Principles of Information Security

Huntsville High School 2020 - 2021

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

Course Number: 520039 Prerequisite: Foundations Pro or ITF+ Certification Exam Fee: $45

I. Course Description:

This is a one-credit course designed to provide students with a basic understanding of various types of computer networks and their security concerns. Students will examine devices, equipment, topologies, and communication protocols. They will explore virtual and cloud technologies and simulate networks in labs to explore properties, settings, and capabilities of networking devices. Routing and Switching protocols will be explored as well as various connectivity media. Security will be examined to understand authentication, and network access controls, security policies, threat mitigation and vulnerability assessment of networking devices and their operating systems.

Students will discover and investigate College and Career pathways that are related to cybersecurity and networking fields. Students complete their course by preparing for and taking the CompTIA Network+ certification exam or another similar exam.

Student involvement and in Skills USA, a career tech student organization, and/or security-based competitions is a requirement of the course and will enhance the concrete benefits of the classroom. This involvement will expand work-place readiness skills and broaden opportunities for personal and professional grow.

Topics Covered:

- Ethics and Safety in the Information Age
- OSI Model and TCP/IP Models of Networking
- Basic Networking Concepts
- Networking Infrastructure
- Network Operations
- Network Security
- Networking Tools and Troubleshooting

II. Course Objective

Students successfully finishing this course should have the knowledge to test and pass the CompTIA Network+ Certification, compete in the Platinum Division of the CyberPatriot competition, complete in the Skills USA State Cybersecurity competition and enroll into the Cyber Forensics Class for the 2022 - 2023 School year.

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.
- Typical Assignment of points:
    - Class Activities: 5pts
    - Class Assignments: 10 – 20 points
    - Projects and Labs: 25 to 50 points
- Late assignments will NOT be accepted during the last week of each grading period.

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. Explain professional, legal, and ethical responsibilities in the field of cyber security, including the need for a diverse work force.
2. Explain the purposes and uses of ports and protocols
3. Explain devices, applications, protocols, and services at their appropriate OSI layers.
4. Explain the concepts and characteristics of routing and switching.
5. Given a scenario, configure the appropriate IP addressing components.
6. Compare the characteristics of network topologies, types, and technologies.
7. Given a scenario, implement the appropriate wireless technologies and configurations
8. Summarize cloud concepts and their purposes.
9. Explain the functions of network services.
10. Given a scenario, deploy the appropriate cabling solution
11. Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them
12. Explain the purposes and use cases for advanced networking devices.
13. Explain the purposes of virtualization and network storage technologies
14. Given a scenario, use appropriate documentation and diagrams to manage the network
15. Compare business continuity and disaster recovery concepts.
16. Explain common scanning, monitoring and patching processes and summarize their expected outputs
17. Given a scenario, use remote access methods
18. Identify policies and best practices
19. Summarize the purposes of physical security devices
20. Explain authentication and access controls
21. Given a scenario, secure a basic wireless network
22. Summarize common networking attacks
23. Given a scenario, implement network device hardening
24. Explain common mitigation techniques and their purposes
25. Explain the network troubleshooting methodology
26. Given a scenario, use the appropriate tool
27. Given a scenario, troubleshoot common wired connectivity and performance issues
28. Given a scenario, troubleshoot common wireless connectivity and performance issues.
29. Given a scenario, troubleshoot common network service issues.