COURSE OUTLINE: NASA207 - CAPSTONE PROJECT

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

Course Code: Title	NASA207: CAPSTONE PROJECT
Program Number: Name	2196: NETWRK ARCH & SEC AN
Department:	COMPUTER STUDIES
Academic Year:	2024-2025
Course Description:	The primary focus of the Capstone Project course is experiential learning through an applied project. This course integrates the knowledge and skills students have obtained throughout the Program. The learner will plan, design, configure, install, secure then test a complex Enterprise Network solution. The platform will incorporate a Domain with multiple domain controllers using multi-master replication and distributed file systems. A complete solution will include: DNS, Web, Mail, VPN and Database Servers. A disaster recovery plan will be assembled as part of supporting the network and data. Network penetration and testing procedures will be applied and Network defense monitoring solutions will be utilized and analyzed. The learner will prepare and submit documentation for the overall project.
Total Credits:	4
Hours/Week:	4
Total Hours:	56
Prerequisites:	NASA101, NASA102, NASA104
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 1 Design an enterprise network by applying knowledge of networking and routing protocols. 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. 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. VLO 8 Identify and plan IT services that support business goals and objectives, and explain specific activities directly related to the delivery and support of the services.
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%, 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**
1.) Plan and design the network model	1.1 Select a network theme for the capstone course 1.2 Research existing network scenario models and solutions 1.3 Prepare a list of key networking vendors and their products / services 1.4 Analyze and compare On-premise vs cloud-based solutions 1.5 Diagram the network model that includes key components 1.6 Assemble an asset procurement plan containing requirements to the network solution 1.7 Timeline the expected roll-out duration of the network implementation
Course Outcome 2	**Learning Objectives for Course Outcome 2**
2.) Install and configure key components of the network	2.1 Install the network operating system 2.2 Install update patches 2.3 Secure the network operating system 2.4 Configure router(s) and switch(es) (if necessary) 2.5 Add users and groups to meet the startup needs of the network 2.6 Create necessary data folders, then apply access control permissions 2.7 Create a multi-master-domain using 2 domain controllers 2.8 Install and configure distributed file systems and file replication services
Course Outcome 3	**Learning Objectives for Course Outcome 3**
3.) Install Server add-ons	3.1 Install and configure the IIS Web server 3.2 Install and configure a database server 3.3 Develop a web interface for Database access via the IIS web server front-end 3.4 Install and configure a VPN server and vpn client 3.5 Install and configure a mail server 3.6 Install and test a mail server client that integrates with the mail server

	3.7 Install and test various network monitoring tools, identify one of choice, then set it as your standard.
Course Outcome 4	**Learning Objectives for Course Outcome 4**
4.) Safeguard the network and data	4.1 Create a disaster recovery plan in the event of network intrusion and / or failure 4.2 Implement fault-tolerant procedures allowing for redundancy support 4.3 Setup network monitoring of the server(s) and traffic 4.4 Maintain daily update procedures and patches to the network and devices 4.5 Create a test a daily backup 4.6 Demonstrate the ability to restore data from backups 4.7 Prepare a `what-if` plan to execute in the event of a cyber security breach
Course Outcome 5	**Learning Objectives for Course Outcome 5**
5.) Test the network security	5.1 Attempt brute-force password logins 5.2 Scan network ports for weaknesses 5.3 Attempt to penetrate open shares 5.4 Test web server vulnerabilities 5.5 Prepare and launch phishing attempts on user accounts 5.6 Utilize packet-sniffing software
Course Outcome 6	**Learning Objectives for Course Outcome 6**
6.) Prepare final documents and presentation	6.1 Assemble documentation of the overall project, then submit for evaluation 6.2 Prepare and maintain documentation of network procedures for network engineers / administrators 6.3 Prepare and present a PowerPoint presentation to your professor and classmates

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
1.) Term Test	30%
2.) Overall Project	50%
3.) Project Documentation	10%
4.) Final Presentation	10%

Date: June 16, 2024

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