COURSE OUTLINE: NASA204 - VIRTUAL PRIVATE NET

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

Course Code: Title	NASA204: VIRTUAL PRIVATE NETWORKS
Program Number: Name	2196: NETWRK ARCH & SEC AN
Department:	COMPUTER STUDIES
Academic Year:	2023-2024
Course Description:	This course will examine the use of virtual private network (VPN) technologies to provide secure communications and configuration for client-to-site and site-to-site VPN solutions. The learner will apply hands-on activities using various vpn protocols and methods in establishing and testing their secure vpn connections. Security policies and rules will be planned then implemented on the VPN networks.
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.
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 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%, 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	**Course Outcome 1** | **Learning Objectives for Course Outcome 1**

Learning Objectives:		
	1. Explore the fundamentals of Virtual Private Networks (VPNs)	1.1 Describe the purpose of a Virtual Private Network 1.2 Explain the benefits of deploying a VPN 1.3 Explain the relationship between encryption and VPNs 1.4 Identify and contrast VPN types
	Course Outcome 2	**Learning Objectives for Course Outcome 2**
	2. Explore VPN Technologies	2.1 Examine differences between software and hardware solutions 2.2 Explain then contrast software vs. hardware VPNs 2.3 Review differences between Layer 2 and Layer 3 VPNs 2.4 Explain Internet Protocol Security (IPSec) 2.5 Examine Layer 2 Tunneling Protocol (L2TP) 2.6 Examine PEAP protocol 2.7 Examine than explain Certificate Server VPNs
	Course Outcome 3	**Learning Objectives for Course Outcome 3**
	3. Examine VPN Management Best Practices	3.1 Develop a VPN policy 3.2 Develop a VPN deployment plan 3.3 Discuss VPN threats and exploits 3.4 Examine commercial and open-source VPNs 3.5 Review differences between personal and enterprise VPNs
	Course Outcome 4	**Learning Objectives for Course Outcome 4**
	4. Explore Real World VPN Scenarios	4.1 Examine operating system-based VPNs 4.2 Examine VPN appliances 4.3 Discuss choosing between IPSec and SSL remote access VPNs 4.4 Review DMZ, Extranet, and Intranet VPN solutions
	Course Outcome 5	**Learning Objectives for Course Outcome 5**
	5. Configure a VPN Server	5.1 Install a VPN Server in a Windows Server environment 5.2 Install and configure Routing and Remote Access in a Windows Server 5.3 Install and configure Network Policy Server in a Windows Server for VPN usage 5.4 Configure RADIUS Server for VPN usage 5.5 Install and configure a Certificate Server 5.6 Configure then test a VPN client for your VPN Server 5.7 Troubleshoot VPN connection issues 5.8 Analyze the role of Federation Services within a VPN concept 5.9 Diagram and Configure a Site-to-Site VPN solution
	Course Outcome 6	**Learning Objectives for Course Outcome 6**
	6. Apply various VPN Client Security Types	6.1 configure and test a PPTP vpn connection 6.2 configure and test a L2TP vpn connection 6.3 configure and test a peap vpn connection 6.4 configure and test a ssl/tls certificate vpn connection
	Course Outcome 7	**Learning Objectives for Course Outcome 7**
	7. Explore Cloud-Based VPNs	7.1 Identify key vendors that provide cloud-based VPN solutions

	7.2 Explore Cisco Meraki VPN configurations including online demonstration 7.3 Diagram and explain a Microsoft Azure VPN setup

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Lab Assignments	40%
Quizzes	10%
Test #1	25%
Test #2	25%

Date: January 4, 2024

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