INSTRUCTIONAL OFFERING: **COMMUNICATION NETWORKS IV**

INSTRUCTIONAL PROGRAM: **BTECH: COMMUNICATION NETWORKS**

EXAMINATION: **Continuous assessment**

5. SILLABUS

- Security

UNIT	SPECIFIC OUTCOME	ASSESSMENT CRITERIA	CREDITS	NOTIONAL HOURS	WEEKS
1	Demonstrate the understand of Researching Network Attacks and Security Audit Tools	Describe the evolution of network security. Describe the drivers for network security. Describe the major network security organizations. Describe the domains of network security. Describe network security policies. Describe viruses, worms, and Trojan Horses. Describe how to mitigate threats from viruses, worms, and Trojan Horses. Describe how network attacks are categorized. Describe reconnaissance attacks. Describe access attacks. Describe Denial of Service attacks. Describe how to mitigate network attacks.	1	6	1
2	Demonstrate an understanding of the Securing of the Router for Administrative	Secure the physical installation of and the administrative access to Cisco routers based on different network	1	6	1

	Access		requirements using the CLI and CCP. Configure administrative roles using privilege levels and role-based CLI. Implement the management and reporting features of syslog, SNMP, SSH, and NTP. Examine router configurations with the Security Audit feature of CCP, and make the router and network more secure by using the auto secure command or the One-Step Lockdown feature of CCP.			
3	Demonstrate the ability to Secure Administrative Access Using AAA and RADIUS		Explain the function and operation of the authentication, authorization, and accounting (AAA) protocol. Configure a Cisco router to perform AAA authentication with a local database. Describe how to configure Cisco ACS to support AAA for Cisco IOS routers. Configure server-based AAA.	2	8	1
4	Demonstrate the ability to Configure CBAC and Zone-Based Firewalls along with IP ACLs		Describe numbered and named, standard and extended IP ACLs. Configure IP ACLs with IOS CLI and CCP. Describe TCP established ACL functionality. Configure ACLs with TCP established. Describe and configure reflexive ACLs. Describe and configure dynamic ACLs. Describe and configure time-based ACLs. Describe attack mitigation with ACLs. Describe the major types of firewalls. Describe and configure CBAC (IOS Stateful Packet Inspection) with CLI. Describe and configure Zone-Based Policy Firewall with CLI and CCP.	2	8	1
5	Demonstrate the ability to configure an Intrusion Prevention System		Describe the underlying IDS and IPS technology that is embedded in the Cisco host- and network-based IDS and IPS solutions. Configure Cisco IOS IPS	2	8	1

			using CLI and CCP. Verify Cisco IOS IPS using CLI and CCP.			
6	Demonstrate the ability to apply Layer 2 Security		Describe endpoint vulnerabilities and protection methods. Describe the vulnerabilities of the Layer 2 infrastructure. Describe the mitigation techniques for securing the Layer 2 infrastructure. Describe MAC address spoofing attacks, STP manipulation attacks, MAC address overflow attacks, LAN storm attacks, and VLAN attacks. Configure and verify port security, BPDU guard, root guard, storm control, and PVLAN Edge. Describe endpoint security with IronPort. Describe endpoint security with Network Admission Control. Describe wireless, VoIP, and SAN security considerations. Describe wireless, VoIP, and SAN security solutions.	1	6	1
7	Demonstrate the ability to understand the Principles of Cryptology		Explain how cryptology consists of cryptography (encoding messages) and cryptanalysis (decoding messages) and how these concepts apply to modern day cryptography. Explain how securing communications by various cryptographic methods, including encryption, hashing and digital signatures, ensures confidentiality, integrity, authentication and non-repudiation. Describe the use and purpose of hashes and digital signatures in providing authentication and integrity. Explain how authentication is ensured. Explain how integrity is ensured. Explain how data confidentiality is ensured using symmetric encryption algorithms and pre-shared keys.	2	8	1

			Explain how data confidentiality is ensured using asymmetric algorithms in a public key infrastructure to provide and guarantee digital certificates.			
8	Demonstrate the ability to Configure VPNs		Describe the purpose and types of VPNs and define where to use VPNs in a network. Describe how to configure a GRE VPN tunnel. Describe the fundamental concepts and technologies of VPNs, and terms that IPsec VPNs use. Describe how to configure a site-to-site IPsec VPN. Configure a site-to-site IPsec VPN with PSK authentication using CLI and Cisco CCP. Describe the two common remote network access methods used in enterprise networks. Describe how the Cisco VPN Client is used in an IPsec remote-access VPN. Describe how Secure Socket Layer (SSL) is used in a remote-access VPN. Configure a remote-access IPsec VPN using CLI and Cisco CCP.	2	8	1
9	Demonstrate the ability to understand how to Mitigate network attacks		Describe the principles of secure network design. Describe threat identification and risk analysis. Describe risk management and risk avoidance. Describe the Cisco SecureX architecture. Describe operations security. Describe network security testing tools and techniques. Describe business continuity and disaster recovery. Describe the system development life cycle concept and its application to a secure network life cycle. Describe the purpose and function of a network security policy.	1	6	1
10	Demonstrate the		Explain how the ASA is	1	6	1

	ability to use an ASA firewall solution		an advanced stateful firewall. Describe types of firewalls. Describe the default configuration of an ASA 5505. Implement an ASA firewall configuration. Configure an ASA to provide basic firewall services using ASDM. Explain and configure access lists and object groups on an ASA. Configure an ASA to provide NAT services. Configure access control using the local database and AAA server. Describe the configuration of Modular Policy Framework (MPF) on an ASA. Implement an AnyConnect SSL VPN and a clientless SSL VPN on an ASA.			