# Content Author Writing Guide
# Virginia Cyber Range

**1880 Pratt Drive, Suite 2006**

**Blacksburg, VA 24061**

**Version 1.0 Updated 3/20/2020**

# Table of Contents

# 1. Introduction

Congratulations! You are joining an august group of authors supporting the Virginia Cyber Range and our mission to enhance cybersecurity education in our public high schools, colleges, and universities. Your efforts are very much appreciated!

## 1.1 PURPOSE

The purpose of the Virginia Cyber Range (VACR) Content Author Writing Guide is to assist you as an author in creating, repurposing, or reformatting your cybersecurity course materials for inclusion in the Virginia Cyber Range's Courseware Repository. This guide will provide the necessary resources, tips, and advice to ensure your successful navigation throughout the authoring process.

## 1.2 SCOPE

This guide pertains specifically to content authors who have a signed Author Agreement, discussed in *Section 2. Becoming an Author*, with the VACR. All content authors should become familiar with this guide. Any questions concerning the guide should be directed toward the Lead Content Coordinator at the VACR; contact information provided below.

If you are interested in becoming an author, please read the next section for details on how to do so. You may also contact us at:

Virginia Cyber Range
1880 Pratt Drive, Suite 2000
Blacksburg, VA 24061
PH: 540-231-4759
Email: content@virginiacyberrange.org

# 2. Becoming an Author

There are two ways you can become an author in the Virginia Cyber Range:

1. **Informal process**. You merely provide your courseware to us for free and we post it to the repository after reviewing its contents to ensure no copyright infringements exist. If interested, please contact us; see *Section 1.2 Scope* for contact information. It's as simple as that!
2. **Formal process**. If, however, you would prefer to be compensated monetarily for your content, you would need to submit an abstract for your proposed content, the first step in the formal process. Abstract submission and subsequent steps in this formal process are addressed in the remainder of this section.

## 2.1 ABSTRACT SUBMISSION

In order to become a content author for the VACR, you must submit an online abstract and other documents as required; this is the first step. You can find the abstract, eligibility requirements and other pertinent information on our Call for Courseware page here. Once submitted, the abstract will be reviewed. This is discussed in the next section.

## 2.2 ABSTRACT REVIEW

Once you have submitted your abstract and other required documents online, a content abstract review subcommittee, comprised of university and college faculty, will be convened. Using specific assessment criteria, this subcommittee will review your abstract and approve it for inclusion in the VACR Courseware Repository. Please keep in mind, the subcommittee can also vote not to approve an abstract for many reasons based on the assessment criteria, especially if the proposed content is already part of the repository or it does not meet our cybersecurity education needs.

If the abstract is approved, the subcommittee determines the grant amount to award you as the author to compensate you for creating, repurposing, and/or reformatting your cybersecurity course materials for inclusion in the Virginia Cyber Range's Courseware Repository. Afterwards, an Author Agreement is drafted and sent to you for review; this is a legal contract between you and the VACR which includes completion date and compensation amount. You will be required to sign the Author Agreement and fill out a W-9 tax form before moving on to the next and most important step: writing content.

The remainder of this guide *Section 3. Writing Content*, *Section 4. Miscellaneous*, and *Section 5. Lessons Learned* will be the keys to your success during the submission, editing, and review of your content. You will be required to format your content using the required VACR templates;

these templates will be provided to you. This process can be time-intensive, requiring a back and forth between you (author) and your assigned content coordinator to ensure relevant, accurate, consistent and quality content until it gets posted in the VACR Courseware Repository. Depending on how your Author Agreement is written, you will be compensated throughout the process, e.g., as each module is completed.

# 3. Writing Content

The following guidance laid out in this guide pertains to VACR content authors with a signed Author Agreement who are creating, repurposing, and/or reformatting cybersecurity course materials for inclusion in the Virginia Cyber Range's Courseware Repository.

Please note we attempted to include as many scenarios and examples as possible with respect to authoring a course, module, lesson, lab exercise, etc.; however, it is impossible to enumerate them all. Please contact your content coordinator for any special or unique requirements.

Finally, whenever possible we have included tips (**TIP**:), important comments (**IMPORTANT**:) and notes (**NOTE**:) throughout to assist you during the editing process to get your attention and focus you on critical information to ensure your success.

## 3.1 TEMPLATES

In accordance with the signed Author Agreement, content authors are required to format content using the templates provided by the Cyber Range. You should have received an email giving you access to the content templates as well as a location (Google Drive folder) to post your completed content. Please contact the Cyber Range if this is not the case.

> **TIP**: *Do not use Google Docs to edit* the provided templates, as Google Docs have been known to drastically alter document formatting. Doing so may likely cause you extra work and rework.

All required content files, described in the next section, must be authored using Microsoft applications (Word and PowerPoint) to ensure standardized formatting. The Cyber Range has templates for all required content files to also ensure this standardization. Authors may include documents using other formats (e.g., pdf) that supplement and support the content; however, in these cases, it is highly recommended you carefully consider submitting supplemental content with format types that are widely used.

Several Word templates are provided to cover the majority of the various files one would expect to see in a course. The following *required* Word templates will be provided to you as an author to use to develop content for your courseware:

- Course Syllabus
- Module Description
- Lesson Plan
- Exams/Quizzes
- Homework
- Lab Exercise

Additionally, there is a *required* PowerPoint template provided for Lesson Presentation Slides. If, however, none of the provided templates appear to meet your needs for supplemental (not required as discussed in the next section) files needed in your courseware, please consult with Cyber Range personnel for any special document requirements early on.

### 3.1.1 Getting familiar with Word templates

Ensure you carefully read all of the guidance in the templates. There are some important information and key points in them that can help you edit and avoid reediting your content.

In general, templates are broken into four sections:

1. **Header**.
    a. After editing the template document, the top portion of the header gets deleted by YOU, i.e. the portion that says, *“[All red text should be replaced by course author and font color changed to black.].”*
    b. The rest of the header stays as is, i.e. *“[Any blue text should be replaced by instructor using material and font color changed to black.].”*

2. **Student section**. This is what the student would see should an instructor using your content provide it to them. This would include everything from below the header until you see the solid line followed by a message to the perspective instructor, i.e.,

   “

   ---

   [This portion of the lesson plan is provided for instructors that will be using this lesson plan and associated material in their class.]”

   *DO NOT delete this line or the message below* it to the instructor. All black text in this section should remain intact and in the order it is presented.

3. **Faculty instruction section**. This section is meant for instructor eyes only along with any text that is typed in blue font throughout the document. Again, all black text in this section should remain intact and in the order it is presented.

4. **Footer**. You should add the current year (e.g., 2020), your name and any title credentials (e.g., Phd, CISSP) if desired in the footer. PLEASE remember to change the font to black for the year and your name and unbold the font. More details on this footer and other required citations are provided in *Section 3.3.5 Required Citations*.

You will also notice three font colors throughout the templates:

1. Black. Anything in black font should remain as is.
2. Red. When you have completely edited a template and are ready to submit it for review, ALL red font should be removed or changed to black before doing so. One exception, of

course, is the top line of the header as discussed above in the Header section; you should delete that in its entirety before submitting.

3. Blue. Feel free to provide notes to the instructors throughout your content files; in fact, we encourage it. We mostly see these used in the lesson plans and lab exercises. Recall also from the Header section, part of the header will contain this blue font, so that instructors using your content can modify it for their needs. See *WRITING LAB TASKS* in *Section 3.4.3 Lab Exercise Area Formatting and Other Considerations* where **Use of Notes to Instructors** goes into may details regarding this topic.

## 3.1.2 Getting familiar with the PowerPoint template

Just like the Word templates, the PowerPoint slides template contains some important information and key points to assist you with editing. It is broken into the following sections:

1. **Lesson Title slide (required).** There are two required footers on this slide. One discusses the use of logos while the other is similar to the footer in the Word templates. Like the one in the Word templates, the second and bottommost footer requires editing by you. More details on these footers and other required citations are provided in *Section 3.3.5 Required Citations*.
2. **Lesson Objectives slide (required).** This slide will ALWAYS be the second slide in all lesson presentation slide decks. There is a footer similar to the one in the Word templates on this slide and the remainder slides that you will need to edit in the master slide.
3. **Lesson slides.** Use as many slides as you need to present the lesson material. Ensure you have enough content on the slides, so that a faculty member with the requisite background understands your intent. Do not be afraid to add more explanatory information in the NOTES section. These slides can be formatted as you like; however, ensure you are consistent with using the same fonts throughout.
4. **Questions? slide (required).** This shall be included as the last slide in all lesson presentation slides.

As in the Word templates, there are some guidance and helpful advice in the PowerPoint template; please read through the slides carefully. Make sure you understand what is being asked of you; ask questions if you do not understand.

> **TIP**: If you are not familiar with using or manipulating the Master Slide in PowerPoint, ask for assistance from Cyber Range personnel or Google it. Once you get the hang of it, it's pretty easy to do.

## 3.2 REQUIRED CONTENT FILES

Per the Author Agreement, you have agreed to provide specific required content files based on the type of content you are submitting. The following sections walk you through all required and optional files you may author. We provide you with templates for all of these files.

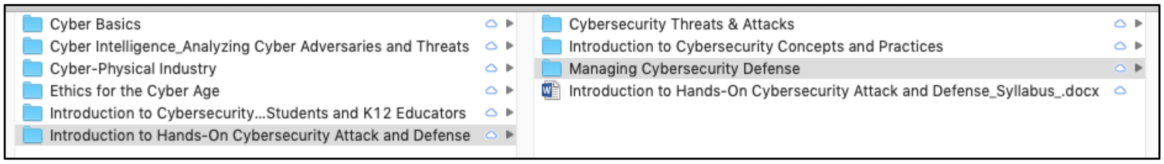
### 3.2.1 Course

Every course, at a minimum, requires the following:

- Course Syllabus (Word template provided)
- Two or more Modules

Other optional files that may accompany a course include, but are not limited to:

- Exams/Answer Keys
- Projects (use homework template)



Cyber Basics
Cyber Intelligence_Analyzing Cyber Adversaries and Threats
Cyber-Physical Industry
Ethics for the Cyber Age
Introduction to Cybersecurity...Students and K12 Educators
Introduction to Hands-On Cybersecurity Attack and Defense

Cybersecurity Threats & Attacks
Introduction to Cybersecurity Concepts and Practices
Managing Cybersecurity Defense
Introduction to Hands-On Cybersecurity Attack and Defense_Syllabus_.docx

As you can see from the image above, the highlighted course **Introduction to Hands-On Cybersecurity Attack and Defense** has a syllabus (required) and three modules (at least two required). For this course example, there are no other optional documents; however, depending on YOUR course's requirements they may be submitted, e.g., course exam.

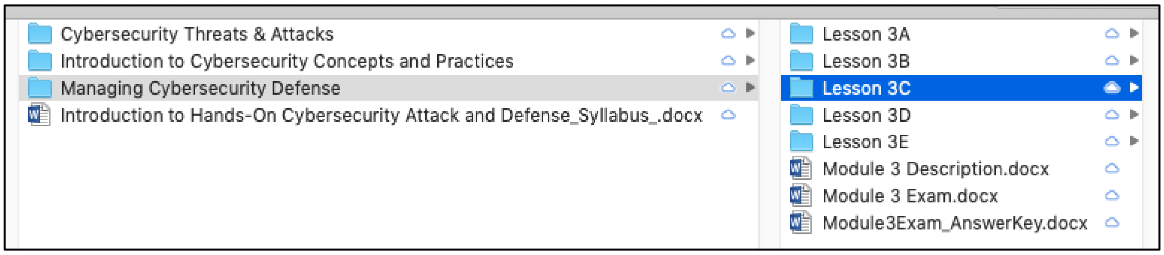
### 3.2.2 Module

Every module, at a minimum, requires the following:

- Module Description (Word template provided)
- Two or more Lessons

Other optional files that may accompany a module include, but are not limited to:

- Module exams/quizzes & answer keys
- Lab exercises
- Homework assignments
- Projects (use homework template)



Cybersecurity Threats & Attacks
Introduction to Cybersecurity Concepts and Practices
Managing Cybersecurity Defense
Introduction to Hands-On Cybersecurity Attack and Defense_Syllabus_.docx

Lesson 3A
Lesson 3B
Lesson 3C
Lesson 3D
Lesson 3E
Module 3 Description.docx
Module 3 Exam.docx
Module3Exam_AnswerKey.docx

As you can see from the image above, the **Managing Cybersecurity Defense** module has a module description (required), module exam/answer key (optional), and five lessons (at least two required).

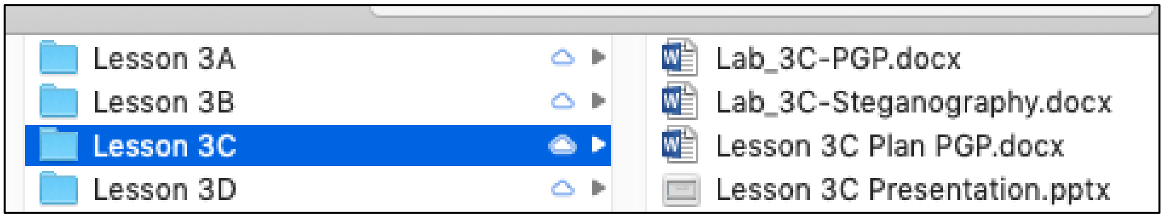
### 3.2.3 Lesson

Every lesson, at a minimum, requires the following:

- Lesson plan (Word template provided)
- Lesson presentation slides (PowerPoint template provided)

Other optional files that may accompany a lesson include, but are not limited to:

- Exams/quizzes
- Labs
- Homework assignments
- Projects (use homework template)



Lesson 3A
Lesson 3B
Lesson 3C
Lesson 3D

Lab_3C-PGP.docx
Lab_3C-Steganography.docx
Lesson 3C Plan PGP.docx
Lesson 3C Presentation.pptx

As you can see from the image above, Lesson 3C has a lesson plan **Lesson 3C Plan PGP** (required), lesson presentation slides **Lesson 3C Presentation** (required), and two optional lab exercises.

### 3.2.4 Lab Exercise

Every lab exercise, at a minimum, requires the following:

- Lab Exercise handout (Word template provided)

If the lab exercise has associated questions for the students to answer, then an accompanying lab exercise answer key must also be provided. This is described in the lab exercise template.

> **TIP**: If you are authoring lab exercises that use virtual machines (VMs), please refer to *Section 3.4 Writing Lab Exercises*, which provides in-depth detail on writing them.

### 3.2.5 Exams/Quizzes

Every exam/quiz, at a minimum, requires the following:

- Exam/Quiz (Word template provided)

As described in the template for the exam/quiz, an accompanying exam/quiz answer key must also be provided. This is described in the exams/quizzes template.

### 3.2.6 Homework

Every homework assignment, at a minimum, requires the following:

- Homework handout (Word template provided)

As described in the template for the homework assignment, an accompanying answer key must also be provided. This is described in the homework template.

> **NOTE**: Use this template for project assignments.

## 3.3 EDITING PROCESS

BEFORE you begin authoring any content, ensure you have looked at and understand all of the required content files you will need to submit described in the previous section. Additionally, it is recommended you open and read through each template to understand the requirements.

> **TIP**: If you don't already have an account in the Cyber Range repository, it is highly recommended you do so to take a look at other content that has already been approved and posted. This will give you an idea of expectations for your content. Please see *Section 3.4.1 Getting a Virginia Cyber Range Account & Creating a Course* to get see how easy it is to request an account.

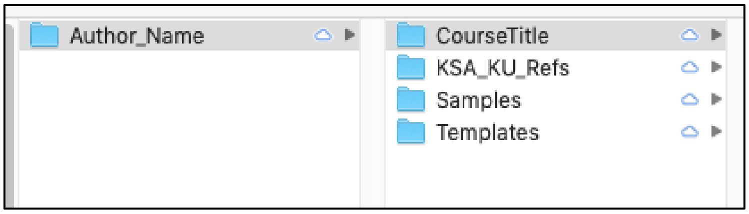
### 3.3.1 Content File Structure

In order to keep the editing process organized, the content file structure is laid out logically, i.e., course → modules → lessons. When you are given access to YOUR specific Google Drive, your folder will be labeled with the initial of your first name followed by your last name; this is done by personnel at the Cyber Range. For example, Joanna Smith would have a folder named JSmith.

> **IMPORTANT**: *While collaboration and sharing are normally encouraged in academia, you are NOT allowed to give anyone permissions to the content in YOUR specific Google Drive. You have entered into a legal contract with the Cyber Range and we own all rights to this drive. If you have determined you would like for a teaching assistant (TA) or other*

*collaborator(s) to assist you in writing content, please contact your content coordinator to discuss this request.*

Once inside YOUR folder, you should see several subfolders to include one labeled with the name of the content you have agreed to submit per the Author Agreement; this is also done by personnel at the Cyber Range. In the image below, CourseTitle would be replaced with the title of your content. The other subfolders are materials to assist you during the editing process.



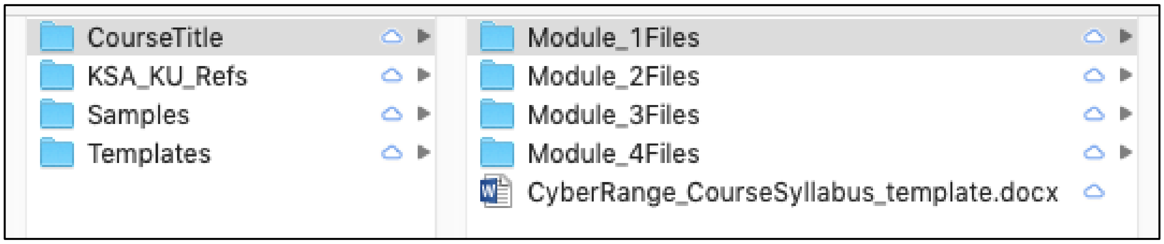
Author_Name

CourseTitle
KSA_KU_Refs
Samples
Templates

The material in these subfolders are explained elsewhere in this document; however, for convenience here is a brief description of each:

- **KSA_KU_Refs** – This folder contains reference documents to assist you with adding the NICE Knowledge, Skills, and Abilities (KSAs) and NSA/DHS Knowledge Units (KUs) to the various content documents. This is discussed more in detail in *Section 3.3.6 Skill Mappings*.
- **Samples** – This folder contains sample documents for you to review.
- **Templates** – This folder contains the templates you will use for your content.

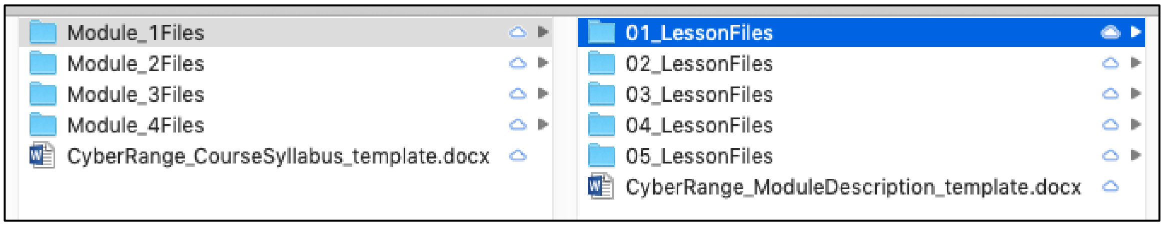
Inside your folder, you will then see the file structure for your content. In the example image below, you see several module folders as well as the template for the course syllabus. Keep in mind, every course, module, workshop, lesson, lab exercise, etc. will be different. So, it will be up to you to delete or add whatever folders are needed for your content.



CourseTitle
KSA_KU_Refs
Samples
Templates

Module_1Files
Module_2Files
Module_3Files
Module_4Files
CyberRange_CourseSyllabus_template.docx

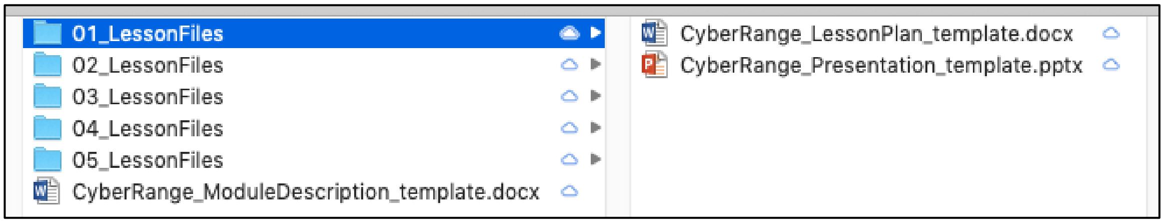
Initially, you will see several lesson folders in each module folder; add or delete as needed. See below image.



Module_1Files
Module_2Files
Module_3Files
Module_4Files
CyberRange_CourseSyllabus_template.docx

01_LessonFiles
02_LessonFiles
03_LessonFiles
04_LessonFiles
05_LessonFiles
CyberRange_ModuleDescription_template.docx

Finally, in each lesson folder it will be up to you to add the required documents, keeping in mind that there should always be at least two files in each lesson, i.e., a lesson plan and presentation slides for that lesson, as shown in the image below.



01_LessonFiles
02_LessonFiles
03_LessonFiles
04_LessonFiles
05_LessonFiles
CyberRange_ModuleDescription_template.docx

CyberRange_LessonPlan_template.docx
CyberRange_Presentation_template.pptx

## 3.3.2 Folder/File naming

There are no restrictions on naming your folders or files; however, please consider using names that would make sense to most people. Also, use some sort of numbering scheme; this ensures editing is done in chronological fashion. There is no need to include the words module or lesson (but it is helpful); feel free to use only the actual module or lesson name preceded/followed by a number. It is preferable that you include more information about what the document contains in the filename without getting too lengthy. The following are a few examples (Good, Better, and Best) of **folders** and filenames:

**Good Example**

- **Module_1Files**
    - **01_LessonFiles**
        - 01_LessonPlan.docx
        - 01_LessonSlides.pptx
    - **02_LessonFiles**
        - 02_LessonPlan.docx
        - 02_LessonSlides.pptx
    - Module_1Description.docx

**Better Example**

- **Module_1**
    - **Lesson 1A**
        - Lesson 1A Plan_Quick View of Trends.docx
        - Lesson 1A Presentation.pptx
    - **Lesson 1B**
        - Lesson 1B Plan_Gen Security Concepts.docx
        - Lesson 1B Presentation.pptx
    - Module_1Description.docx
    - Module_1 Exam.docx
    - Module_1 ExamKey.docx

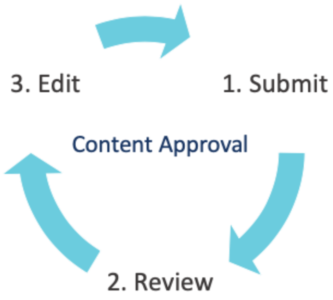
**Best Example**

- **Module 1_Reconnaissance**
    - **Lesson 1_Passive and Active Footprinting**
        - Passive and Active Footprinting LessonPlan.docx
        - Passive and Active Footprinting.pptx
        - Passive and Active Footprinting Lab Exercise.docx
    - **Lesson 2_Competitive Intelligence**
        - Competitive Intelligence Lesson Plan.docx
        - Competitive Intelligence.pptx
        - Competitive Intelligence Homework.docx
        - Competitive Intelligence Homework_Key.docx
    - Reconnaissance Module_Description.docx
    - Reconnaissance Module_Exam.docx
    - Reconnaissance Module_ExamKey.docx

### 3.3.3 Submitting your first files

Your first inclination might be to submit your entire course, module, etc. all at once. This is not a recommended plan and highly discouraged. Instead, submit only the documents from the first lesson in your content for example. At a minimum, submit the edited lesson plan and presentation slides, using the provided templates after carefully reading the guidance contained within them. Looking at the provided sample documents in the **Samples** folder can also assist you with authoring expectations. Also, as recommended previously, get an account in the Cyber Range repository to take a peek at other content to see what approved content looks like. Again, look at *Section 3.4.1 Getting a Virginia Cyber Range Account & Creating a Course*, which explains the steps to request an account.

Once you notify your Cyber Range Content Coordinator you have files for them to review, we recommend you DO NOT move on without getting feedback first, since you do not want to have to correct the same issue(s) throughout. After it has been reviewed by your content coordinator, you will be notified if there are any required edits by you. If there are, then you will need to correct and resubmit. This process cycle of submit – review – edit continues until the content is approved by the Cyber Range as shown in the image below.



> **TIP**: Once you have a “blessed” document for each of the various templates, it is highly recommended you use this as a starting point for the next one. For example, after submitting your first lesson plan and lesson presentation slides, use these two files as the starting point for follow-on lessons. This way you are guaranteed to have correct footers, slide masters, etc., and you will not have to edit or correct these standard requirements each time.

This process continues with the remainder of the files you plan to submit per your Author Agreement.

## 3.3.4 Fonts

### *TYPES*

There are basically three different font types used throughout the templates: Arial, Calibri and Courier New. Arial is used primarily in Word documents, while Calibri is the standard in PowerPoint files. Courier New is used solely for commands (e.g., Linux/Unix, Windows, macOS, powershell, etc.) and programming/scripting languages (e.g., Python). The key when using fonts is consistency. Regardless of which font you prefer, Arial or Calibri, please ensure you are consistent with the font type.

### *FONT SIZES*

Font sizes may vary depending on which template you are using. It is recommended you use the font sizes (and types) you will encounter in the Word templates. For example, in the lesson plan template the title of the lesson is at 14pt while the remainder of the lesson plan (subsections and text) are at 11pt.

In the PowerPoint template, this is where you may deviate from a standard font size. Again, it is recommended you use the font sizes (and types) you will encounter in this template; however, at times, slide titles or text on a slide may be too long and you may wish to make the font size smaller to fit it on one line.

Finally, whenever you cite sources on slides, these citations should be at 10pt or smaller. You need to cite sources, but the citations are not emphasis of the slide; this is why we recommend using a very small font size.

### *SPECIAL FONT CONSIDERATIONS WHEN USING COMMANDS OR CODE SNIPPETS*

If you are using commands or snippets of code, you must use the Courier New font type. For example, you might see the following in a lab exercise or slide presentation:

> Execute this command: **`cat file1 file2 > newfilename`**
>
> **NOTE**: There will be *much more detail* on using commands or snippets of code in *Section 3.4 Writing Lab Exercises*.

### 3.3.5 Required Citations

*FOOTER CITATIONS*

Standard footer citation. When you open any of the templates, you should notice the following required standard footer citation in both Word (all pages) and PowerPoint (slide 2 and beyond) templates:

© YEAR Virginia Cyber Range. Created by YOUR NAME. (CC BY-NC-SA 4.0)

You should change the word YEAR to the current 4-digit year, e.g., 2020. Where you see YOUR NAME, you should add your name, any title credentials (e.g., Phd, CISSP), and organization affiliation (if desired). Here are a few examples of what the footer may look like after editing:

© 2020 Virginia Cyber Range. Created by Jane Smith, Ph.D., CISSP, ODU. (CC BY-NC-SA 4.0)

© 2020 Virginia Cyber Range. Created by Jane Smith, Ph.D., CISSP. (CC BY-NC-SA 4.0)

© 2020 Virginia Cyber Range. Created by Jane Smith. (CC BY-NC-SA 4.0)

You should note that all content for which the Virginia Cyber Range provides grants will fall under a Creative Commons Attribution, Non-Commercial, Share-Alike license. For more details on this licensing model, visit https://creativecommons.org or click on the CC BY-NC-SA 4.0 link above.

Title Slide footer citations. You will see two required footer citations on the Title slide in the PowerPoint template. The first one is the following logos disclaimer footer:

> "All logos used are the property of their respective trademark owners. Their use in these educational materials is not authorized by, sponsored by, or associated with the trademark owners. No endorsement of the trademark owners by the creator of or educational institution is given or should be inferred."

This text should remain intact, unedited and on the title slide even if no logos are used; it is just required boilerplate language. The second footer is very similar to the standard footer and requires editing by you as the author. This is the title slide creative commons citation:

> © YEAR Virginia Cyber Range. Created by YOUR NAME. This course content is provided under an Attribution-NonCommercial-ShareAlike 4.0 International Creative Commons License (https://creativecommons.org)

This footer merely spells out for the potential user what CC BY-NC-SA 4.0 actually means. Again, this should remain intact, unedited with the exception of the YEAR and YOUR NAME and on the title slide.

> **TIP**: If you are unfamiliar with Creative Commons licenses, take some time to look at and get acquainted with the various CC licenses and examples.

### *CITING IMAGES*

Let's face it, slides with just words on them tend to be boring and most students are visual learners. Many faculty authors choose to add images to their slides to reinforce concepts and enhance the learning experience for their students. While most use of copyrighted material is allowed under Fair Use, just as you would ask students to cite sources for their papers and projects, you must do so for any images used in your slides.

Minimum requirements. At a minimum, please ensure the following when citing images:

- Add words to the effect of "Image source: URL" below the image.
- *The URL should take the reader to the image or the webpage where the image is actually located NOT to the main homepage*.
- Font should be 10pt or less; See example below.

BUT WHEN SHE TRACED THE KILLER'S IP ADDRESS... IT WAS IN THE 192.168/16 BLOCK!
GASP!

Cartoon courtesy of xkcd: https://imgs.xkcd.com/comics/campfire.png

Of course, you can always get very specific when citing images as you will see in these next examples.

Images/photos you created. If you use a photo taken or an image created by you, the format would be as follows:

© Your Name BY-NC-SA 4.0

Therefore, a photo taken by Jane Smith would be cited as follows:

© Jane Smith BY-NC-SA 4.0

Images/photos created by someone else. If you use a photo taken or an image created by someone else, the format would be as follows:

Original Creator Name or Username. Image Name. Access Date <URL>

So, if you found the photo Fishing Lake Ohrid online on February 3, 2020 and will use it in your content, it would be cited as follows:

> Jason Rogers. Fishing Lake Ohrid. 03 Feb 2020. <https://www.flickr.com/photos/17642817@N00/2340896333>

Creative Commons images. When you click on the URL for the Fishing Lake Ohrid photo, you should notice there are “Some rights reserved” for this image. This image is actually licensed under Creative Commons Attribution 2.0 Generic (CC BY 2.0). While the above citation is acceptable, the more proper way to cite this Creative Commons image/photo would be as follows:

> Fishing Lake Ohrid by Jason Rogers is licensed under CC BY 2.0.

Thus, the format for creative commons images is as follows:

> Title of image/video [linked to original image] by Author [linked to profile page] is licensed under [linked to license deed].

Public Domain Images. If you are using any public domain images in your slides or any other content you are authoring for the Cyber Range, your attribution should follow this format:

> Title of work [linked to original image] by Author, Date (if known, or n.d. if not known). Public Domain.

So, an example of a public domain image citation would be as follows:

> Two yellow autumn leaves by alegri, 2019-03-05. Public Domain.

### *CITING OTHER PEOPLE’S IDEAS AND QUOTING VERBATIM*

At times, you may need to cite other people's ideas or actually want to use a quote verbatim. In these cases, the following guidance is provided:

At a minimum, please ensure the following when citing other people's ideas:

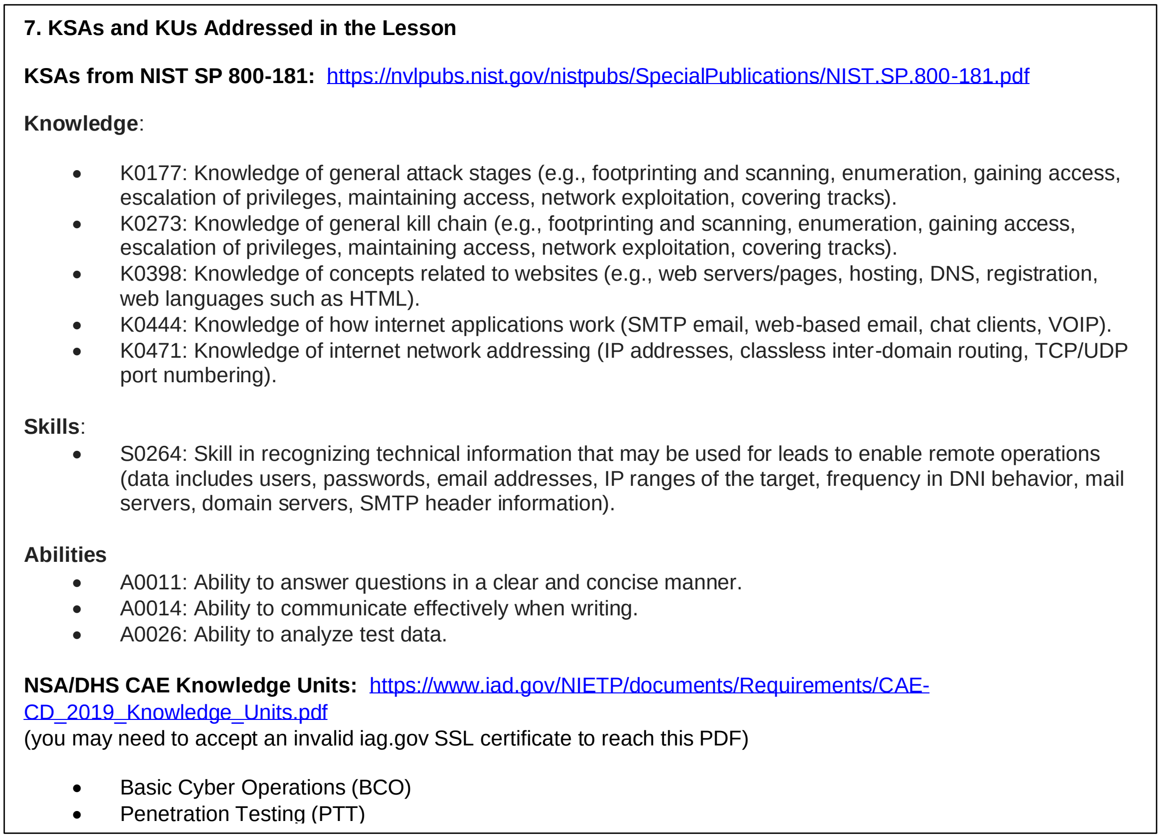
- **Web**
  - Add words to the effect of “Source: URL” on the slide.
  - *The URL should take the reader to the actual webpage where the words/ideas are located NOT to the main homepage*.
  - Font should be 10pt or less.
- **Books/periodicals**
  - You can never go wrong using the MLA format. Take a look here at a few examples of frequently used MLA formats.
  - Again, font should be 10pt or less.

**NOTE**: In the case of verbatim quotes, don't forget the quote marks ("Quoted text.").

### 3.3.6 Skill Mappings

When you submitted your abstract, you were asked to indicate how your content will map (down to the lesson/lab/exercise level) to NIST NICE Workforce Framework Knowledge, Skills, and Abilities (KSAs) and/or NSA/DHS CAE Knowledge Units (KUs). In *Section 3.3.1 Content File Structure*, you were introduced to the **KSA_KU_Refs** folder. Recall this folder contains the reference documents to assist you with adding the NICE Knowledge, Skills, and Abilities (KSAs) and NSA/DHS Knowledge Units (KUs) to the various content documents. More on those references in a moment.

There are three documents where you will be asked to add the KSAs and KUs: lesson plans, lab exercises, and module descriptions. Look at the image below; this is a good example of what you may see with respect to a listing of KSAs and KUs in any one of these three documents.



**7. KSAs and KUs Addressed in the Lesson**

**KSAs from NIST SP 800-181:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

**Knowledge**:

- K0177: Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- K0273: Knowledge of general kill chain (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- K0398: Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).
- K0444: Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).
- K0471: Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).

**Skills**:

- S0264: Skill in recognizing technical information that may be used for leads to enable remote operations (data includes users, passwords, email addresses, IP ranges of the target, frequency in DNI behavior, mail servers, domain servers, SMTP header information).

**Abilities**

- A0011: Ability to answer questions in a clear and concise manner.
- A0014: Ability to communicate effectively when writing.
- A0026: Ability to analyze test data.

**NSA/DHS CAE Knowledge Units:** https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf
(you may need to accept an invalid iag.gov SSL certificate to reach this PDF)

- Basic Cyber Operations (BCO)
- Penetration Testing (PTT)

**Example KSA/KU listing**

From the example KSA/KU listing above, you should note a few things:

1. Links to the definitive references are always provided, since many faculty, especially K12, may not be familiar with KSAs and/or KUs.

> **NOTE**: As an author, you will be provided with electronic copies of these references. We are aware that there are issues with the link to download the KU reference for many. This is an issue with the iad.gov site; we have notified them of this issue.

2. KSAs are always listed in that order, i.e., knowledge first, followed by skills, and then abilities. Within each category, they are then listed in order by their numerical designation and the associated plain language description.
3. KUs are always listed in alphabetical order followed by their three-letter designation in parentheses.

### *DETERMINING WHICH KSAS AND KUS APPLY*

So, you know how to add KSA/KUs to and format them in your documents, but how do you determine which ones apply to your content? In a nutshell, the answer is "keyword search." Since you are intimate with your content, the expectation is, by conducting a "keyword search" of the reference documents, you should be able to find *most* of the KSAs and KUs that apply to your various lessons and lab exercises. We acknowledge and understand this is NOT a perfect science or methodology, but presently it is how authors identify and list the applicable KSA/KUs.

KSAs tend to be much easier to determine for most authors since they are very specific and granular in nature. Authors merely conduct a keyword search of the KSA reference to identify the appropriate knowledge, skills and abilities and list them for each lesson and lab exercise.

Identifying the appropriate KUs for content, on the other hand, tends to be difficult for authors at first. Again, a keyword search can be used. Keep in mind, however, KUs are very broad and not as specific as KSAs. For example, if your content is explaining how firewalls work, you might search for the keyword "firewall." This search would yield several hits in the KU reference document: Network Defense (NDF), Industrial Control Systems (ICS), IT Systems Components (ISC), and Basic Networking (BNW). When you look at each one of these KUs, you will see many more topics than just firewalls are covered, and that's okay. Firewalls only need be an element of a KU. After reading through them, you will need to make the judgment call as to which one or ones apply.

> **TIP**: It is VERY rare that no KSAs or KUs apply in lessons, lab exercises or modules. Many times, if an author submits "None" for KSA/KUs, the content will be sent back to the author to relook at the KSA/KU sections. It is in your best interest to do your due diligence in determining which KSA/KUs apply before submitting your content for review.

Once you've identified the KSA/KUs for your lessons and exercises, it's pretty straightforward to list the KSAs and KUs at the module level. Any and all KSA/KUs from the lessons and lab exercises should be listed in the associated module description. We never expect to see KSAs and/or KUs listed at the module level that are not found in any lesson or lab contained within.

### *WHAT ABOUT INCLUDING NIST NICE FRAMEWORK TASKS?*

When you look at Appendix A (p. 24) of the reference for the KSAs (NIST SP 800-181), you will see it also lists tasks. Several authors provide a listing of tasks as well as the KSAs; however, these are not required. If you feel compelled to include them, they will be left untouched and posted in the final approved content.

## 3.3.7 Prohibited Content

### *FILES OF COPYRIGHTED PRINTED MATERIALS*

Many times, authors want to provide students with copies of reading materials for a lesson, e.g., book chapters, sections, pages, research papers, websites, and other required and optional reading assignments related to the lesson. Please note we cannot put PDF copies of whole chapters (or sections) of textbooks (or journal articles that must be paid for) in the courseware repository.

> **TIP**: In the Reading Assignment section in the lesson plan, provide title, author, ISBN, and URL where the text/article may be purchased. For other papers, news articles, etc., rather than download the documents to post, just provide the URL to the resource.

### *SOFTWARE APPLICATIONS/TOOLS*

Some authors may have lab exercises and/or homework assignments that require special software applications or tools. Given the fact that we provide a virtual environment for students to use to complete lab exercises and/or homework assignments, we do not want to host any special applications or tools, especially proprietary ones. In these cases, we prefer you see what's already available in our virtual environment. If it does not meet your needs, then we will work with you to find an optimal solution to accommodate your requirements. Some of your questions regarding specific applications, tools, and/or artifacts to be used with lab exercises and/or project/homework assignments may be answered in *Section 3.4 Writing Lab Exercises*.

### *REFERENCES TO THE "VIRGINIA" CYBER RANGE*

We ask that you not refer to the Virginia Cyber Range in any of your content documents, specifically in the following cases:

- Other than appearing in document footers, please do not refer to the Cyber Range as the *Virginia* Cyber Range (or abbreviate it as VACR). Once approved, your content is posted on both the Virginia Cyber Range and U.S. Cyber Range websites. Referring to it as simply the *Cyber Range* should make sense to any Virginia Cyber Range users and will alleviate any confusion for users on the U.S. Cyber Range site.
- Please do not use any hypertext links that link directly to anywhere within the Virginia Cyber Range website. For example, you may be tempted to provide a link to the Exercise Area on our website in a lab exercise. Again, since your content will be used on both Virginia Cyber Range and U.S. Cyber Range websites, this will cause confusion

since the URL for the Exercise Area on each site will be different. In this case, you should simply tell the students to log into their *Cyber Range* account.

## 3.4 WRITING LAB EXERCISES

If you plan to write lab exercises, we prefer that you write them to use the virtual environment of the Cyber Range's Exercise Area. There are several reasons why we ask this:

1. The audience you are writing these labs for are instructors and students spread throughout the Commonwealth of Virginia (and U.S. Cyber Range users throughout the country) and they use our Exercise Area almost exclusively for completing hands-on cybersecurity lab exercises.
2. Unlike most virtual machine (VM) solutions (e.g., VirtualBox and VMWare), our virtual environment is cloud-based and has its own unique requirements to access the various VMs available to instructors and students. When writing lab exercises, you will need to be able to explain how instructors/students access and use these VMs.
3. Our cloud-hosted Exercise Area actually makes it easier for you to develop lab exercises since:
    a. You can access it from anywhere, e.g., home, office, favorite coffee shop, etc..
    b. You can log in and access the Cyber Range from any device; you just need a web browser and an internet connection.
    c. Many of the VM environments you will likely be writing cybersecurity lab exercises for already exist in it and you will have access to them all, including Kali Linux, Kali Linux with Metasploitable, openSUSE Linux, Windows 7, Windows Server 2016 virtual machine with a Windows 10 user interface, Ubuntu, among others.

Of course, you may opt to write cybersecurity lab exercises that use other VM solutions (e.g., VirtualBox and VMWare) or you may have some exercises that require no VMs at all.

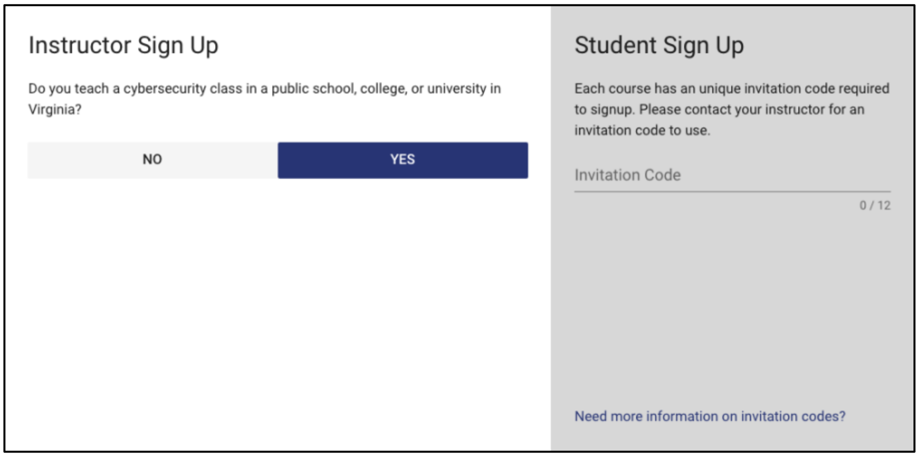
The next two sections that follow, *Section 3.4.1 Getting a Virginia Cyber Range Account & Creating a Course* and *Section 3.4.2 Accessing the Exercise Area and Adding VMs to Your Course*, pertain to lab exercises written specifically for the Cyber Range. If you are not writing lab exercises that use the Cyber Range, you may skip to *Section 3.4.3 Lab Exercise Formatting and Other Considerations*.

> **IMPORTANT**: Regardless, for any lab exercises you write, you will need to use the required lab exercise template discussed earlier in *Section 3.2.4 Lab Exercise* and adhere to the guidance found in *Section 3.4.3 Lab Exercise Formatting and Other Considerations*.

## 3.4.1 Getting a Virginia Cyber Range Account & Creating a Course

BEFORE you begin authoring any lab exercises, your first step will be to sign up on the VACR website to get an account, if you have not done so already. This account will give you access to the Exercise Area, the place you will use VM environments to write your cybersecurity lab exercises, as well as to the Courseware Repository. Once you go through the following steps to get an account, we highly encourage you to peruse the Courseware Repository as well to look at other author's content and get an idea of expectations.

To request a Virginia Cyber Range account, go to the Instructor Sign Up page here. You should see the below image displayed on the webpage.



Instructor Sign Up

Do you teach a cybersecurity class in a public school, college, or university in Virginia?

Student Sign Up

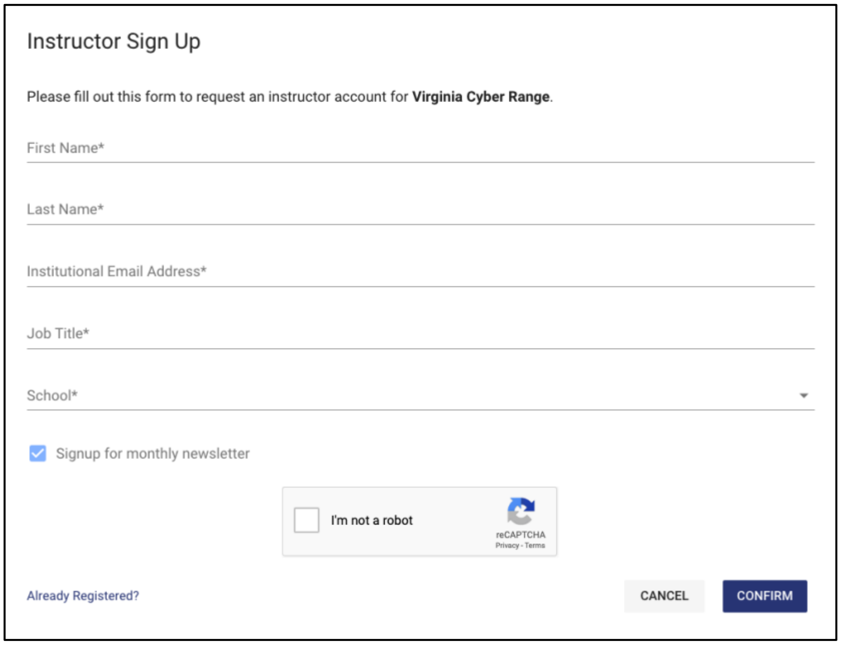
Each course has an unique invitation code required to signup. Please contact your instructor for an invitation code to use.

Invitation Code

0 / 12

Need more information on invitation codes?

Next, click on YES and completely fill out the web form (see image below), ensuring to use your academic institutional email address. Using your institutional email address is important, since it is how you will be vetted to approve your account request. Once you click the **CONFIRM**



Instructor Sign Up

Please fill out this form to request an instructor account for **Virginia Cyber Range**.

First Name*

Last Name*

Institutional Email Address*

Job Title*

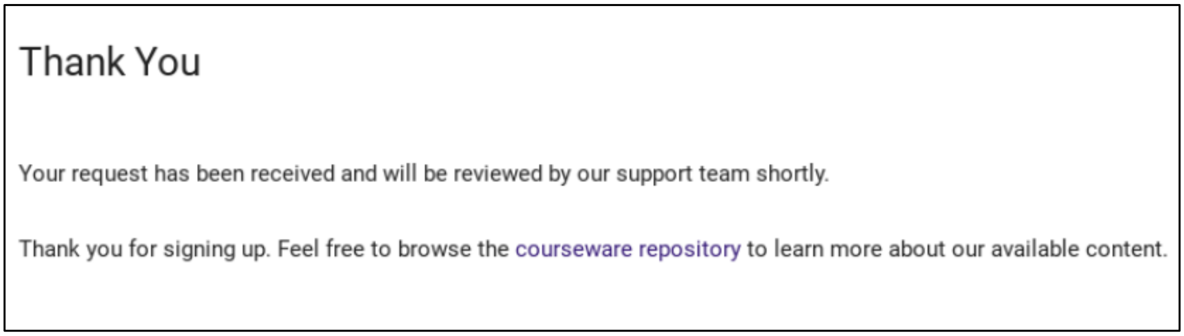
School*

☑ Signup for monthly newsletter

□ I'm not a robot

button, you will see a thank you message as seen in the image below.

> **TIP**: If for any reason your request is denied, contact your content coordinator and let them know. They will ensure your account gets approved.

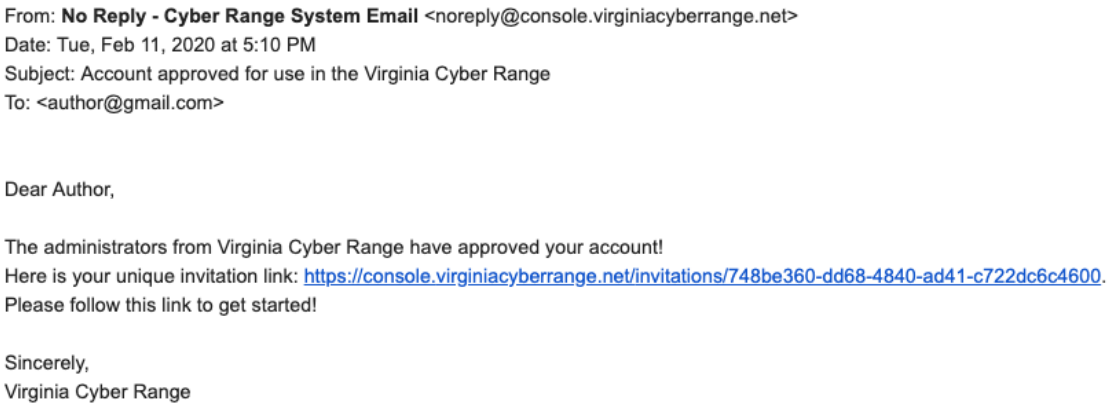


Thank You

Your request has been received and will be reviewed by our support team shortly.

Thank you for signing up. Feel free to browse the courseware repository to learn more about our available content.

Once your account request is vetted and approved, you will receive an email with the subject **Account approved for use in the Virginia Cyber Range** and containing a unique login URL; you will click on this URL to log in to the range. It should look something like the image below.



From: **No Reply - Cyber Range System Email** <noreply@console.virginiacyberrange.net>
Date: Tue, Feb 11, 2020 at 5:10 PM
Subject: Account approved for use in the Virginia Cyber Range
To: <author@gmail.com>

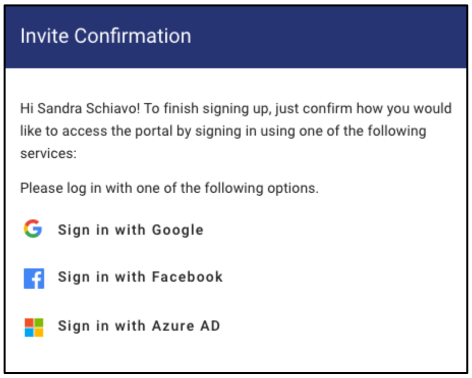
Dear Author,

The administrators from Virginia Cyber Range have approved your account!
Here is your unique invitation link: https://console.virginiacyberrange.net/invitations/748be360-dd68-4840-ad41-c722dc6c4600.
Please follow this link to get started!

Sincerely,
Virginia Cyber Range

> **TIP**: To decrease token conflicts, it's better to open the invite link as an anonymous incognito or private browsing tab session until you get successfully logged in.

After clicking on your invitation link, log in to the Virginia Cyber Range with your preferred third-party authentication provider (e.g. Google, Facebook, Azure AD).

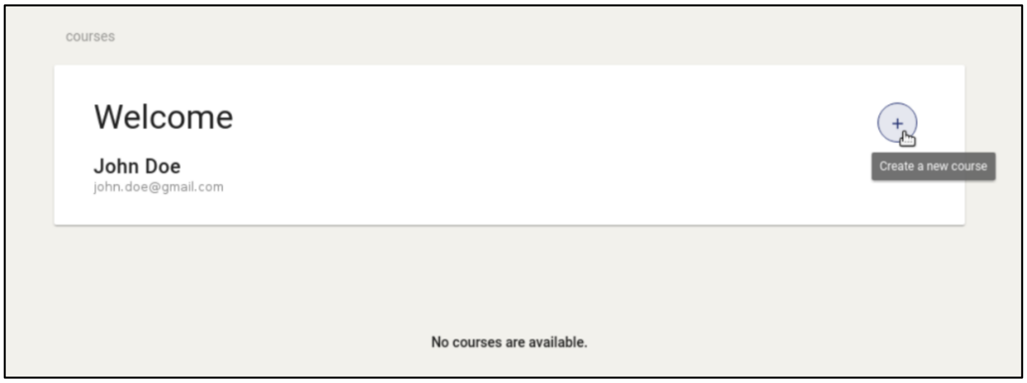


Invite Confirmation

Hi Sandra Schiavo! To finish signing up, just confirm how you would like to access the portal by signing in using one of the following services:

Please log in with one of the following options.

Upon selecting your third-party authentication provider, you may be directed to their site for login. Once successfully logged in, you will be re-directed back to the Virginia Cyber Range. Once you get logged into the Cyber Range for the first time, you will get an empty course listing. See the image below.



Welcome

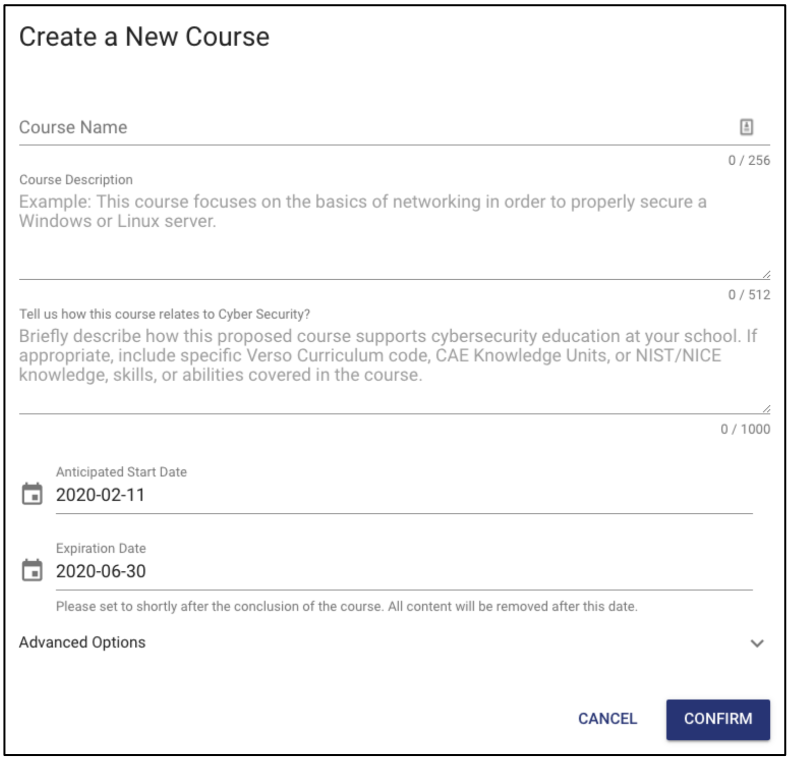
John Doe
john.doe@gmail.com

No courses are available.

At this point, you have two options:

1. You can click on the **COURSEWARE** menu button at the top and go out to look at the Courseware Repository, or
2. You can create a new course. As an author writing labs to work with the Cyber Range, this is exactly what you want to do; we explain how to below.

Click on the circular "+" icon to request and "create a new course." The form seen below should be displayed. Since you are not really requesting a new course be created to teach, but rather



Create a New Course

Course Name
0 / 256

Course Description
Example: This course focuses on the basics of networking in order to properly secure a Windows or Linux server.
0 / 512

Tell us how this course relates to Cyber Security?
Briefly describe how this proposed course supports cybersecurity education at your school. If appropriate, include specific Verso Curriculum code, CAE Knowledge Units, or NIST/NICE knowledge, skills, or abilities covered in the course.
0 / 1000

Anticipated Start Date
2020-02-11

Expiration Date
2020-06-30
Please set to shortly after the conclusion of the course. All content will be removed after this date.

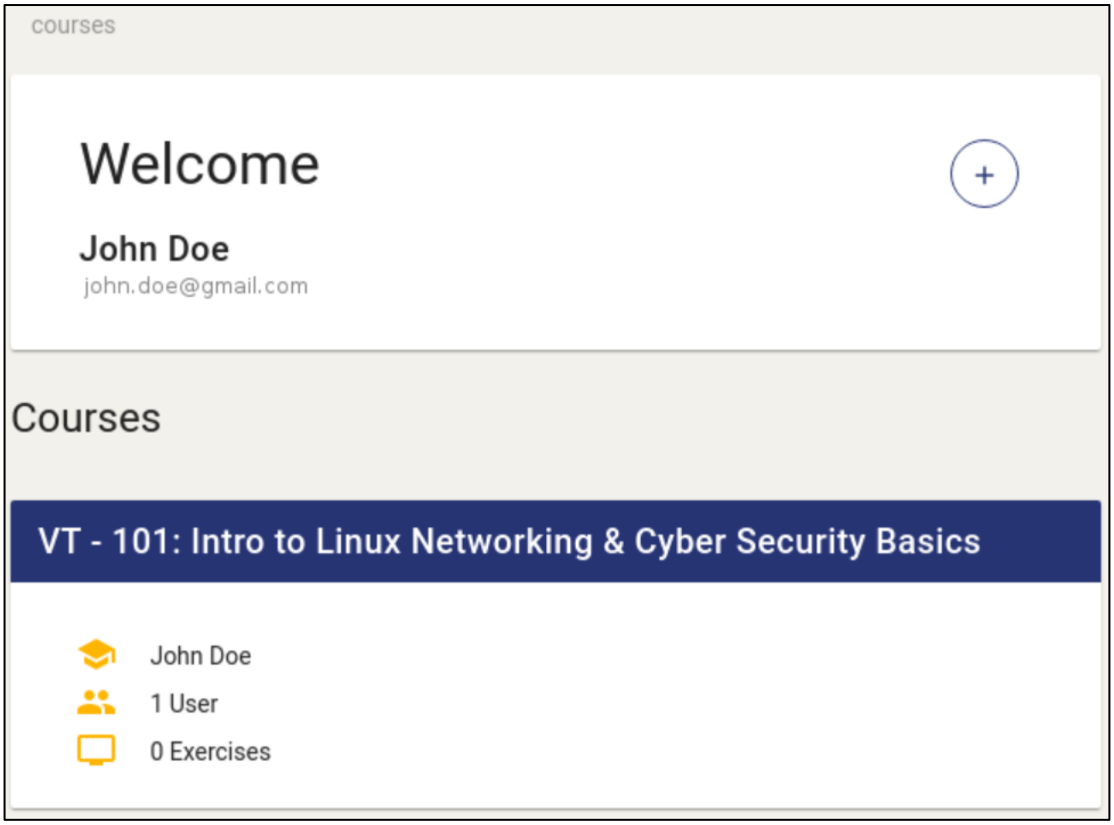
will be writing content to use the Cyber Range's Exercise Area, you will need to fill out this form as follows:

- Course Name. For this field, type in the following: **Title of YOUR content**.
- Course Description. For this field, type the following:

  **My name is [First name Last name]. I have a signed Author Agreement to write content for the VACR. I require access to the VACR Exercise Area to write lab exercises using the following kinds of VMs: [list the VMs needed, e.g., Kali Linux].**

- How course relates to Cyber Security: **Free form; fill out as desired**.
- Dates: **Pick an end date *at least a year out***.
- Advanced Options. Ignore.

Click on the **CONFIRM** button. After you create your "new course" request within the Cyber Range, you will see your course placeholder as shown below.



Welcome

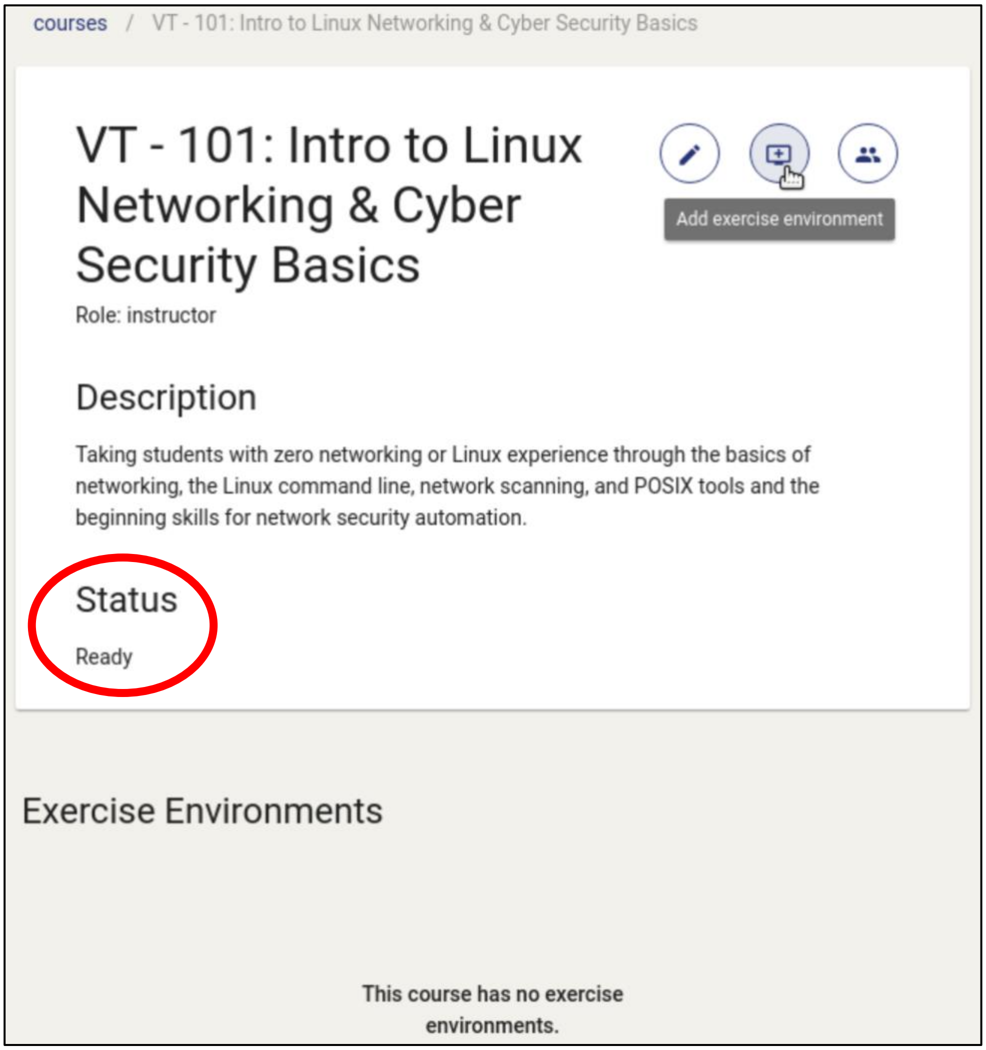
John Doe
john.doe@gmail.com

Courses

VT - 101: Intro to Linux Networking & Cyber Security Basics

John Doe
1 User
0 Exercises

If you click into the "new course" you just requested and created, you will see that its current status is "Pending." Once a course admin approves your request, it will change from "Pending" status to "Ready." See the image on the next page.


courses / VT - 101: Intro to Linux Networking & Cyber Security Basics

VT - 101: Intro to Linux Networking & Cyber Security Basics

Role: instructor

Description

Taking students with zero networking or Linux experience through the basics of networking, the Linux command line, network scanning, and POSIX tools and the beginning skills for network security automation.

Status

Ready

Exercise Environments

This course has no exercise environments.

## 3.4.2 Accessing the Exercise Area and Adding VMs to Your Course

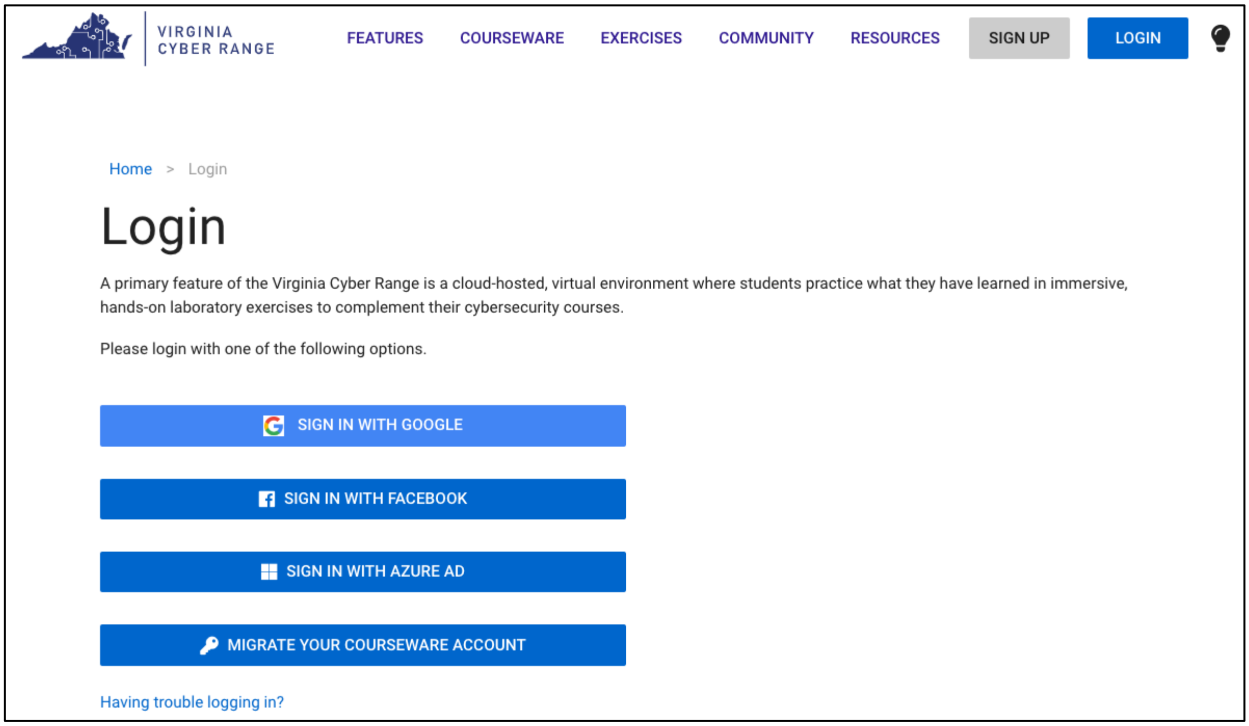
This section assumes you already have a Virginia Cyber Range account and an approved course in the Exercise Area. If not, read the previous section.

In this section, we focus on how to add virtual machine (VM) environments to your "course." As stated before, there are several VM environments available to you and they are very easy to add to your newly created course.

> **IMPORTANT**: Given VM storage requirements and associated costs, as good stewards of taxpayer dollars, we limit you to only three VMs or less at any given time. We ask that you only add the VMs needed to write your lab exercises.

### *ACCESSING THE EXERCISE AREA*

You must be logged in to the Virginia Cyber Range website to access the Exercise Area. You can log in from anywhere in the site by clicking on the LOGIN button in the upper right corner. When you do, you should see the following login page:



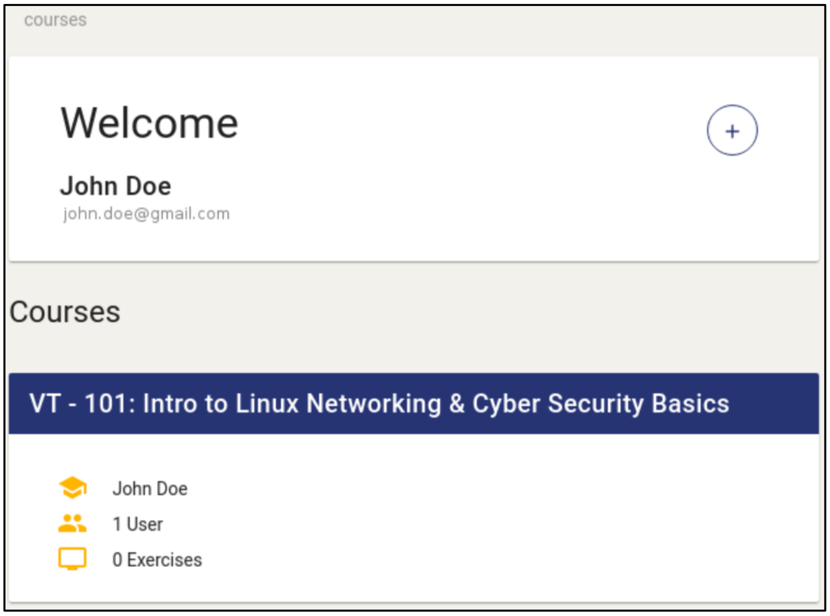
Login

A primary feature of the Virginia Cyber Range is a cloud-hosted, virtual environment where students practice what they have learned in immersive, hands-on laboratory exercises to complement their cybersecurity courses.

Please login with one of the following options.

Click on the openID authentication service you used when you signed up for your Virginia Cyber Range account. When you do, a window will pop up for you to enter your credentials (username, password). Once you are authenticated, then you will be redirected to the Virginia Cyber Range website. You should notice that in the upper righthand corner you no longer see the **SIGN UP** or **LOGIN** buttons. This means you are now logged in to our site.

In order to access the Exercise Area, click on the **EXERCISES** menu/button located at the top of the website in the middle. Once you do, your course should be displayed. See image below.



Welcome

John Doe
john.doe@gmail.com

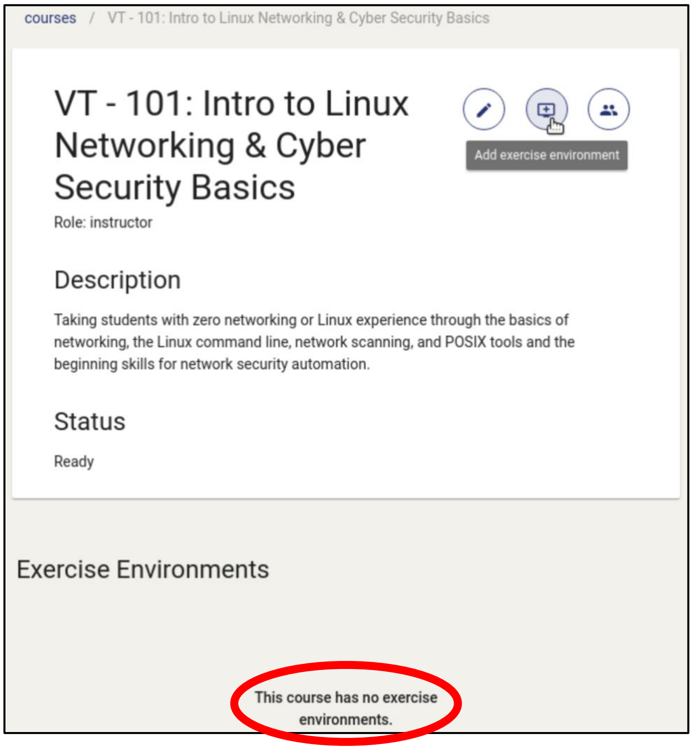
Courses

VT - 101: Intro to Linux Networking & Cyber Security Basics

John Doe
1 User
0 Exercises

## *ADDING VMS TO YOUR COURSE*

At this point, click on your course. You should notice at the bottom of your course it says, "This course has no exercise environments." See the image below.



courses / VT - 101: Intro to Linux Networking & Cyber Security Basics

VT - 101: Intro to Linux Networking & Cyber Security Basics

Role: instructor

Description

Taking students with zero networking or Linux experience through the basics of networking, the Linux command line, network scanning, and POSIX tools and the beginning skills for network security automation.

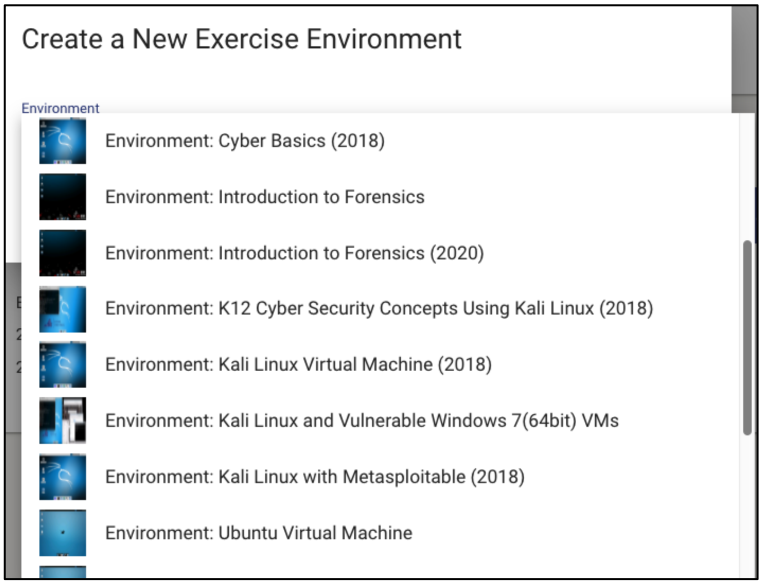
Status

Ready

Exercise Environments

This course has no exercise environments.

Let's add an exercise environment. You should see a button that looks like a computer with a "+" sign in it at the top righthand side. When you hover over it with your mouse it says, "Add exercise environment." Click on it and you will see a listing of all available environments; see image below. Let's add the Kali Linux with Metasploitable (2018) environment to our course, since we plan to write a lab exercise using Metasploitable.

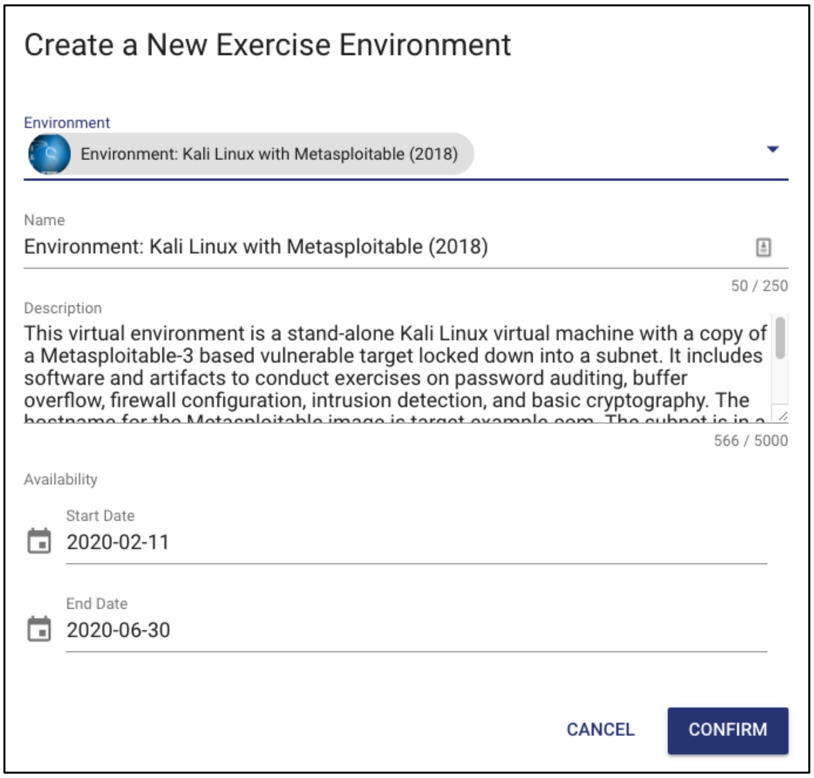


Create a New Exercise Environment

Environment

- Environment: Cyber Basics (2018)
- Environment: Introduction to Forensics
- Environment: Introduction to Forensics (2020)
- Environment: K12 Cyber Security Concepts Using Kali Linux (2018)
- Environment: Kali Linux Virtual Machine (2018)
- Environment: Kali Linux and Vulnerable Windows 7(64bit) VMs
- Environment: Kali Linux with Metasploitable (2018)
- Environment: Ubuntu Virtual Machine

When you select this environment, a window pops up to create a new exercise environment. See the image below. Several of the fields are editable, but as an author the only field you really need to consider changing is the end date. We recommend choosing an end date at least one year out.



Create a New Exercise Environment

Environment: Environment: Kali Linux with Metasploitable (2018)

Name: Environment: Kali Linux with Metasploitable (2018)

50 / 250

Description: This virtual environment is a stand-alone Kali Linux virtual machine with a copy of a Metasploitable-3 based vulnerable target locked down into a subnet. It includes software and artifacts to conduct exercises on password auditing, buffer overflow, firewall configuration, intrusion detection, and basic cryptography. The hostname for the Metasploitable image is target.example.com. The subnet is in a

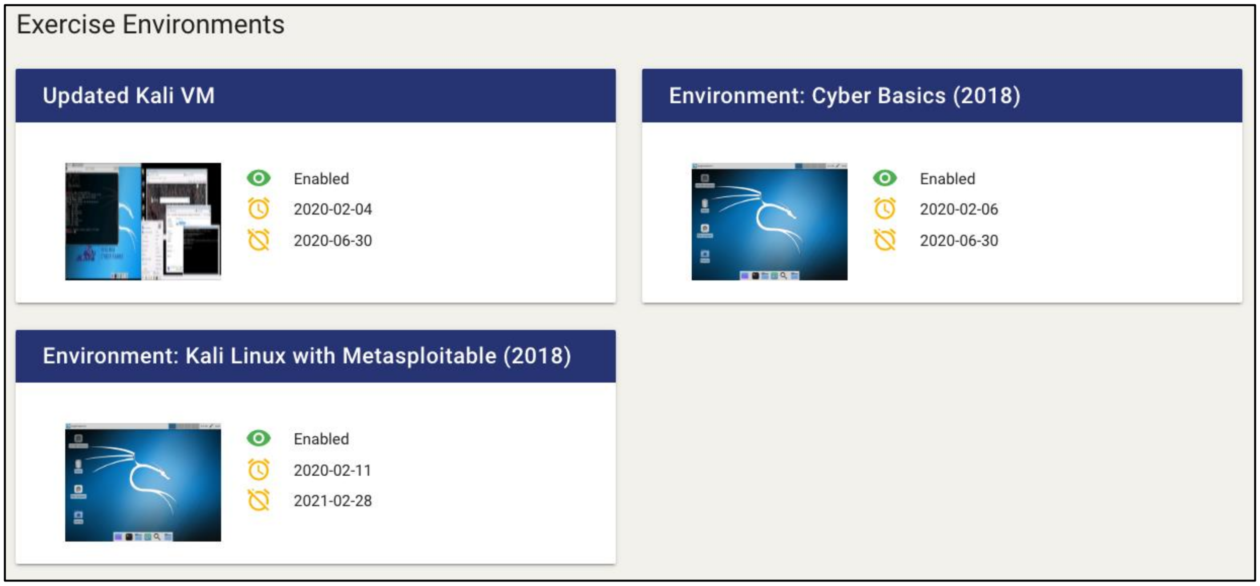
566 / 5000

Availability

Start Date: 2020-02-11

End Date: 2020-06-30

When you click on the **CONFIRM** button, this exercise then gets added to your course. Looking at the image below, you can see the Kali Linux with Metasploitable (2018) environment is in our course along with two other exercise environments.



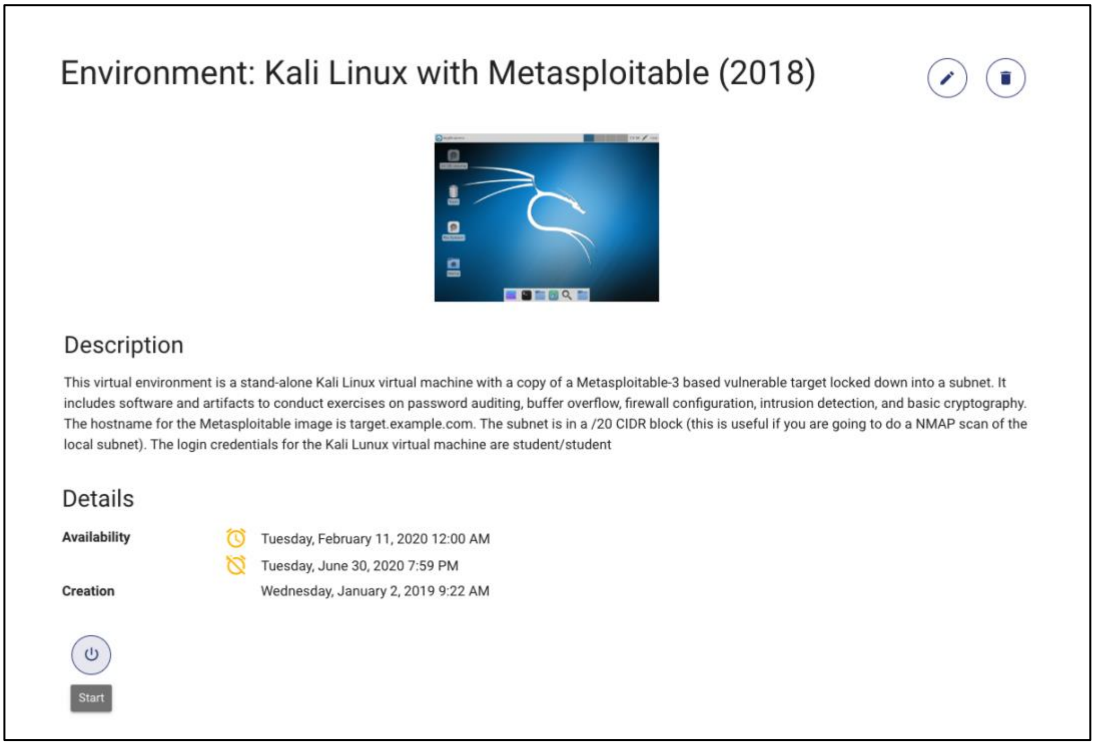
Exercise Environments

Updated Kali VM
Enabled
2020-02-04
2020-06-30

Environment: Cyber Basics (2018)
Enabled
2020-02-06
2020-06-30

Environment: Kali Linux with Metasploitable (2018)
Enabled
2020-02-11
2021-02-28

To use any one of the exercise environments you have added to your course, you only need to click on it. When you do, you will see the environment exercise window open which includes an environment description and the details, i.e., availability and creation dates. See image below.



Environment: Kali Linux with Metasploitable (2018)

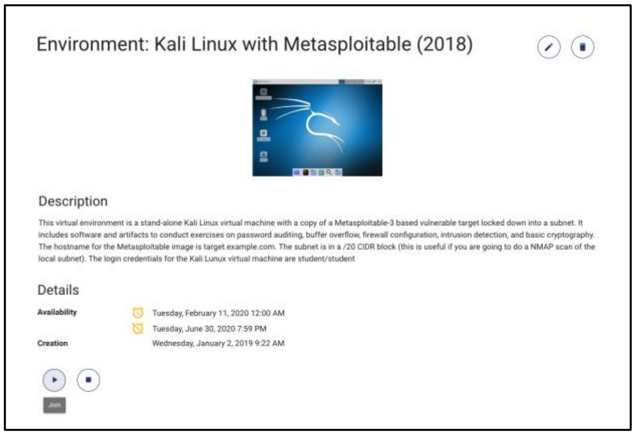
Description

This virtual environment is a stand-alone Kali Linux virtual machine with a copy of a Metasploitable-3 based vulnerable target locked down into a subnet. It includes software and artifacts to conduct exercises on password auditing, buffer overflow, firewall configuration, intrusion detection, and basic cryptography. The hostname for the Metasploitable image is target.example.com. The subnet is in a /20 CIDR block (this is useful if you are going to do a NMAP scan of the local subnet). The login credentials for the Kali Lunux virtual machine are student/student

Details

| | |
|---|---|
| **Availability** | Tuesday, February 11, 2020 12:00 AM<br>Tuesday, June 30, 2020 7:59 PM |
| **Creation** | Wednesday, January 2, 2019 9:22 AM |

Like any computer, VMs need to be turned on. Click the **Start** button located on the lower left-hand side. It may take several minutes for the VM to start, so be patient. Once the VM has been started, you will then see a **Join** button. See image below on left. Click on this button to access ("join") the VM and log into it. This particular VM requires login credentials; however, not all VMs do.



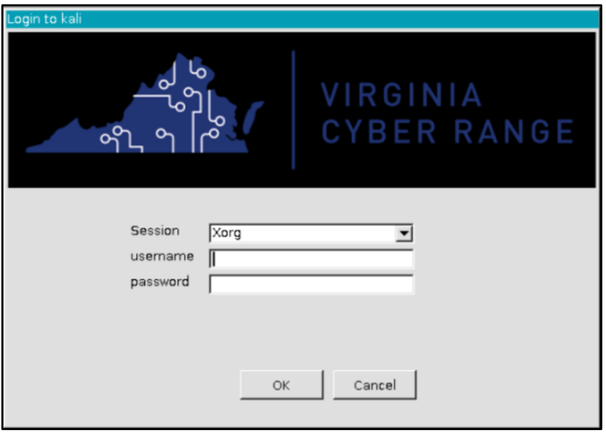
Environment: Kali Linux with Metasploitable (2018)

Description

This virtual environment is a stand-alone Kali Linux virtual machine with a copy of a Metasploitable-3 based vulnerable target locked down into a subnet. It includes software and artifacts to conduct exercises on password auditing, buffer overflow, firewall configuration, intrusion detection, and basic cryptography. The hostname for the Metasploitable image is target.example.com. The subnet is in a /20 CIDR block (this is useful if you are going to do a NMAP scan of the local subnet). The login credentials for the Kali Lunux virtual machine are student/student

Details

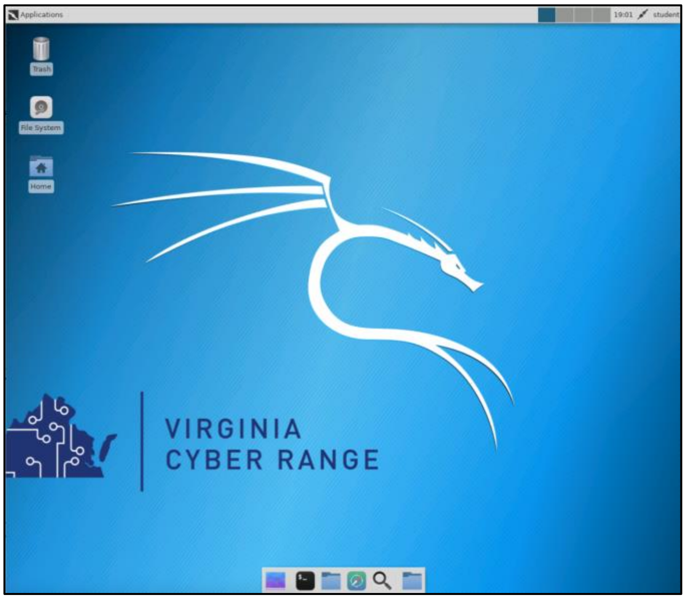
Availability Tuesday, February 11, 2020 12:00 AM
Tuesday, June 30, 2020 7:59 PM
Creation Wednesday, January 2, 2019 9:22 AM



Login to kali

Session Xorg
username
password

After clicking the **Join** button, we log in to the Kali VM using the credentials (student/student) as described in the description. See image above on right. Once we hit **OK**, then we are on the desktop of the Kali VM. See the image at the top of the next page.



At this point, you can begin to use the VM to test out and write your lab exercises.

## *OTHER THINGS TO KNOW ABOUT USING OUR VMS*

Network Restrictions and VM Limitations. Like any computer network or computer on the network, there are always restrictions and limitations. VM environments in the Cyber Range are no exception. We will list a few of the most important ones here, but for more details please refer to our online Knowledge Base (KB). You will likely find what you are looking for in the FAQ and Troubleshooting sections; however, we encourage you to peruse and become familiar with the entire KB, as it will help you in writing labs for our environment.

> **NOTE**: Please keep in mind that the KB is written for the end user and not an author.

The following list is a few of the important Cyber Range virtual environment restrictions and limitations to know while writing labs:

- **Most VMs on the Cyber Range are restricted to 1-2 vCPU and 1-4GB of RAM**. If you need a more powerful VM for your lab(s), please let your content coordinator know. We will evaluate your situation and let you know if we can accommodate your requirement.

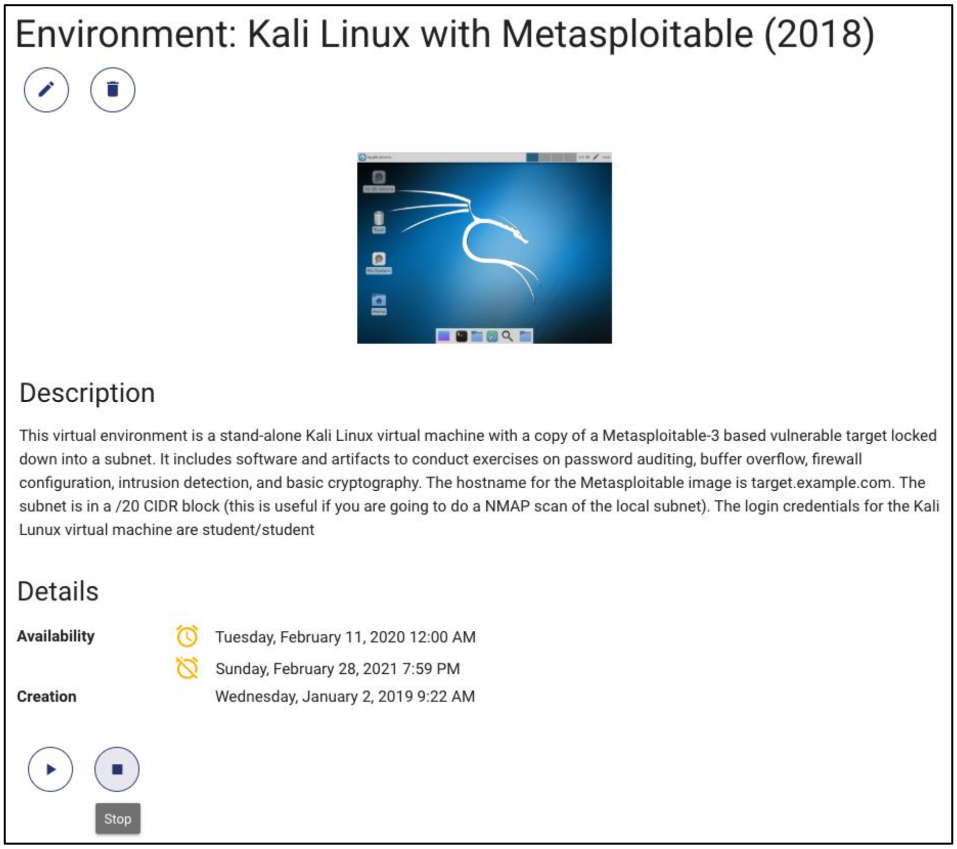
  > **NOTE**: VMs in the Cyber Range use time-shared CPUs; this means continual processor-intensive operations may not perform well in the lab setting. When designing brute force lab exercises, use enough data to prove the point, but do not require running scripts for 5+ minutes, especially sequentially.

- **The Cyber Range provides a monitored and filtered web proxy for basic non-malicious internet usage** such as system patching, lab setup, and/or browsing websites. No other traffic on any protocol is permitted to leave the Cyber Range; this means tools like nmap, ping, ssh, and functions like DNS queries or SMTP traffic can fail.

- **Additional VMs can be added to an environment and set up to facilitate the needs of lab exercises for things like vulnerable attack targets, port-scanners, etc.**. This is the only approved way to attack or reach other systems on the restricted network of the Range. Attacking ANY of the Range's cloud infrastructure, name servers, Layer2/layer3 networks, ARP/DNS spoofing, proxies, etc. is strictly prohibited.
- **We have implemented child safety filters** to prevent access to inappropriate websites such as gambling, pornography, social media, and streaming video web sites in order to ensure schools can maintain compliance with the Children's Internet Protection Act (CIPA).
- **CAPS Lock Bug**. One potential bug while using our environments is that while using caps lock, the lock will get stuck on or off. For a workaround, check here.

Resetting and Making Copies of your VM(s). While you are getting used to the VM environments in the Cyber Range and using them to write your lab(s), you might have made numerous changes to a VM environment and, for whatever reason(s), may want to reset it back to its initial condition. Prior to resetting the VM, you may also want to make a copy of the VM in its current state so as to preserve any changes you have made. You actually have the capability to do both: reset and copy a VM environment in the Cyber Range.

*In order to reset or copy an environment, the VM must be stopped first*. The **Stop** button is located to the right of the **Join** button as shown in the image below. Once the VM is stopped,



Environment: Kali Linux with Metasploitable (2018)

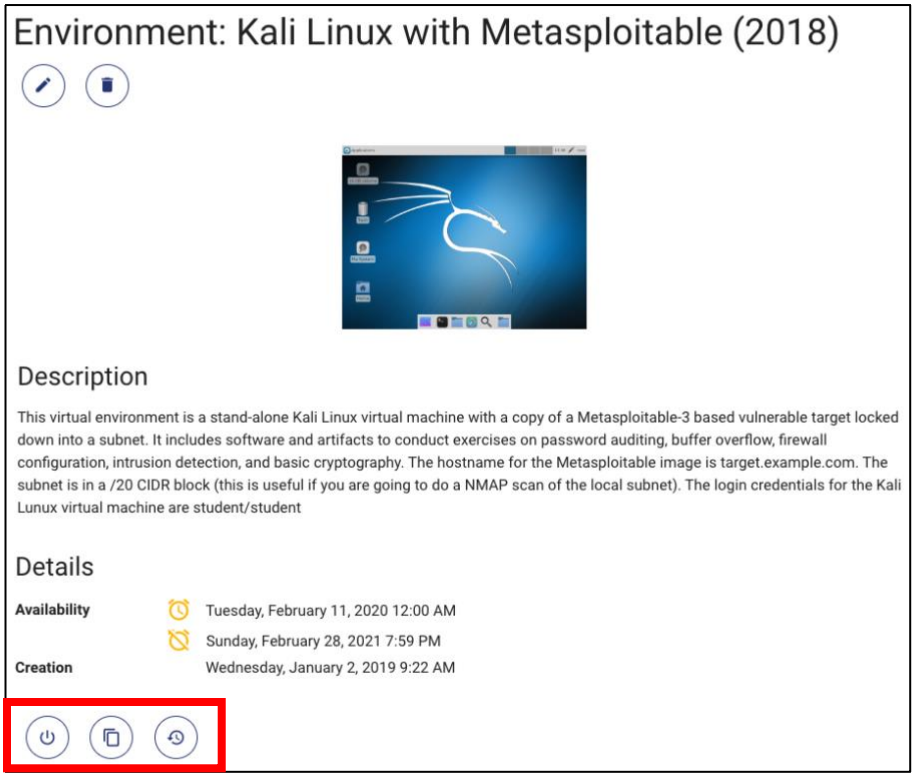
Description

This virtual environment is a stand-alone Kali Linux virtual machine with a copy of a Metasploitable-3 based vulnerable target locked down into a subnet. It includes software and artifacts to conduct exercises on password auditing, buffer overflow, firewall configuration, intrusion detection, and basic cryptography. The hostname for the Metasploitable image is target.example.com. The subnet is in a /20 CIDR block (this is useful if you are going to do a NMAP scan of the local subnet). The login credentials for the Kali Lunux virtual machine are student/student

Details

| | |
|---|---|
| Availability | Tuesday, February 11, 2020 12:00 AM<br>Sunday, February 28, 2021 7:59 PM |
| Creation | Wednesday, January 2, 2019 9:22 AM |

you should notice that there are three buttons on the bottom left-hand corner available to you to use with the VM: **Start**, **Copy**, and **Reset**. See the red box in the image on the following page.



Environment: Kali Linux with Metasploitable (2018)

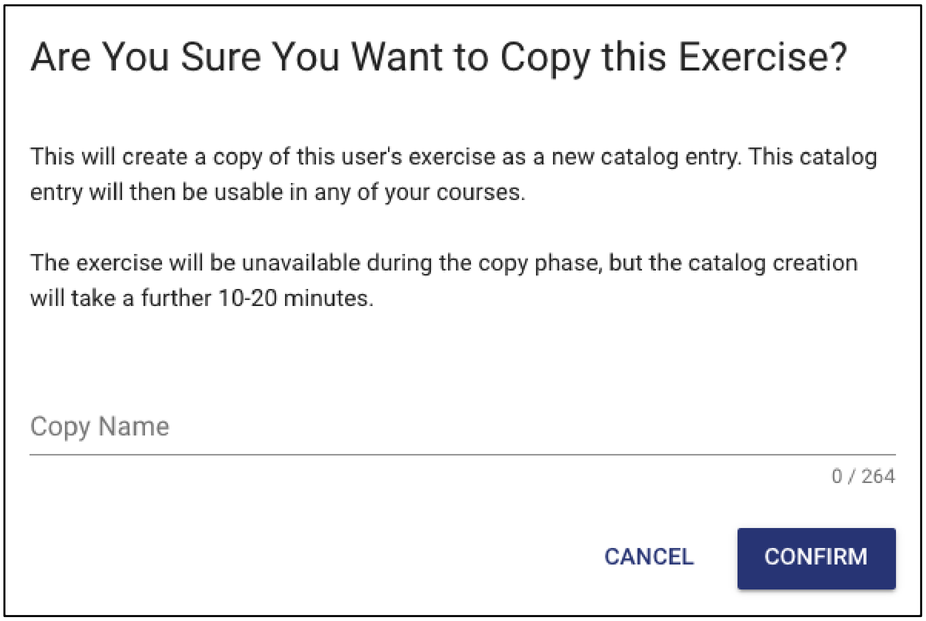
Description

This virtual environment is a stand-alone Kali Linux virtual machine with a copy of a Metasploitable-3 based vulnerable target locked down into a subnet. It includes software and artifacts to conduct exercises on password auditing, buffer overflow, firewall configuration, intrusion detection, and basic cryptography. The hostname for the Metasploitable image is target.example.com. The subnet is in a /20 CIDR block (this is useful if you are going to do a NMAP scan of the local subnet). The login credentials for the Kali Lunux virtual machine are student/student

Details

| | |
|---|---|
| Availability | Tuesday, February 11, 2020 12:00 AM |
| | Sunday, February 28, 2021 7:59 PM |
| Creation | Wednesday, January 2, 2019 9:22 AM |

As discussed in the previous section, the **Start** button (on the far left) will allow you to **Join** and get you access to the desktop of this VM environment. If you want to make a copy of this VM, click on the **Copy** button (in the middle) to do so. When you do, the below window pops up.



Are You Sure You Want to Copy this Exercise?

This will create a copy of this user's exercise as a new catalog entry. This catalog entry will then be usable in any of your courses.

The exercise will be unavailable during the copy phase, but the catalog creation will take a further 10-20 minutes.

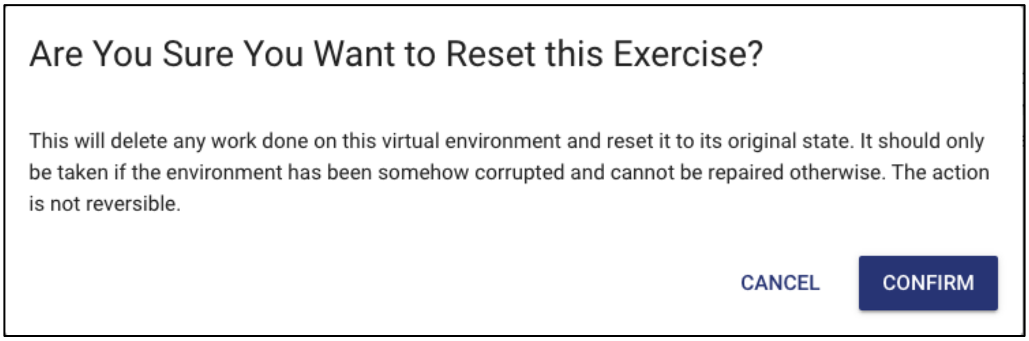
Copy Name

0 / 264

After typing in a name for this copy of the VM environment, click on the **CONFIRM** button. At this point, your copy will get created and then you will be able to access it in *your* listing of available environments. Now you can add this copy to your course.

If you want to reset this VM, click on the **Reset** button (on the far right) to do so. When you do, the below window and warning pops up.

> **IMPORTANT**: Any work you have done in this virtual environment will be lost and the VM will be reset back to its original state; *this is why it may be a good idea to make a copy before resetting the VM environment*.



Are You Sure You Want to Reset this Exercise?

This will delete any work done on this virtual environment and reset it to its original state. It should only be taken if the environment has been somehow corrupted and cannot be repaired otherwise. The action is not reversible.

Please note that resetting an environment can take several minutes, as long as 10-20 minutes.

### 3.4.3 Lab Exercise Formatting and Other Considerations

This section assumes you already have a Virginia Cyber Range account, an approved course in the Exercise Area, and you have added the necessary environments to it in order to write your lab exercise(s). If not, read the previous section.

In this section, we focus on actually writing and formatting your lab exercise handouts. We also discuss special considerations that will help faculty and students to better use your labs.

#### *LAB EXERCISE TEMPLATE*

As discussed in *Section 3.1 Templates*, there is a template for almost all content you will submit as an author for the Cyber Range. So, your first step in writing a lab exercise would be to open and carefully read through the contents of the provided lab exercise template. This lab exercise template is laid out as explained in *Section 3.1.1 Getting familiar with Word templates*, i.e., it contains a header, a student section, faculty instruction section, and a footer. Now, we will go more in-depth into the student and faculty instruction sections, since the header and footer have been explained previously and should be self-explanatory.

Student Section. The student section of the lab exercise includes the following sections:

1. Overview
2. Resources required
3. Initial Setup

4. Tasks
5. References

We will look at each of the above sections in turn.

1. **Overview**. This section should be a description of the lab exercise and what the student will learn in completing the exercise. Typically, the overview will start with language for example: "In this lab, the student will…" or After completing this lab, the student will…" Keep in mind this language will be the first thing viewed by faculty who may desire to use your content. There must be enough information to convey what the objective of the lab is and what the students will learn. Here is an example of what an overview for a lab might look like:

   > In this lab, the student will use a common steganography tool to embed secret messages and data within sample graphic images and extract them on the receiver side. By the end of this lab, the student should be able to discuss some of the security risks and detection methods associated with steganography.

   In the overview, you may also include background information about the subject for the students and/or talk about the VM environment(s) and tools the students will use in the lab. Continuing with the steganography example from above, here's what some additional information in the overview might look like:

   > Steganography is the art of secret communications by hiding data within other files. The data is secure as long as it is not discovered. The use of steganography dates back to Ancient Greece where secret communications were carved into the wooden surface of a writing tablet and then recovered with wax leaving the tablet to appear blank. When the wax was melted away, the secret message was revealed.
   >
   > While Steganography is often used commercially to hide copyright information and digital watermarks in graphic, music or video files, hackers and spies also use it to hide secret data or communications through insecure channels, in plain sight.

   Of course, you do not want to get too wordy in the overview. Again, it should provide enough information so faculty and the student understand what the student will learn after completing the lab.

2. **Resources required**. This section should describe virtual machines, software documentation, and any other resources required to complete the lab exercise. Recall, these lab exercises do not have to use the Cyber Range; however, if they do, here is where you want the faculty and students to understand what the minimum requirements will be to successfully complete the lab. In the case of a lab written for the Cyber Range, an example of resources required may simply be:

   > This exercise requires a Kali Linux VM running in the Cyber Range.

This simple requirements statement may also be useful for faculty who desire to use another VM solution besides the Cyber Range; they can adapt the lab exercise to work with their alternate Kali Linux VM solution in this case.

> **TIP**: If you are writing labs for use in the Cyber Range, please ensure the below note to instructors is included in this section. It should be bracketed and in the blue font as shown.
>
> [Note to instructors: This lab exercise requires an account on the Cyber Range. To sign up for an account on The Range, please visit our Sign-Up page. Your students will also require an account on the Cyber Range; this will be explained in the setup of your course.]

3. Initial Setup. In this section, you will want to provide any steps required for the student to set up or gain access to the environment in which they will complete the lab exercise. This might include logging in to the Cyber Range, selecting a specific environment, and/or downloading and configuring software on a VM. This section should also include credentials for VMs (if needed) used in the execution of the exercise. Here is another example of what you might see in this section:

> For this exercise, you will log in to your Cyber Range account and select the Kali Linux with Metasploitable (2018) environment, then click "start" to start your environment and "join" to get to your Linux desktop login. Log in using these credentials:
>
> Username: **`student`**<br>
> Password: **`student`**

4. Tasks. This section is the heart of the lab. It contains the tasks you want the students to accomplish in the lab exercise. Each of the major tasks should be described sufficiently so that the student (or team) can complete it. Tasks should be listed numerically, starting with task 1, task 2, task 3, …, and ending with task N. Given how important this topic is, many more details are provided in the next section: *Writing Lab Tasks*.

5. References. In this section, you will list any references that were used in the creation of this lab exercise. You may also include references for students to learn more about the specific lab topic. In some cases, this may actually be N/A or None. Here is an example of what you may see here:

    - For more info on various steganography tools on Linux, including the popular "steghide," see: https://0xrick.github.io/lists/stego/
    - And more information on the general topic see: https://en.wikipedia.org/wiki/Steganography

Faculty Instruction Section. The faculty instruction section of the lab exercise includes the following sections:

1. Just below the line
2. KSA/KUs Listing

We will look at each of the above sections in turn.

1. Just below the line. After the end of the student section, i.e., the listing of references, you should see the following visible line that separates what the students are expected to see in the lab exercise handout from what the instructors are allowed to see:

   "

   [This portion of the lab is provided for instructors that will be using this lab and associated material in their class.]"

   Just below this line is where you would provide detailed instructions for faculty that will use this lab exercise, including any special requirements to access virtual machines, other required resources, or how virtual systems should be networked. Imagine if you were the faculty member about to use this lab with their students. What would you want to know before using it? This is the place to put such comments.

   In the section, you also might recommend this lab exercise as a team or an individual assignment. Additionally, this is your opportunity to share any thoughts on where you think students might run into trouble when completing the lab.

   Finally, while you may provide answers to lab questions in this section, we prefer you use the template to develop an answer key and provide it in the specific lesson folder along with the associated lab exercise file naming it appropriately, e.g. "Lab1Exercise_AnswerKey.docx."

2. KSA/KUs Listing. As you might expect, this is where you will add the KSA/KU lists associated with the lab exercise.

Finally, we'd like to leave you with a comment and tip regarding the lab exercise template. While it is not formatted as such or required, we highly recommend you include page numbers in your lab exercises. We have seen many lab exercise handouts exceed 20 pages, especially when including screen shots.

> **TIP**: By numbering the pages in your lab exercise handouts, you will assist faculty and students who are using printed copies to complete the lab exercise. It also allows faculty and students to refer to a specific location in the lab handout.

### *WRITING LAB TASKS*

As discussed above, step 4 (Tasks) in the student section of the lab template is the most important part of the lab.  It contains the tasks you want the students to accomplish in the lab exercise, and it must be written logically and in enough detail so the student understands what they need to do and can complete it successfully. In this section, we will discuss several things that can help you to logically organize and format your lab exercises, along with recommendations that will help faculty and students to better use your labs. Specifically, we will look at the use of:

- Task numbering
- Multilevel numbered lists
- White space and indention
- Commands/snippets of code
- Notes to instructors
- Screen shots
- Artifacts

Use of Task Numbering. Tasks numbering is required within section 4 (Tasks) of the lab exercise template. To reiterate, tasks should be listed numerically, starting with task 1, task 2, task 3, …, and ending with task N. For example, the following high-level tasks are from a lab exercise called "Evading Detection Systems:"

- **Task 1: Fragmenting packets**
- **Task 2: Changing the mtu size**
- **Task 3: Setting the Metasploit SQL database to run on startup**
- **Task 4: Bypassing detection systems using the msfconsole**
- **Task 5: Bypassing Firewalls with Nmap Scripts**
- **Task 6: Service Version UDP Scanning**

Once you determine what the major tasks of your lab are, then you are free to provide any supplemental information and write the subtasks involved for the students to accomplish under each of these major task headings.

Use of Multilevel Numbered Lists. Another approach some authors may choose is to number their lab tasks by using multilevel numbered lists. While not required, the use of multilevel numbered lists is highly encouraged and can assist faculty and students when referring to a specific task or subtask in a lab. Also, if you have added questions in particular tasks or subtasks, then it may be easier for faculty and students to refer to them. For example, the following high-level tasks and subtasks are from a lab exercise called "Lab 3C – PGP Cryptography Using PGP:"

- **4.1: Install PGP Desktop Win64-10.1.1 and Create Your Own Keys**
  - **List of 4.1.1 to 4.1.15 subtasks**
- **4.2: Encrypt Files Using Keys**
  - **List of 4.2.1 to 4.2.5 subtasks**

The author of this lab chose to number his task list starting with 4.1, since the section of the lab is 4 (Tasks). He could have easily started with Task 1 and then listed subtasks as 1.1 to 1.15 and then Task 2 with subtasks 2.1 to 2.5. As long as you are consistent with your numbering scheme throughout your course, modules, and lessons, that is what matters most.

> **TIP**: Frequently when you start to type a number followed by a period, Microsoft Word will automatically start to create a multilevel numbered list for you. If you indent, then it will start to create the next level list, and so on. Please note you may have to define the format of your numbering scheme in Word. If you are unfamiliar with using Microsoft Word's multilevel numbered list, you can always use the application help tool as well as go out to Google and search for information on this topic.

Use of White Space and Indentation. Just as you have seen throughout this guide, white space and indentation can aid in comprehension and present material in a more readable fashion. The same is true when writing lab exercises for students. White space and indentation can assist them to comprehend better what they need to do, especially when looking at and executing commands. Let's take a look at a few examples.

**Bad Example**:

> For this lab, complete the following tasks: Open a terminal window. Type sudo su to become root. Type service postgresql start since Metasploit uses the Postgre SQL database. Type msfdb init to initialize the Metasploit database. Type msfconsole to start the Metasploit framework. Type db_status to verify that the database has connectivity.

**Good Example**:

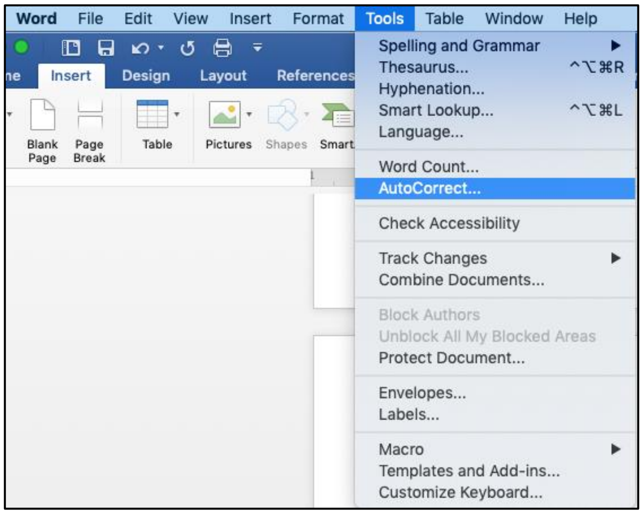
> For this lab, complete the following tasks:
>
> - Open a terminal window and at the prompt type the following:
>     - `sudo su` and press enter to become root.
>     - `service postgresql start` and press enter. We do this since Metasploit uses the Postgre SQL database.
>     - `msfdb init` and press enter. This command initializes the Metasploit database.
>     - `msfconsole` and press enter. This starts the Metasploit framework.
>     - `db_status` and press enter. We do this to verify the database has connectivity.

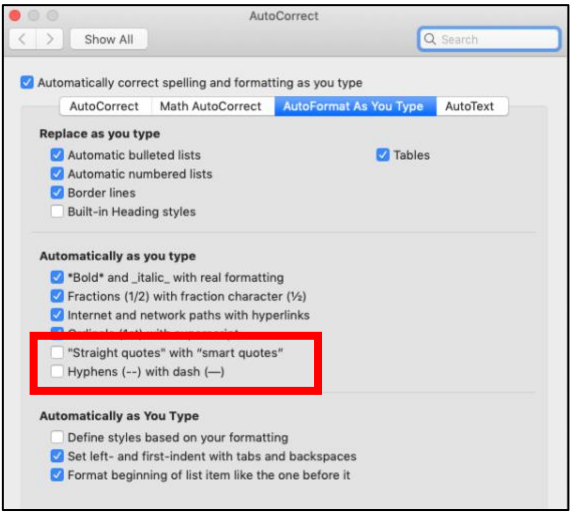
From the examples above, we would hope you agree the "good" example is much easier to follow and read, and the white space and indentations helped immensely. This is true especially when you have to type in commands at a command prompt. Instead of bullets, the "good example" could also easily be modified to have task numbers and subtask numbers. Again, it will be up to you as the author to choose what numbering scheme you wish to use…just be consistent!

Use of Commands/Snippets of Code. Invariably when you write a cybersecurity lab exercise, you will likely be writing commands or snippets of code. As discussed in *Section 3.3.4 Fonts*, ***you***

***must use the Courier New font type in these cases***. There are some other good practices when writing commands or snippets of code.

> **IMPORTANT TIP**: Microsoft Word, by default, has several “autoformat as you type” options turned on for you. It is HIGHLY recommended, even before you begin to write any lab exercise tasks, you turn off these two options: “'Straight quotes' with ‘smart quotes’” and “Hyphens (--) with dash (–),” as they can cause many problems for the faculty and students who will use your lab exercises; this is especially true for commands and snippets of code. You can turn these options off by going to the **Tools** menu in Word and selecting ***AutoCorrect…*** (see left image below) and then unchecking the appropriate boxes (see right image below.)





☑ Automatically correct spelling and formatting as you type

**Replace as you type**

☑ Automatic bulleted lists ☑ Tables
☑ Automatic numbered lists
☑ Border lines
□ Built-in Heading styles

**Automatically as you type**

☑ *Bold* and _italic_ with real formatting
☑ Fractions (1/2) with fraction character (½)
☑ Internet and network paths with hyperlinks
□ "Straight quotes" with “smart quotes”
□ Hyphens (--) with dash (—)

**Automatically as You Type**

□ Define styles based on your formatting
☑ Set left- and first-indent with tabs and backspaces
☑ Format beginning of list item like the one before it

> Why is this recommended? Many teachers may provide their students with electronic copies of the lab exercises. If so, students have the ability to copy and paste the commands into the command line interface (CLI) of their VM. These smart quotes and dashes are NOT recognized in this environment and will cause errors. This will likely confuse and frustrate instructors and students alike. For example, if you leave the "Straight quotes" with “smart quotes” option checked, double and single quotes will be displayed and interpreted differently in the VM’s CLI. Let’s take a look with an example:

```
student@kali ~/Downloads/tmp $ echo "x = $x    And y = $y"
x =          And y =
student@kali ~/ $ export x="one two three...    "  ## Correct CLI quoting
student@kali ~/ $ export y=“four five six...”      ## Smart Quotes
bash: export: `six...”': not a valid identifier

student@kali ~/ $ echo "x = $x    And y = $y"
x = one two three...       And y = “four
student@kali ~/ $
```

> Similar issues occur if you leave the “Hyphens (--) with dash (–)” option checked. Do yourself and others who will use your lab exercises a favor, turn off the two “autoformat as you type” options highlighted above before writing them.

In the previous section, we already saw how useful white space and indentation can assist with readability. Something we did not highlight about the example in the previous section, however, was the use of **bold fonts**. While not required, it can be very helpful to bold commands you want the students to type at the command prompt. Again, let's look at the previous example, which includes commands in bold font:

- Open a terminal window and at the prompt type the following:
  - **`sudo su`** and press enter to become root.
  - **`service postgresql start`** and press enter. We do this since Metasploit uses the Postgre SQL database.
  - **`msfdb init`** and press enter. This command initializes the Metasploit database.
  - **`msfconsole`** and press enter. This starts the Metasploit framework.
  - **`db_status`** and press enter. We do this to verify the database has connectivity.

Now let's see what it looks like without commands in bold font:

- Open a terminal window and at the prompt type the following:
  - `sudo su` and press enter to become root.
  - `service postgresql start` and press enter. We do this since Metasploit uses the Postgre SQL database.
  - `msfdb init` and press enter. This command initializes the Metasploit database.
  - `msfconsole` and press enter. This starts the Metasploit framework.
  - `db_status` and press enter. We do this to verify the database has connectivity.

It's still readable, but the commands do not stand out as much. Let's look at another example of how using bolded font and indenting can focus the student on what they need to type and what they will see as output. You are also encouraged to bold and italicize specific parts of output/commands/code when you want to grab the student's attention. First we look at the "bad" example:

**Bad Example**:

```
student@kali ~/Downloads/tmp $ ls
dir1  dir2  topfile
student@kali ~/Downloads/tmp $ ls -la
total 112
drwxr-xr-x  4 student student  4096 Mar  6 14:40 .
drwxr-xr-x 54 student student 94208 Mar  6 11:45 ..
drwxr-xr-x  2 student student  4096 Mar  6 14:40 dir1
```

```
drwxr-xr-x  2 student student  4096 Mar  6 14:40 dir2
-rw-r--r--  1 student student   268 Mar  6 14:40 topfile
student@kali ~/Downloads/tmp $ ls -la dir2/
total 24
drwxr-xr-x 2 student student 4096 Mar  6 14:40 .
drwxr-xr-x 4 student student 4096 Mar  6 14:40 ..
-rw-r--r-- 1 student student  268 Mar  6 14:40 2_file1
-rw-r--r-- 1 student student  536 Mar  6 14:42 2_file2
-rw-r--r-- 1 student student  268 Mar  6 14:40 2_file3
-rw-r--r-- 1 student student   28 Mar  6 14:44 2_file4
student@kali ~/Downloads/tmp $ file dir2/2_file4
dir2/2_file4: ASCII text
student@kali ~/Downloads/tmp $ cat dir2/2_file4
Contents of file 2_file4...
student@kali ~/Downloads/tmp $
```

Now let's take a look at how we can change the above "bad" example to a "good" one. Notice how bolding fonts and indenting the related command output of the above example can greatly enhance its readability. Also, note how we can bring the student's attention to a specific part of the output (e.g., in the example output below: ***2_file4***) just by bolding and italicizing it.

**Good Example**:

```
        student@kali ~/Downloads/tmp $ ls
        dir1  dir2  topfile
        student@kali ~/Downloads/tmp $ ls -la
        total 112
        drwxr-xr-x  4 student student  4096 Mar  6 14:40 .
        drwxr-xr-x 54 student student 94208 Mar  6 11:45 ..
        drwxr-xr-x  2 student student  4096 Mar  6 14:40 dir1
        drwxr-xr-x  2 student student  4096 Mar  6 14:40 dir2
        -rw-r--r--  1 student student   268 Mar  6 14:40 topfile
        student@kali ~/Downloads/tmp $ ls -la dir2/
        total 24
        drwxr-xr-x 2 student student 4096 Mar  6 14:40 .
        drwxr-xr-x 4 student student 4096 Mar  6 14:40 ..
        -rw-r--r-- 1 student student  268 Mar  6 14:40 2_file1
        -rw-r--r-- 1 student student  536 Mar  6 14:42 2_file2
        -rw-r--r-- 1 student student  268 Mar  6 14:40 2_file3
        -rw-r--r-- 1 student student   28 Mar  6 14:44 2_file4
        student@kali ~/Downloads/tmp $ file dir2/2_file4
        dir2/2_file4: ASCII text
        student@kali ~/Downloads/tmp $ cat dir2/2_file4
        Contents of file 2_file4...
        student@kali ~/Downloads/tmp $
```

In the end, it is up to you to decide to bold your commands or not; however, please note many books written on programming and scripting languages use several typographical conventions to include always bolding commands or text to be typed by the user. If you would like to see more on this topic and others regarding how to write commands/snippets of code, please visit O’Reilly Style Guide and Word List and jump to the Typography and Font Conventions section.

After reading it, you may decide to adopt many of these conventions. Whatever you decide, when writing these labs all we ask is for consistency.

Use of Notes to Instructors. You should feel free to insert notes to instructors anywhere, and as many as needed, throughout the lab exercise document. These notes should contain advice, recommendations, cautionary comments, etc., that you would want any instructor to know about using your lab depending on where they are in the lab exercise handout. It will be left up to the instructor using your lab exercise to delete these notes, as *they are not meant for the students to see*. Let's take a look at a few examples...

**Example 1**: This note was inserted in the Overview section for two-part lab exercise:

> [Note to instructors: This lab exercise is Part-1 of a two-part series. See explanation of what is covered in this Part 1 lab below.]

**Example 2**: This note was inserted in the Resources Required section and should always be included for all lab exercises using the Cyber Range:

> [Note to instructors: This lab exercise requires an account on the Cyber Range. To sign up for an account on The Range, please visit our Sign-Up page. Your students will also require an account on the Cyber Range; this will be explained in the setup of your course.]

**Example 3**: This note was inserted at the end of the Initial Setup section in an OS hardening lab:

> [Note to instructors: It is recommended once completing this lab that you reset all student VMs (as not to affect future or repeat labs using this environment). This is also a good opportunity to refresh students' knowledge of host-based hardening exercises and discuss/explore what ports are still open even in "Public network" mode (port 3389 stays open!). A good way to run this class is to show the class each step passively inspected (but not changed) as to compare the vulnerability assessment results both before and after hardening; this is done in step 4.17 and 4.19 using nmap scans from the Kali VM. Take note that these steps are not meant to include all aspects of OS hardening; however, they do address some of the most fundamental concerns. Remember: one can never achieve 100% secure, which is why we apply security at multiple layers. As the student accomplished various tasks the instructor may consider asking students to take screenshots as deliverables for assignment credits.]

**Example 4**: This note was inserted right after the Tasks header in an advanced port scanning lab:

> [Note to instructors: This is an advanced course. Students should have experience with the basics of Nmap from previous courses. If this is not the case, it may be beneficial to search the Cyber Range repository for lessons on scanning with Nmap. Students should also be knowledgeable about Networking Protocols such as UDP and TCP.]

**Example 5**: This note was inserted in the Tasks section after a comment explaining why the students might see some extra things during the lab that normally wouldn't be there:

[Note to instructors: It is common for students to accidentally do this.]

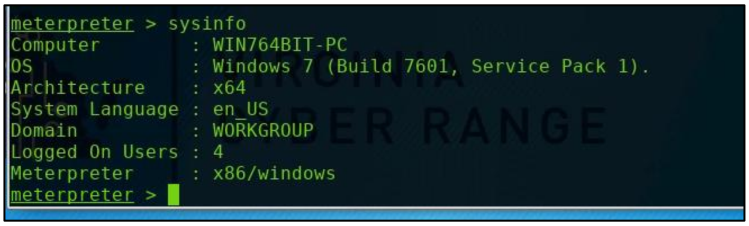
**Example 6**: This note was inserted at the end of the lab in the faculty instruction section, i.e. below this line:

> "
>
> ---
>
> [This portion of the lesson plan is provided for instructors that will be using this lesson plan and associated material in their class.]"
>
> [Note to instructors: The list below is a summary of general hardening practices at the host level.]

From the examples, you can clearly see these notes to instructors can be found anywhere in a lab exercise, and they should be helpful to the instructor who chooses to use the lab(s). Of course, you shouldn't feel compelled to insert them, just for the sake of inserting them, unless you feel they are really needed and worthwhile.

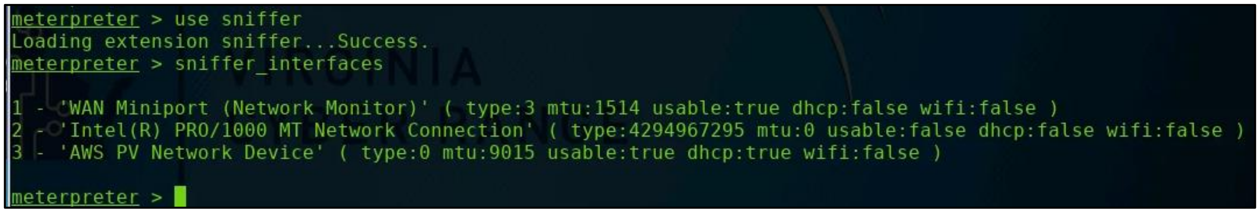
Use of Screen Shots. As they say, "a picture is worth a thousand words." You only need to look in sections *3.4.1 Getting a Virginia Cyber Range Account & Creating a Course* and *3.4.2 Accessing the Exercise Area and Adding VMs to Your Course* of this guide to understand the power of screen shots. Strategically placed in your lab exercises, they provide helpful visual cues and confirmation to the student they are progressing through the lab successfully, especially when executing commands at a command line interface. Imagine the following excerpt from a lab without screen shots:

> Now that we have a privileged account, we can do lots of things.
>
> - In the meterpreter session, type `sysinfo` and press enter.



```
meterpreter > sysinfo
Computer        : WIN764BIT-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter >
```

> - Type `use sniffer` and press enter; this will start the sniffer software.
> - Type `sniffer_interfaces` and press enter to see what networks we can dump packets from.



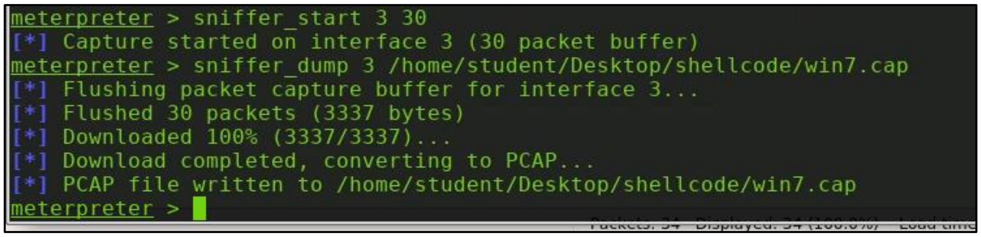
```
meterpreter > use sniffer
Loading extension sniffer...Success.
meterpreter > sniffer_interfaces

1 - 'WAN Miniport (Network Monitor)' ( type:3 mtu:1514 usable:true dhcp:false wifi:false )
2 - 'Intel(R) PRO/1000 MT Network Connection' ( type:4294967295 mtu:0 usable:false dhcp:false wifi:false )
3 - 'AWS PV Network Device' ( type:0 mtu:9015 usable:true dhcp:true wifi:false )

meterpreter >
```

We want to connect to the network device and sniff a few packets.

- Type `sniffer_start 3 30` and press enter; 30 is the amount of packets we want to collect and 3 is the AWS PV Network device that the system uses to access the internet. The other two devices that are listed in the screenshot above are out of scope.
- Type `sniffer_dump 3 /home/student/Desktop/shellcode/win7.cap` and press enter. We are saving the sniffed packets to a file named win7.cap and saving it to the shellcode folder you created on the Desktop.



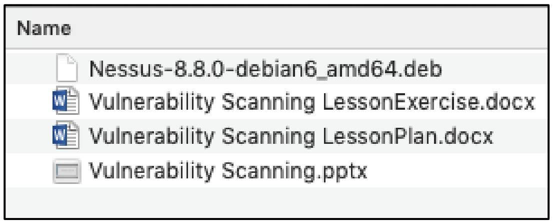
```
meterpreter > sniffer_start 3 30
[*] Capture started on interface 3 (30 packet buffer)
meterpreter > sniffer_dump 3 /home/student/Desktop/shellcode/win7.cap
[*] Flushing packet capture buffer for interface 3...
[*] Flushed 30 packets (3337 bytes)
[*] Downloaded 100% (3337/3337)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to /home/student/Desktop/shellcode/win7.cap
meterpreter > 
```

You can open the .cap file in Wireshark by navigating to the /home/student/Desktop/shellcode/ folder and opening the win7.cap file. If you are using the GUI, you can double click and the file will open in Wireshark.

From the above example, when the student types the meterpreter commands, they can look at the lab handout and be confident they are getting the same results. Without screen shots, they may be wondering if they are getting the right output and what it all means. While not required, don't be surprised if your content coordinator recommends adding screen shots in your lab exercises to assist in the student's learning experience.

Use of Artifacts. Many authors write lab exercises that require the students to install a software package or use specific files to complete the tasks listed in the lab handout. Often, they provide URLs to download these applications/tools and/or files. Since URLs and the applications/tools themselves could change in the future, we want to provide these artifacts directly to the students as opposed to them going out to get them.

If your lab exercise requires specific artifacts (files, applications, tools, etc.), these should be submitted in the lesson folder along with the lab exercise Word document. As an example in the image below from the Vulnerability Scanning lesson, the author submitted the **Nessus-8.8.0-debian6_amd64.deb** (Kali Linux 64 bit version of Nessus) file along with the other required lesson files in their Google Drive. This file then was linked within the lab exercise handout using a *special technique.



| Name |
|---|
| Nessus-8.8.0-debian6_amd64.deb |
| Vulnerability Scanning LessonExercise.docx |
| Vulnerability Scanning LessonPlan.docx |
| Vulnerability Scanning.pptx |

> **IMPORTANT**: If you submit artifacts requiring any special installation codes or passwords, please ensure you provide them in the lab document as well.

*At the time of the writing of this guide, your content coordinator is responsible for getting your artifacts linked in your lab handout. The only thing you are required to do is insert a placeholder before you submit your lab exercise for review. This placeholder can be as simple as including the following text:

> **"Navigate to the following link <to be inserted later> to download…"**

# 4. Miscellaneous

## 4.1 VIRGINIA CYBER RANGE SUPPORT PAGE

We have an online resource, the Virginia Cyber Range Support Page, where you will find a collection of knowledge base (KB) articles to assist you in using the Cyber Range and exercise environments. This resource will be particularly helpful if you plan to write lab exercises that will use the Cyber Range's virtual environments. You will likely find what you are looking for in the FAQ and Troubleshooting sections; however, we encourage you to peruse and become familiar with the entire KB, as it will help you in writing labs for our environment. Please keep in mind, however, that the KB is written more for the end user and not an author.

## 4.2 SUBMITTING VIDEO CONTENT

Some authors may desire to submit video content as supplemental material to accompany their written lab exercises. Since these videos will be posted online and will be intended for students at all educational levels from K12 to graduate, these videos must comply with federal accessibility laws. If you plan to submit video content, at a minimum, you must provide transcripts for each video you submit.

At the time of the writing of this guide, we are looking into the ability for our authors to close caption videos instead of providing transcripts. We will notify you if and when this capability is available.

## 4.2 GRANTING OTHERS PERMISSION TO YOUR GOOGLE DRIVE

While collaboration and sharing are normally encouraged in academia, you are NOT allowed to give anyone permissions to the content in YOUR specific Google Drive. As an author, you have entered into a legal contract with the Cyber Range and we own all rights to this drive. If you have a need for other collaborator(s) to assist in writing content, you should contact your content coordinator to discuss this request.

# 5. Lessons Learned

We asked authors who are already published in the repository to provide some lessons learned to assist you as you continue to create/re-purpose/reformat content. We have also put a few of our own lessons learned as the folks who are reviewing the content. Here is what they said (in no particular order):

**Get feedback early!** As you complete a lesson plan, for example, ask for initial feedback to ensure you are on the right track. This goes for all of the other content categories: syllabus, module description, labs/exercises, slides, and exams/quizzes.

**Reserve plenty of time to work on your course content.** If you think it will take one week, plan on three! Making sure that another instructor can deliver your course requires lots of careful planning and reflection, and sometimes you don't realize just how much until you get into the middle of the course creation process.

**When preparing Module overviews, think about it from the perspective of another instructor who is seeking teaching materials.** Put as much information on the Module overview so that the instructor knows what resources are needed to do this collection of lessons. Include pointers to lecture slides, labs, exams, answer keys, and resources (books and journal articles) that support the lessons.

**Look at documents already posted in the repository.** These are properly formatted and use the templates provided.

**Properly cite sources for all images, charts, diagrams, etc. in your PowerPoint slides.** If you cannot properly cite, then replace it with something you can cite properly or delete it altogether.

**Do not provide copyrighted material**, but feel free to provide links to journal articles or recommended texts (for purchase). The VA Cyber Range cannot host this content. If at all possible, try to point to open source references using hypertext links.

**Test all lab exercises** to be sure that all steps function properly, and no critical information is left out. Instructions for how to access virtual machines, required data, and required software should be clear and (if possible) more than one way to get the information. Provide answer keys (or relevant guidance for instructors) for labs.

**Explain how each lesson's content enhances the student's understanding of cybersecurity.** This can promote interest and engagement for both students and instructors.

**Use the NICE Specialty Areas to navigate KSAs.** If you can narrow down the emphasis of your lesson to 1-3 NICE areas, this will reduce the number of places you need to look for KSAs. You can use the links in the Table of Contents (NIST SP 800-181) to bring you to the Knowledge, Skills, and Abilities that best fit your material.

**Use keyword searches to look for KSAs and KUs** addressed in the content you provide. At first it seems a bit daunting, but it's pretty easy to do.

**Feel free to use your own file structure to post your documents.** For example, one author put all Module 1 files (module description, lesson plans, slides, exercises, and exams) in one folder labeled Module 1, and then Module 2 files, etc. The initial file structure on Google Drive is meant merely to draw your attention to what documents are required. As long as all required documents are there and easy to find, there is no need to file away each document in its own folders.