Course Details: The course is second in a series to introduce high school students to cybersecurity concepts and inspire interest in cybersecurity careers. The course is able to be delivered completely on Chromebooks with no specialized equipment. It includes access to a cyber range for online labs at zero cost to districts. The course incorporates the 2020 New Jersey Student Learning Standards – Computer Science and Design Thinking.

This course is designed for students who are interested in exploring careers in, and the foundations of Cybersecurity. Building on the concepts from Introduction to Cybersecurity, instruction will focus on vulnerabilities found in digital systems and methods to implement defense. Students will apply tools to identify vectors of attack and ways to mitigate vulnerabilities. Advanced forms of cryptography will be explored along with the role they play in securing remote transactions. Hands-on labs executed in a cyber range provide practice in the configuration and mitigation of system vulnerabilities. Each unit integrates current events with cyber ethics and law. *Ethics agreement must be signed by all students and parents during the first 2 weeks of class. PRE: Intro to Cybersecurity I

Syllabus

Learning Objectives:
Upon conclusion students will be able to:

- Explore ethical issues associated with information security.
- Examine the laws and rules that apply to digital activities.
- Define techniques for reconnaissance of digital targets.
- Apply Google Dorking methods for advanced searching.
- Identify how the Internet structure and Domain Name System can be used for reconnaissance and attacks.
- Use the Terminal for Linux commands and tools.
- Configure network IP addressing and subnetting.
- Identify types of network-based attacks including DoS, spoofing, MITM and transitive.
- Define the vulnerabilities of Wireless and Mobile technologies.
- Examine the use of Virtual Private Networks to protect public communications.
- Explore the use of cybersecurity tools for pentesting and for exploits.
- Define cyberwar and examine the use by nation states of cybersecurity attack tools.
- Identify vulnerabilities in web applications including SSL, input validation, Javascript, XSS, and buffer overflow.
- Define databases, SQL and the steps of a SQL injection attack as well as best practices for protection.
- Compare the characteristics of the Defense in Depth and the Zero Trust theories.
- Describe and compare defensive hardware/software devices including firewalls and intrusion detection systems.
- Identify how access control and segmentation can be implemented as defense tools.
- Apply basic cryptographic ciphers including hashes and symmetric.
• Apply advanced cryptographic ciphers including asymmetric and digital signatures.
• Identify organizations and tools available to assist with vulnerability assessment and mitigation.
• Complete tasks with cyber tools including Linux CLI, Wireshark, Nmap, CyberChef, Burp Suite, browser Developer Tools, Metasploit and SQL programming.
• Explore career opportunities in cybersecurity and evaluate the skills and education requirements in areas of career interest.

Instructional Units

Unit 6 Law & Ethics
6.1 Impact of Law and Ethics on Cybercrime

Unit 7 - Reconnaissance
7.1 Recon Introduction and Google Dorking
7.2 WHOIS and Nslookup
7.3 Network Scanning

Unit 8 – Network & System Threats
8.1 Denial of Service (DoS)
8.2 Spoofing & Sniffing
8.3 Wireless, Mobile & VPNs
8.4 Pentesting & Exploits
8.5 Cyber War

Unit 9 – Securing Online Components
11.1 Interactive Web Vulnerabilities
11.2 Basic Web Code Attacks
11.3 SQL Database Attacks

Unit 10 – Defensive Tools and Techniques
9.1 Network Defense
9.2 Monitors and Alarms
9.4 Encryption for Online Security

Through course labs, students will be introduced to cyber competitions including PicoCTF, CyberStart America and CyberPatriot. These events provide students with opportunities to independently expand their cybersecurity learning, to win scholarships, and to access career pathways.