Cybersecurity

Teaching Guide

Lessons

The lessons follow the CompTIA Security+ (SYO-601) objectives and are broken down into 155 individual lessons. Every lesson contains a summary PowerPoint which teachers can use to guide the students through the content. The PowerPoint lessons were created to be presented to students with the teacher explaining/guiding the students through each slide. The PowerPoints are not meant to take up an entire class period, teachers should be able to combine several related PowerPoint lessons into a single class period.

Teacher Notes

Every PowerPoint lesson has a Teacher Notes to go along with the lesson. These Teacher Notes are intended to be used to provide background and explain the different concepts for the teacher who will be guiding the class. It is up to the teacher's discretion whether to share these notes with students.

Labs (Resource)

The Labs are hands-on lab exercises in the form of an attack, example, or tool that help support the lessons. An attack lab will show the students a real-world example of how a malicious user can attack an unsuspecting user's system and how this user can defend themselves. An example lab has the students run through a concept and see an example of how things work. The tool lab has the students use and explore different tools used in pen and vulnerability testing. The labs use a Kali Linux Machine and a Windows 7 Machine connected on the same network. Although the labs were written on the US Cyber Range, they can be done on most ranges or environments that include the two machines.

Most of the labs in Cybersecurity utilize a Kali Linux environment. This may be a foreign concept to a lot of students (and educators). The Linux Command Line appendix contains a PowerPoint to introduce the students to Linux and why it is such a powerful operating system and the role of Linux in cybersecurity. There is also a *Linux 101* and *102* lab on a Linux machine to introduce the students to the Linux environment. It is highly recommended to have the students with no prior Linux experience work through the *Linux 101* and *102 Lab* before attempting other labs.

Case Studies (Resource)

Some lessons have case studies which involves a scenario that happened in the real world. Each case study contains an entire article, along with the source, author, and date published. After the article, there is also a teacher summary, guided questions, and links to further readings on the topic. It is intended for the students to read through the article and then the teachers present the guided questions to the students to think about the concept. If a student is super engaged in a case study and want to learn more, the teacher can then present the student with the further readings. The teacher summary is to quickly summarize the scenario for the teacher so they can get an idea of what the article is about, and whether they would like to use the case study, without having to read the entire article. It is up to the teacher if they give the teacher summary, guided questions, or further reading to their students.

Quizzes

All 155 lessons have an assessment, or quiz questions in either multiple choice, multiple selection, or true/false format. Quizzes are provided in Word format for easy modification for classroom use. Quizzes are also provided in QTI format for easy import into most modern, robust Learning Management Systems (LMS) like Google Classroom, Moodle, etc.

Appendices (Supplemental Materials)

There are three appendices contain additional information about the Networking and Cyber Law. These materials are not required for or tested on the Security+ certification exam, though several state standards rely on one or more of these topics to be addressed in a Cybersecurity course.

The *Networking* appendix introduces students to fundamental networking concepts that they will see, and use, throughout the Cybersecurity course. The Networking appendix covers the OSI Model of networking, explains the basics of IP addresses and ports, and gives a brief explanation of major networking concepts. This appendix is helpful for gaining a quick understanding of networking for students with no prior experience.

There are a lot of legal and ethical concerns when dealing with cybersecurity. Key to understanding legal constraints is what is referred to as cyber law. These topics are covered in the *Legal Considerations* lesson in Appendix C which covers major landmark legal cases and laws. Many of the Case Studies offered throughout Cybersecurity also talk about legal and ethical concerns in the real world.

Worm (Supplemental Materials)

Worm is a book written by Mark Bowden about the Conficker worm and the group of people who helped stop this malware from potentially taking down the internet. We have provided a series of questions and answers for each chapter of *Worm* that the students can work through as they read the book. This content is not a required component for the Cybersecurity course, but in the book, Mark Bowden explains challenging cybersecurity topics in a way that makes it easy for students to understand while telling the story of the Conficker worm and the mechanisms created to thwart future cybersecurity threats on the internet.

Support Materials

In the support materials, there is the *Teaching Guide* (this document) which helps explain how the course is laid out and helps explain the purpose of the content to educators.

There are also Lab and Case Study description documents. These guides are meant to explain to teachers the purpose of each lab and case study to help teachers determine which lab/case study are suitable and beneficial their students and/or if they are capable of running particular labs.

There is an *Acceptable Use Policy* which the teachers can have the students sign at the beginning of the course. The document lays out different terms and conditions for the students and the course and is designed to help deter the students from using the knowledge and skills gained from this course in a malicious manner. The *Acceptable Use Policy* document is formatted into two pages. The students would review and keep page 1 while they would sign and return page 2 to their classroom teacher.

Lastly, there are the links to the *CompTIA Security+ SYO-601 Certification Objectives* and the *CAE-CD Knowledge Units* that the Cybersecurity course is aligned to.

Security+ Exam and Standards Alignment

CYBER.ORG chose to align this course to the CompTIA Security+ certificate because not only is it an industry-recognized certification but it also covers most states' existing cybersecurity standards (at then some!). At the end of the course, students may opt to take the CompTIA Security+ exam to become Security+ certified which will allow students to obtain an industry-accepted cert as well as making them more marketable as they pursue careers after high school.

Many states use industry-recognized certifications as justification for classifying various courses as CTE-applicable. This status may provide access to Perkins funding or may impact a state's school accountability rating. Laws and policies for this vary from state to state and district to district. A first stop for guidance should be your school's CTE or Curriculum & Instruction leadership.

For additional assistance in aligning CYBER.ORG's Cybersecurity course (CompTIA Security+ Objectives) to your state's standards, or for help verifying if Security+ is a CTE course in your state, please reach out to Joe MacAdam at joe.macadam@cyber.org and Jonathan Bartles at jonathan.bartles@cyber.org For any additional questions, please contact the CYBER.ORG team: info@cyber.org.