COURSE OUTLINE: NASA104 - FUND OF NET SECURITY

Prepared: Sam Laitinen
Approved: Corey Meunier, Chair, Technology and Skilled Trades

Course Code: Title	NASA104: FUNDAMENTALS OF NETWORK SECURITY
Program Number: Name	2196: NETWRK ARCH & SEC AN
Department:	COMPUTER STUDIES
Semesters/Terms:	20F
Course Description:	This course provides an in-depth study of network security principles, standards, cryptography, best practices and current threats. Supported by extensive lab work, system vulnerabilities, network attacks will be investigated and solutions implemented using a variety of operating systems and security tools.
Total Credits:	4
Hours/Week:	4
Total Hours:	60
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Essential Employability Skills (EES) addressed in this course:	EES 1 Communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience. EES 2 Respond to written, spoken, or visual messages in a manner that ensures effective communication. EES 3 Execute mathematical operations accurately. EES 4 Apply a systematic approach to solve problems. EES 5 Use a variety of thinking skills to anticipate and solve problems. EES 6 Locate, select, organize, and document information using appropriate technology and information systems. EES 7 Analyze, evaluate, and apply relevant information from a variety of sources. EES 8 Show respect for the diverse opinions, values, belief systems, and contributions of others. EES 9 Interact with others in groups or teams that contribute to effective working relationships and the achievement of goals. EES 10 Manage the use of time and other resources to complete projects. EES 11 Take responsibility for ones own actions, decisions, and consequences.
Course Evaluation:	Passing Grade: 50%, D A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.
Other Course Evaluation &	NOTE: You must obtain a minimum mark of 50% in both the Theory portion and the Lab portion

In response to public health requirements pertaining to the COVID19 pandemic, course delivery and assessment traditionally delivered in-class, may occur remotely either in whole or in part in the 2020-2021 academic year.

Assessment Requirements:

of the course. Failing to do so, will result in an overall failing grade (F).

The professor reserves the right to adjust the mark up or down based on attendance, participation, leadership, creativity and whether there is an improving trend.

- Students must complete and pass both the test and lab portion of the course in order to pass the entire course.
- All Assignments must be completed satisfactorily to complete the course.
- A minimum of 80% attendance required in the lectures and labs.
- Makeup Tests are at the discretion of the instructor and will be assigned a maximum grade of 50%.
- The professor reserves the right to adjust the number of tests, practical tests and quizzes based on unforeseen circumstances. The students will be given sufficient notice to any changes and the reasons thereof.
- A student who is absent for 3 or more times without any valid reason or effort to resolve the problem will result in action taken.

NOTE: If action is to be taken, it will range from marks being deducted to a maximum of removal from the course.

Books and Required Resources:

CCNA Cybersecurity Operations Lab Manual
Publisher: Cisco Networking Academy
ISBN: 9781587134388

CCNA Cybersecurity Operations Course Booklet
Publisher: Cisco Networking Academy
ISBN: 9781587134371

Course Outcomes and Learning Objectives:

Course Outcome 1	**Learning Objectives for Course Outcome 1**
Explain the basics of Cyber security	• Examine the dangers of security incidents • Examine the roles of those in the security industry
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Explore the Security Functions of the Windows Operating System	• Explore the history of the Windows Operating System • Describe the Windows Architecture and Operations • Explore the process of administering Windows
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Explore the Linux Operating System	• Explore the basics of Linux • Work with the Linux Shell • Explore the process of administering Linux • Explore working with the Linux Hosts
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Explore Network Protocols and Services	• Explore Network and Communication protocols • Explore IPV4 and IPV6 addressing • Explore the Address Resolution Protocol • Examine Network Services
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Network Infrastructure Overview	• Explore Network Communication Devices and the function of those devices • Overview of the Network Security Infrastructure and how

	various devices fit into that infrastructure • Explore Network Representations
Course Outcome 6	**Learning Objectives for Course Outcome 6**
Explore the Principles of Network Security	• Define the Principles of Security • Overview of Attackers and tools that they use • Explore Common Threats and Attacks
Course Outcome 7	**Learning Objectives for Course Outcome 7**
Explore Network Attacks	• Examine Attackers and the tools they use • Examine the attacks used on the foundation of the network • Examine exposed services like email, databases, and http
Course Outcome 8	**Learning Objectives for Course Outcome 8**
Explore ways to Protect the Network	• Examine defenses and security policies • Explore Access Control • Explore Threat Intelligence Services
Course Outcome 9	**Learning Objectives for Course Outcome 9**
Explore Cryptography and PGP	• Explore Cryptography and Encryption • Explore Public Key Infrastructure
Course Outcome 10	**Learning Objectives for Course Outcome 10**
Explore Endpoint Security and Analysis	• Explore Malware Protection • Explore Host based Intrusion Protection • Explore an Endpoint Vulnerability Assessment
Course Outcome 11	**Learning Objectives for Course Outcome 11**
Explore Security Monitoring	• Explore Monitoring Security Protocols • Explore Log Files including end device and network logs
Course Outcome 12	**Learning Objectives for Course Outcome 12**
Explore Intrusion Data Analysis	• Examine evaluating alerts • Explore working with network security data • Define and Explore Digital Forensics
Course Outcome 13	**Learning Objectives for Course Outcome 13**
Explore Incident Response and Handling	• Examine Incident Response Models • Example Incident Handling

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Attendance and Assignments	10%
Labs	30%
Quizzes	10%
Tests	50%

Date: October 1, 2020

Addendum: Please refer to the course outline addendum on the Learning Management System for further information.

In response to public health requirements pertaining to the COVID19 pandemic, course delivery and assessment traditionally delivered in-class, may occur remotely either in whole or in part in the 2020-2021 academic year.

In response to public health requirements pertaining to the COVID19 pandemic, course delivery and assessment traditionally delivered in-class, may occur remotely either in whole or in part in the 2020-2021 academic year.