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:	2024-2025
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:	5
Total Hours:	70
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 advance, during class. Labs and assignments that are deemed late will have a 10% reduction per academic day to a maximum of 5 academic days at 50% (excluding weekends and holidays). Example: 1 day late - 10% reduction, 2 days late, 20%, up to 50%. After 5 academic days, no late assignments and labs will be accepted. If you are going to miss a lab / assignment deadline due to circumstances beyond your control and seek an extension of time beyond the due date, you must contact your professor in advance of the deadline with a legitimate reason that is acceptable. 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 can be up to 50 minutes after class starts 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
Explain and describe the concepts and purposes of Network Security Monitoring	1.1 Identify and explain the seven data types 1.2 Identify locations where data collection mechanisms must be placed on devices and in the network 1.3 Demonstrate network data flow techniques 1.4 Explain the concepts of Network Address Translation (NAT), ip address assignment and Network port addressing 1.5 Describe the methods of network traffic collection 1.6 Explain the 9 Key Aspects of Operational Triage
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Explore the Enterprise Security Life Cycle and Threat Intelligence	2.1 Explain the four phases of the ESLC 2.2 Identify the sub-phases of the Detection and Response phases 2.3 Explain the six phases of the Intelligence Cycle 2.4 Identify how Threat Intelligence relates to Security Operations 2.5 Explain the benefits of Threat Intelligence 2.6 Describe the Threat Intelligence frameworks
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Document Operations Team Building	3.1 Describe the NICE Framework and its categories and specialty areas 3.2 Identify the explain the steps to build out and organize cybersecurity 3.3 Describe what a Blue Team is 3.4 Identify the defensive technologies used at each security layer 3.5 Explain what a CIRT is
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Explain Physical Network Security	4.1 Document planning that goes into a secure facility design 4.2 Identify key assets that require protection 4.3 Identify the three kinds of controls 4.4 Explain protection methods for key assets 4.5 Prioritize the functional order of security control 4.6 Identify and explain the two classifications of physical threat
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Investigate Cybersecurity Threats	5.1 Identify, draw and explain the key components of the CIA Triad 5.2 Describe the Destruction Triad 5.3 Identify the objectives of malware attacks 5.4 Identify the motivations of a social engineer 5.5 Discover how social engineers gather information 5.6 Determine and explain psychological principles behind social engineering 5.7 Identify and explain methods to combat social engineering 5.8 Identify and explain the delivery mechanisms for malware attacks 5.9 Identify general protection mechanisms that fight malware attacks

	5.10 Investigate and research the variety and kinds of malware attacks including specific prevention measures that fight those attacks

Course Outcome 6	Learning Objectives for Course Outcome 6
Deploy, Configure and utilize Cybersecurity Virtual Machines for Network Security	6.1 Deploy a Windows or Kali Linux VM 6.2 Install and configure Wireshark for packet capturing of data 6.3 Install and utilize NetworkMiner for analyzing network traffic and identifying potential security threats or anomalies 6.4 Utilize CyberChef for analyzing, decoding, encoding, encrypting, and manipulating data in various formats 6.5 Identify and describe four kinds of IDS/IPS 6.6 Explain how IDS/IPS systems functions and their limitations 6.7 Identify the difference between a signature, vulnerability, and exploit 6.8 Utilize Snort for intrusion detection and intrusion prevention in real-time
Course Outcome 7	**Learning Objectives for Course Outcome 7**
Participate in a professor-led Collaborative Hunting Exercise	7.1 Apply investigative techniques for researching a cyber incident 7.2 Prepare a cyber incident report 7.3 Prepare Intrusion Detection System (IDS) rules to detect potentially malicious or anomalous activity within a network.
Course Outcome 8	**Learning Objectives for Course Outcome 8**
Create and deliver a presentation on Security Awareness (Group Assignment)	8.1 Deliver an educational presentation on a cybersecurity topic focused on enhancing non-technical users understanding 8.2 Create an interactive exercise for the presentation 8.3 Create campaign materials for the cybersecurity topic and presentation 8.4 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: October 24, 2024

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