COURSE OUTLINE: NASA104 - FUND OF NET SECURITY

Prepared: D. Kachur
Approved: Martha Irwin, Dean, Business and Information Technology

Course Code: Title	NASA104: FUNDAMENTALS OF NETWORK SECURITY
Program Number: Name	2196: NETWRK ARCH & SEC AN
Department:	COMPUTER STUDIES
Academic Year:	2024-2025
Course Description:	This course provides an in-depth study of network security principles, standards, cryptography, best practices and current threats. The learner will apply extensive hands-on work in establishing secure network platforms using both Windows and Linux on-premise and cloud-based solutions, then test them for system vulnerabilities using a variety of security tools and methods.
Total Credits:	4
Hours/Week:	4
Total Hours:	56
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
This course is a pre-requisite for:	NASA207
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 6 Design and implement a virtualization and cloud computing focused infrastructure specifically addressing security risks associated with incorporating virtualization into an organizations infrastructure. VLO 7 Deploy servers to host web applications, focusing on securing the server and web from identified security risks.
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 & 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.

Books and Required Resources:

CompTIA Security+ Study Guide by Mike Chapple, David Seidl
Publisher: Wiley-Sybex Edition: 9th
ISBN: 978-1-394-21141-8

Course Outcomes and Learning Objectives:

Course Outcome 1	**Learning Objectives for Course Outcome 1**
1. Explore the concepts of Network Security	1.1 Identify components that are part of Cyber/Network security 1.2 Define and research attack types including Phishing, Ransomware and Social Engineering 1.3 Examine the roles of those in the security industry to defend networks and devices 1.4 Research and analyze recent and current cyber security threats 1.5 Research Cyber Security job / career opportunities 1.6 Discuss 2 and 3 factor authentication options
Course Outcome 2	**Learning Objectives for Course Outcome 2**
2. Explore Firewalls	2.1 Discuss how Firewalls work and what they do 2.2 Discuss both software and hardware Firewalls 2.3 Create Firewall Rules 2.4 Test your Firewall 2.5 Discuss Firewall network policies 2.6 Monitor Firewall activity and logs
Course Outcome 3	**Learning Objectives for Course Outcome 3**
3. Setup a secure Windows Server Infrastructure	3.1 Examine, then diagram components and resources required in a LAN / WAN and Enterprise Network 3.2 Install a Windows Server as part of the Network Infrastructure process 3.3 Update the Windows Server with the latest patches 3.4 Examine Windows Defender 3.5 Secure, then Administer the Windows Server including Firewall 3.6 Test Windows Security including setting up Alert Monitoring 3.7 Review Network Security Policies and the the important role they play in helping keep the workplace safe from attacks 3.8 Explore Monitoring Security Protocols 3.9 Explore Log Files including end device and network logs
Course Outcome 4	**Learning Objectives for Course Outcome 4**
4. Explore Cryptography and its relation to Network	4.1 Explain cryptography and encryption 4.2 Explain asymmetric and symmetric

	Security	4.3 Analyze public and private Key infrastructure 4.4 Explain encryption algorithms
	Course Outcome 5	**Learning Objectives for Course Outcome 5**
	5. Apply Network Policies in a Windows Server Environment	5.1 Create an Organizational Unit (OU) 5.2 Apply Network Policy Server to the Organizational Unit 5.3 Explain and Apply Group Policy to the network 5.4 Test your OU and Group Policy security from a Windows client
	Course Outcome 6	**Learning Objectives for Course Outcome 6**
	6. Explore the Linux Operating System	6.1 Install a Linux OS 6.2 Perform hands-on administration and security of Linux 6.3 Work with the Linux Shell 6.4 Explore Linux security strengths and weaknesses 6.5 Apply Firewall rules in a Linux environment 6.6 Apply user, group, folder and file permissions in Linux 6.7 Apply then secure webpages on the Apache Web-Server
	Course Outcome 7	**Learning Objectives for Course Outcome 7**
	7. Monitor and Test Network Security	7.1 Use WireShark to analzye network traffic 7.2 Inject certificates into Network Monitoring to analyze encrypted connections 7.3 Analyze network bandwidth patterns 7.4 Create network bandwidth alerts 7.5 Review Security / Health Score Audit procedures 7.6 Discuss Network Security Insurance policies and purchase options
	Course Outcome 8	**Learning Objectives for Course Outcome 8**
	8. Explore Cloud Security	8.1 Identify major industry Cloud Service Providers 8.2 Identify tools used to monitor Cloud Server Security 8.3 Explore SAML in relation to Cloud Server authentication 8.4 Contrast RADIUS vs SAML 8.5 Analyze common customer configuration weaknesses for Cloud Networking

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Lab Assignments	40%
Test #1	30%
Test #2	30%

Date: June 16, 2024

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