Cyber Forensics and Advanced Cyber Forensics

Huntsville High School 2020 - 2021

Instructor: Jim Morse, james.morse@hsv-k12.org, 256.428.8050 ext. 237

Course Number: 520042, 520040 Prerequisite: Network Pro Certification or Principles of InfoSec

Fee: $45

I. Course Description:

This is a one-credit course designed to provide students with skills involving a hands-on, career-oriented approach to learning enterprise network security that includes practical experiences using forensics tools. This course implements activities using secure networking and computing best practices along with other practical activities for developing security standards that govern organizational compliance. This course includes concepts and exercises that emphasize different aspects of security in terms of implementations, processes and procedures, and career opportunities..

Topics Covered:

- Linux Terminal Tools
- Defending against attacks
- Recon and intel gathering
- Vulnerability scanning and management
- Incidence response
- Forensic analysis
- Policies and compliance
- Access Control Management
- Software development security
- Developing a forensic toolkit

II. Course Objective

Students successfully finishing this course should have the knowledge to test and pass the CompTIA Linux+ and/or CSA+ Certifications, compete in the Platinum Division of the CyberPatriot competition, complete in the Skills USA State Cybersecurity competition and participate in local and online Forensic Capture the Flag competitions.

III. Resources, Materials and Tools:

- Online Curriculum: Testout.com and Cisco Academy (netacad.com)
- Other online resources

IV. Classroom Expectations: Students are expected to:

- **respect** others.
- follow the Huntsville City Schools and Huntsville High School's Disciplinary Guidelines as laid out in the student and parent handbook and the BLOOM documentation.
- follow the Huntsville City Schools Computer Use Policy that the student and parent signed when picking up their student computer.
- follow the Huntsville City Schools Cyber Academy's **Code of Conduct**.
- attend class as directed by their schedules, arrive on time and be ready to learn something new each day the class meets.
- understand that cybersecurity is a **difficult subject,** and they are expected to use the class time on cybersecurity.
- check the SCHOOLOGY page for this class daily, realizing that even if they miss a class, they are responsible for the materials presented and for completing assignments. All class resources used in class will be posted to the class Schoology page.
- follow the **Honor Code** by doing their own work and by not plagiarizing when completing assignments and projects. Follow copyright laws.
- be responsible for their education. Do your work, study for tests, ask questions, do not let others distract you and research subjects you are having difficulty with.

V. Grading Policy

Students will receive grades for completing assignments, assessment, and class activities as well as creating individual and group projects, and preparing for and competing in Skills USA and/or CyberPatriot. Official grades will be posted to PowerSchool weekly.

Assignments:

- Make up 40% of each 9 week's grade.
- Includes: class assignments, competition assignments, minor projects, minor labs
- All assignments will be posted on the Schoology class page and should be submitted to the Schoology class page for credit.
- Assignments may direct the student to another resource to complete an activity, with proof of completion submitted on Schoology.
- Assignments are expected to be turned in on due date unless circumstances prohibit the student from doing so OR the student has an IEP or 504 plan that allows extended time for completion.
- Assignments missed will receive a zero (0) for the assignment until completed.
- Assignments submitted after the due date will receive a maximum grade based on the following:
    - One class day late: 30% deduction.
    - Two class day: 40% deduction.
    - Three or more days late: 50% deduction.
    - No late work accepted after 5 class days late.
    - Late assignments will NOT be accepted during the last week of each grading period.
- Typical Assignment of points:
    - Class Activities: 5pts
    - Class Assignments: 10 – 20 points
    - Projects and Labs: 25 to 50 points

Assessments:

- Make up 60% of each 9 week's grade.
- Assessments will be posted on Schoology as a calendar event and as an assignment,
- Assessment delivery:
    - Online Question/Answer or Simulated labs
    - In person, hands-on labs
- Assessments should be completed using the student's skills, abilities, and knowledge. Phones, and use of other web pages other than the test page will be deemed as a violation of the Honor Code.
- Assessments may be timed to limit the opportunity for students to use outside resources to complete the assessment as well as prepare for the certification exam at the end of the course which is timed.
- With some assessments, students will have the opportunity to have additional attempts to receive a satisfactory grade. When this occurs, grades will be determined by averaging the attempts together or accepting the first attempt's score if it is higher.
- If an assessment is missed with a school related or excused absent, students will have until the next assessment to complete it. If it is not completed in time, a zero will be posted for the assessment grade.
- If an assessment is missed with an unexcused absence, students will take the exam during the next 48 hours, either before school, after school, during Panther hour or lunch.

Exams:

Exams are assessments that are given at the end of each semester of the course to assess the long-term understanding of the concepts presented in the class thus far.

- Exams may be Q/A type, Hands-on, or a combination.
- If a student misses an exam, their exam score will be a 0%

Final Grade Calculations:

- Semester Grade Make-up:
    - First 9 weeks: 45%
    - Second 9 weeks: 45%
    - Semester Exam: 10%
- Final Grade Make-up:
    - First Semester: 50%
    - Second Semester: 50%

VI. Sample Lessons

- Students will demonstrate their understanding of computer hardware by building a simple LAN that includes a server that provides a game server to its clients.
- Students will demonstrate their understanding of IP Address conversion by competing in a class competition on the Cisco Conversion Game.
- Students will read and review various cybersecurity articles.
- Students will choose an entry level networking career and complete a written research report on it's:
    - Employment Requirements
    - Average national salary
    - Best location to work based on employability, cost of living, etc…
    - Time requirements

VII. Learning Standards

1. Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes.
2. Given a network-based threat, implement or recommend the appropriate response and countermeasure.
3. Explain the purpose of practices used to secure a corporate environment.
4. Analyze the output of a vulnerability scan.
5. Compare common vulnerabilities found in the various enterprise target devices.
6. Distinguish threat data and behavior to determine the impact of an incident.
7. Prepare a cyber security toolkit and use appropriate forensic tools during an investigation.
8. Explain the importance of communication during an incident response.
9. Analyze common symptoms to select the best course of action to support incident response.
10. Use data to recommend remediation of security issues related to identity and access management
11. Review security architecture and make recommendations to implement compensating controls
12. Use application security best practices while participating in the software development life cycle.
13. Compare the general purpose and reasons for using various cybersecurity tools and techniques.