Intro to Cybersecurity

Course Syllabus

Course Details:
The goal of this year long course is to introduce students to basic cybersecurity concepts and inspire interest in cybersecurity careers. This course does not require any prerequisite knowledge in computing or cybersecurity for either the student or teacher. The course can be delivered completely on Chromebooks with no specialized equipment. It includes the use of the CYBER.ORG Range, which is a no cost cyber range for all K-12 educators. The course is meant as an introduction course to CYBER.ORG's Cybersecurity course.

Catalog Course Description:
This course is designed for students who are interested in exploring careers in Cybersecurity. The focus of instruction will include the implementation and monitoring of security on network and computer systems. Students will investigate strategies to identify and protect against security threats such as hackers, eavesdropping and network attacks. The basics of cryptography and logic reasoning will be explored. Hands-on labs in the CYBER.ORG Range provide practice in the configuration and mitigation of system vulnerabilities. Each unit integrates current events and related cyber ethics and law. *Ethics agreement must be signed by all students and parents during the first 2 weeks of class.

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

GALANTECH with GARDEN STATE CYBER
CYBER.ORG

Learning Objectives

- Compare and contrast different types of social engineering techniques.
- Define the CIA Triad and key principles of cybersecurity.
- Identify authentication methods, types of attacks on authentication and best practices for mitigation.
- Identify types of malware and methods of mitigation.
- Define social engineering techniques, phishing and tools for OSINT (Open Source Intelligence).
- Use the Terminal for Linux and Windows commands and tools.
- Apply best practices for secure device configuration.
- Apply threat modeling to home and personal IOT threats
- Compute binary and hexadecimal numbers.
- Apply basic encoding and cryptographic ciphers.
- Identify key parts of a PC and define interaction of PC components.
- Identify the components, major services and protocols deployed on TCP/IP networks.
- Capture and analyze network packets.
- Complete tasks with cyber tools including Wireshark, CyberChef, binwalk, exiftool, hex editor, vulnerability scanner and bash scripting.
- Explore career opportunities in cybersecurity and evaluate the skills and education requirements in areas of career interest.
- 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 and MITM.
- 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 cookie manipulation, input validation, command injection, XSS, and buffer overflow.
- Define databases, SQL and the steps of a SQL injection attack as well as best practices for protection.
- 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.

Instructional Units

Unit 1 - Foundations & Threats

- 1.0 - Cybersecurity Careers, course objectives and Ethics Agreement
- 1.1 - The CIA Triad and Authentication
- 1.2 - Identifying Security Threats
- 1.3 - Introduction to CLI (Command Line Interface)

Unit 2 - The Human Factor

- 2.1 - Social Engineering
- 2.2 - OSINT & Phishing

Unit 3 - Data Safety and Best Practices

- 3.1 - System Hardening
- 3.2 - IOT Threat Modeling

Unit 4 - Cryptography and Linux

- 4.1 - Bits, Binary and Encoding
- 4.2 - Basic Concepts of Cryptography
- 4.3 - Advanced Linux Command Line Interface
- 4.4 - Crypto Issues of Privacy vs Security

Unit 5 - Devices and Networking

- 5.1 - Computing Devices
- 5.2 - Networking Fundamentals
- 5.3 - Protocols and Packets

End of Part 1 Projects (Extension materials)

- Biometric Authentication Product Pitch
- Social Engineering PSA Video
- Benchmark Selections for OS Hardening
- Making an Impact with Technology

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 Net Attacks - Denial of Service (DoS)
- 8.2 Spoofing & Sniffing
- 8.3 Wireless, Mobile & VPNs
- 8.4 Pentesting & Exploits
- 8.5 Cyber War

Unit 9 - Online Threats

- 9.1 Basic Web Concepts
- 9.2 Web Vulnerabilities
- 9.3 SQL Database Attacks

Unit 10 - Encryption Security Tools

- 10.1 Symmetric & Asymmetric Encryption
- 10.2 SSL for Online Security

Cyber Competitions: through course labs students will be introduced to cyber competitions including the National Cyber Cup, 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.