COURSE OUTLINE: NASA203 - SECURING THE EDGE

Prepared: Christopher Barnett
Approved: Martha Irwin, Dean, Business and Information Technology

Course Code: Title	NASA203: SECURING THE EDGE & SECURITY ANALYTICS
Program Number: Name	2196: NETWRK ARCH & SEC AN
Department:	COMPUTER STUDIES
Academic Year:	2023-2024
Course Description:	This course will study the theory of monitoring and securing an organization. Cybersecurity principles will be studied to understand both external and internal threats an organization may face. The course will explore the principles of Network Security Monitoring along with its implementation and analysis of network captures. It delivers technical knowledge, insight, and hands-on training needed to prepare a network against and monitor a network for intrusion.
Total Credits:	5
Hours/Week:	4
Total Hours:	56
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Vocational Learning Outcomes (VLO's) addressed in this course: **Please refer to program web page for a complete listing of program outcomes where applicable.**	**2196 - NETWRK ARCH & SEC AN** VLO 2 Perform network monitoring, analysis and troubleshooting to determine efficient and secure operations. VLO 3 Develop a security architecture plan to incorporate both perimeter and endpoint security controls and devices to provide layers of security.
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 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 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 & Assessment Requirements:

A+ = 90-100%
A = 80-89%
B = 70-79%
C = 60-69%
D = 50-59%
F < 50%

Students are expected to be present to write all tests in class, unless otherwise specified. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning. Should the student fail to contact the professor, the student shall receive a grade of zero on the test.

If a student is not present 10 minutes after the test begins, the student will be considered absent and will not be given the privilege of writing the test.
Students exhibiting academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information.

In order to qualify to write a missed test, the student shall have:
a.) attended at least 75% of the classes to-date.
b.) provide the professor an acceptable explanation for his/her absence.
c.) be granted permission by the professor.

NOTE: The missed test that has met the above criteria will be an end-of-semester test.
Labs / assignments are due on the due-date indicated by the professor. Notice by the professor will be written on the labs / assignments and verbally announced in the class. Labs and assignments that are deemed late will have the following penalty: 1 day late - 10% reduction, 2 days late, 20% reduction, 3 days late, 30% reduction. After 3 days, no late assignments and labs will be accepted. It is the responsibility of the student who has missed a class to contact the professor immediately to obtain the lab / assignment. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical or near identical in content may constitute academic dishonesty and result in a zero grade.

Students are expected to be present to write in-classroom quizzes. There are no make-up options for missed in-class quizzes.

Students have the right to learn in an environment that is distraction-free, therefore, everyone is expected to arrive on-time in class. Should lectures become distracted due to students walking in late, the professor may deny entry until the 1st break period, which is 50 minutes into the class or until that component of the lecture is complete.

The total overall average of test scores combined must be 50% or higher in order to qualify to pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher.

Course Outcomes and Learning Objectives:

Course Outcome 1	**Learning Objectives for Course Outcome 1**
Introduction to Network Security Monitoring	• Understand the goal of Network Security Monitoring • Understand the concepts of Network Security Monitoring • Understand the importance of time • Know the seven data types

Course Outcome 2	**Learning Objectives for Course Outcome 2**
Enterprise Security Life Cycle	• Understand the four phases of the ESLC • Understand the sub-phases of the Detection and Response phases • Know how to apply the ESLC
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Collecting Network Traffic	• Learn about collecting network traffic via a NSM deployment case • Understand where collection mechanisms must be placed • Understand network data flow • Understand the concept of Network Address Translation • Understand the concept of IP Address Assignment • Understand the concept of Network Port Address Translation • Understand the methods of network traffic collection • Learn about the 9 Key Aspects of Operational Triage • Learn about what the Security Monitoring Requirements are for each key aspect of operational triage • Learn about a Defensible Network Architecture
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Operations & Building a Team	• Understand the Operational Trap • Learn about the NICE Framework and its categories and specialty areas • Learn about how to build out and organize cybersecurity • Understand what a Blue Team is • Understand the defensive technologies used at each security layer • Understand what a CIRT is
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Cybersecurity Threats	• Review the attack vectors • Learn about the CIA Triad • Learn about the Destruction Triad • Understand the objectives of malware attacks • Understand the delivery mechanisms for malware attacks • Understand general protection mechanisms that fight malware attacks • Learn about a variety of kinds of malware attacks and specific prevention measures that fight those attacks
Course Outcome 6	**Learning Objectives for Course Outcome 6**
Social Engineering	• Understand what Social Engineering is • Understand the motivations of a social engineer • Discover how social engineers gather information • Understand the psychological principles behind social engineering • Know what social engineers seek to exploit • Understand how to combat social engineering
Course Outcome 7	**Learning Objectives for Course Outcome 7**

	Deploy and Configure Cybersecurity Virtual Machine and Packet Analysis Tools	• Learn about VM capacity requirements • Deploy a Windows or Kali Linux VM • Install Wireshark • Configure Wireshark for practical labs • Install NetworkMiner • Explore Wireshark and NetworkMiner functionality • Explore CyberChef
	Course Outcome 8	**Learning Objectives for Course Outcome 8**
	Collaborative Hunting Exercise	• Participate in a professor-led interactive hunting exercise • Learn investigative techniques for researching a cyber incident • Learn how to write a cyber incident report
	Course Outcome 9	**Learning Objectives for Course Outcome 9**
	Threat Intelligence	• Understand what Threat Intelligence is • Understand the six phases of the Intelligence Cycle • Understand how Threat Intelligence relates to Security Operations • Understand the benefits of Threat Intelligence • Understand the Threat Intelligence frameworks
	Course Outcome 10	**Learning Objectives for Course Outcome 10**
	Physical Security	• Understand the planning that goes into secure facility design • Identify key assets that require protection • Understand the three kinds of controls • Learn how to protect the four kinds of key asset • Learn the functional order of security control • Learn about the two classifications of physical threat
	Course Outcome 11	**Learning Objectives for Course Outcome 11**
	Lab Work	Using case studies on topics such as malware infections and brute force attacks students will learn to: • Use tools like WireShark, and NetworkMinerto review PCAP files • Identify indicators of compromise • Identify compromised assets • Attribute compromised assets to users • Write an incident report detailing findings • Write IDS rules to help identify indicators of compromise
	Course Outcome 12	**Learning Objectives for Course Outcome 12**
	Intrusion Detection Systems and Intrusion Prevention Systems	• Understand what an IDS/IPS is, where it is deployed, and what they can do • Understand how an IDS/IPS functions • Learn about the four kinds of IDS/IPS • Learn about Snort • Understand the difference between a signature, vulnerability, and exploit • Understand the limitations of IDS
	Course Outcome 13	**Learning Objectives for Course Outcome 13**

Snort Rule Writing	• Learn the components of a snort rule • Learn how to write snort rules
Course Outcome 14	**Learning Objectives for Course Outcome 14**
Security Awareness Presentations (Group Assignment)	• Give an educational presentation on a cybersecurity topic focused on enhancing non-technical users understanding • Create an interactive exercise for the presentation • Create campaign materials for the cybersecurity topic and presentation • Create a plan for the delivery and implementation of the educational presentation and materials

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Coursework and Labs	40%
Group Assignment	30%
Practical Test	15%
Theory Test	15%

Date:

January 3, 2024

Addendum:

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