? Please let us know.

https://www.sec504.org/feedback (https://www.sec504.org/feedback)

You can also reach out to Josh or Mike directly:

- Joshua Wright – jwright@willhackforsushi.com (mailto:jwright@willhackforsushi.com)
- Mike Murr – mmurr@codeforensics.net (mailto:mmurr@codeforensics.net)

Thank you!!

Update: 20191010-002