Syllabus for Cybersecurity (CYBER.ORG Partnership)

About this course:

Cybersecurity lays a foundation for understanding cyber law and policy, Linux, networking technology basics, risk assessment, cryptography, and a variety of cybersecurity tools – all the essential knowledge and skills needed to begin a future in the cybersecurity workforce. Not only does Cybersecurity introduce the breadth of cybersecurity concepts and skills to students, but it also prepares them to verify their technical know-how through the CompTIA Security+ certification.

At the end of this course, you will:

- Understand the concepts behind cybersecurity (lessons)
- Practice a variety of cybersecurity skills in a safe setting (labs)
- Have a greater understanding of the history of cybersecurity (case studies)

Security+ Exam:

The content in the Cybersecurity course from CYBER.ORG is built around the CompTIA Security+ certification exam because it is an exceptional industry-recognized certification. Additionally, it is a credential that has been approved by a variety of state departments of education as a contributing component to earning a diploma. The course introduces all of the Security+ objectives SY0-601 as well as providing a secure and safe laboratory environment to practice those objectives. Students should be encouraged to obtain the certification before graduation, making them significantly more marketable as they pursue careers after high school.

Security+ Objectives:

- Threats, Attacks, and Vulnerabilities
- Architecture and Design
- Implementation
- Operations and Incident Response
- Governance, Risk, and Compliance

Required Resources:

Within this course, there are labs in the form of hands-on exercises that demonstrate an attack, example, or tool that help support the lessons. An attack lab will demonstrate 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 users run through a concept and see an example of how things work. The tool lab explores different tools used in penetration and vulnerability testing. The labs use a pair of Kali Linux and Windows 7 machines 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.

Instructional Units:

1. Linux Basics (20 hours)
2. Security Basics (35 hours)
3. Actors and Vulnerabilities (30 hours)
4. Malware and Attacks (60 hours)
5. Organizational Security (35 hours)

Sequencing:

There are a total of 155 lessons the instructional units above. Every lesson is a short instructional moment that is designed to introduce a concept and prepare for an exercise. It is the intent of the curriculum design team for teachers to present multiple lessons in a 50- or 80-minute class and supplement them with a lab or case study. While the numbered list provides a suggested order of delivery for the content, it is only a recommendation. Classroom teachers may present lessons in any order that works best for their particular classroom and students' needs. Pacing, scheduling differences, and student learning differences will affect timelines differently. Suggested contact hours are stated in parenthesis.

Student Diversity and Equity:

CYBER.ORG believes in empowering all students. By expanding student participation in cybersecurity and computer science, we hope to enable student agency in a range of disciplines. Delving into a variety of topics within the course seeks to demystify the technological world around us and, in turn, provide opportunities for further learning through personal curiosity.