

	Department/program: Networking	Course Code: CPT 224		Contact Hours: 96
	Subject/Course WEB Access & Network Security:			Theoretical: 2 Hours/week
	Year Two Semester: Two	Pre-requisite:	NET304	Practical: 4 Hours/week
<p>General Objectives:</p> <ol style="list-style-type: none"> 1- Explain the need for network security. 2- Identify the various elements of an effective security policy. 3- Describe encryption and identify the main encryption methods used in internetworking. 4- To apply security principles, and identify a security attack. 5- Describe the principles for effective network security, and give guidelines to create affective specific solution 6- To understand security issues with communication protocols 7- Identify firewall types and common firewall terminology. 8- Plan a firewall system that incorporates several levels of protection. 9- Deploy a network firewall. 10- To Respond appropriately to a security breach, and to Identify security organizations that can help you in case your system is attacked 				

Theoretical Content			Practical Content			
Objectives: 1) Explain the need for network security.						
Week /s	Specific Learning Outcome	Teachers Activities	Resources	Specific Learning Outcome	Teachers Act ivies	Resources
1	<p>TO understand:</p> <p>Security concepts and standards.</p> <p>Network Security Background.</p> <p>Different types of Security?</p>	<p>To Explains :</p> <p>Security concepts and standards</p> <p>The need for network security</p> <ul style="list-style-type: none"> - Identify resources that need security. - Identify the two general security threat types. - List security standards and organization. <p>Hacker Statistics.</p> <p>What is the Risk?</p> <p>Security Services.</p> <p>Security Mechanisms</p> <p>Additional Security Standards</p> <p>The Myth of 100-Percent Security.</p> <p>Attributes of an Effective Security Matrix.</p> <p>Know what you are trying to Protect.</p> <p>Who is the Threat?</p>	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board</p>	<p>Ability to:</p> <ul style="list-style-type: none"> - View and modify the default access control settings in Windows. - Create an access control list for a Server. - View the effects of hostile JavaScript in Netscape Navigator - Configure execution control lists in Windows. - Creating an Execution Control list for the SU command in Linux 	<ul style="list-style-type: none"> - To explain how to modify access control settings in Windows environment loaded with default values. - Show the student how to create an access control list for apache Server; and Viewing the effects of hostile JavaScript in Netscape Navigator - Explaining how to configure execution control lists in Windows. - Creating an Execution Control list for the SU command in Linux 	<p>A networked Computer Laboratory loaded with an appropriate network operating system.</p>
e: - 2) Identify the various elements of an effective security policy.						

Week/s	Specific Learning Outcome	Teachers Activities	Resources	Specific Learning Outcome	Teachers Act ivies	Resources
2	<p>To understand:</p> <p>Security Concepts and Mechanisms.</p> <p>Identification & authentication</p> <p>Understand Access Control</p> <p>Auditing</p>	<p>To explain:-</p> <p>Elements of Security. The Security Policy. What encryption does? Encryption techniques. Encryption Categories. Encryption strength</p> <p>Authentication Methods. Specific authentication Techniques.</p> <p>Access Control List (ACL) Execution Control List (ECL)</p> <p>The concept of auditing. Active Auditing Passive auditing</p>	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board.</p>	<p>To implement:</p> <p>Security concept.</p> <p>Authentication methods</p> <p>Effective access control</p>	<p>Set appropriate lab work to address:</p> <p>Security concept, authentication methods, and access control.</p> <p>Help students in their practical work.</p>	<p>A networked Computer Laboratory loaded with an appropriate network operating system.</p>
Objectives: 3) Describe encryption and identify the main encryption methods used in internetworking.						
Week /s	Specific Learning Outcome	Teachers Activities	Resources	Specific Learning Outcome	Teachers Act ivies	Resources
3	<p>To understand:</p> <p>The Encryption concepts</p> <p>Symmetric-key Encryption</p>	<p>To explain:</p> <p>The meaning of encryption.</p> <p>Reasons to Use Encryption</p> <p>Know the method to create trust Relationships.</p> <p>Rounds, Parallelization and Strong Encryption. Symmetric Algorithms Symmetric algorithms created by the RSA Security Corporation.</p>	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board</p>	<ul style="list-style-type: none"> - Reviewing symmetric encryption algorithms. - Using MD5sum to create checksums in Red Hat Linux. - Installing PGP in windows 2000. - Generating a key pair using PGP for windows 2000. - Exporting and signing public keys using PGP for windows 2000. - Exchanging encrypted messages using PGP for windows 2000. 	<ul style="list-style-type: none"> - Explaining how to encrypt a file using Rijndael encryption algorithm. - Show how to use the MD5 utility and to verify if changes have been made to sensitive files and directories. - Explain how installing PGP, and generating a key pair using PGP. - Explain how trusting 	<p>A networked Computer Laboratory loaded with an appropriate network operating system.</p>

	<p>Hash Encryption</p> <p>Applied Encryption Processes</p>	<p>Hash algorithms Secure Hash Algorithm</p> <p>Encryption Drives Secure Sockets Layer and Secure HTTP.</p> <p>Create a trust relationship using public-key cryptography.</p> <p>A list of specific forms of symmetric, asymmetric and hash encryption.</p> <p>Public-key encryption in windows 2000 and Linux.</p>		<ul style="list-style-type: none"> - Encrypting files with PGP in windows 2000. - Generating a key pair using gpg for Red Hat Linux. - Exchanging and signing public keys in Linux. - Encrypting and decrypting files using gpg. - Creating a signature file. - Signing files with gpg. - Creating a key distribution center. 	<p>relationship established using asymmetric-key encryption.</p> <ul style="list-style-type: none"> - Explaining how using PGP and outlook to send encrypted e-mail, and how to use PGP to encrypt file. - Explain how implement public-key cryptography using the GPG including with Red Hat Linux. - Describe how exchange public-key with other computer, and how using PGP to encrypt a file to another public key computer. - Explain how to create a signature file, then give it to your partner. You will then sign a document. - The partner will then use your signature file to verify the document. - Explain how export pgp signatures to your instructor's computer using FTP. Your instructor's computer will become a key distribution center. 	
<p>Objectives:- 4) To apply security principles, and identify a security attack.</p>						
<p>Week</p>	<p>Specific Learning Outcome</p>	<p>Teachers Activities</p>	<p>Resources</p>	<p>Specific Learning Outcome</p>	<p>Teachers Act ivies</p>	<p>Resources</p>
	<p>To recognize:</p>	<p>To describe specific types of</p>		<ul style="list-style-type: none"> - Using web Cracker in Linux 	<ul style="list-style-type: none"> - In this exercise student 	<p>A networked</p>

4	<p>Different types of attacks</p> <p>Attacks categories.</p> <p>A Brute-Force and Dictionary Attacks.</p> <p>System Bugs and Back Doors.</p> <p>Social Engineering and Non-direct Attacks.</p>	<p>security attacks.</p> <p>To explain how to recognize specific attack incidents.</p> <p>To explain Dictionary base attack.</p> <p>To highlight and state possible system Bugs such as Buffer Overflow</p> <p>Common buffer overflow attacks</p> <p>To explain how social engineering and non-direct attacks function.</p>	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board</p>	<p>and Windows 2000.</p> <ul style="list-style-type: none"> - Examining a buffer overflow attack. - Sending fake E-mail. - Installing Tribe Flood network 2000. - Analyzing an attack in progress. 	<p>will work with a partner together to identify the steps necessary to wage a dictionary attack.</p> <ul style="list-style-type: none"> - Explain how to compile code onto a Linux system. This code exploits default installations of windows 2000. - Explain how sending fake E-mail to your partner. - Describe how to install TFN2K on Linux system. - Explain how to analyze a UDP DOS attack as it occurs. 	<p>Computer Laboratory loaded with an appropriate network operating system.</p>
<p>Objectives: 5) To describe the principles for effective network security, and give guidelines to create an effective and specific solution.</p>						
Week	Specific Learning Outcome	Teachers Activities	Resources	Specific Learning Outcome	Teachers Act ivies	Resources
5	<ul style="list-style-type: none"> • Understand Common Security Principles. • Use an integrated Security strategy. • Identify Security Business Issues. • Consider Physical Security • Know Protocol Layers and Security. 	<ul style="list-style-type: none"> - Describe the universal guidelines and principles for effective network security. - Use universal guidelines to create effective specific solutions. 	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board</p>	<ul style="list-style-type: none"> - Exploiting and protecting Red Hat Linux single-boot mode. - Conducting a physical attack against a Windows 2000 Server 	<ul style="list-style-type: none"> - Explain conducting a physical attack against Red Hat Linux. - Demonstrating how to use the freeware windows NT change password utility to gain administrative access to a windows 2000 server. 	<p>A networked Computer Laboratory loaded with an appropriate network operating system.</p>
6	<ul style="list-style-type: none"> • Introduction TCP/IP Security • Understand TCP/IP and Network Security. • Understand the TCP/IP Suite and the OSI Reference Model. 	<ul style="list-style-type: none"> - Describe the list of protocols that pass through a firewall. - Identify potential threats at different layers of the TCP/IP stack. 	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p>	<ul style="list-style-type: none"> - Enabling TCP/IP filtering on Windows 2000. - Using a port listener on Windows 2000 to conduct a trace back. 	<ul style="list-style-type: none"> - Show the student how to configure windows 2000 so that it will not accept connections on ports student specifies. 	<p>A networked Computer Laboratory loaded with an appropriate</p>

COMPUTER NETWORKING: FOURTH TERM

	<ul style="list-style-type: none"> Understand the <ul style="list-style-type: none"> Physical Layer Network Layer Transport Layer Application Layer 		<p>Online lecture notes for the course.</p> <p>White board</p>		<ul style="list-style-type: none"> Describe how to use a simple port listener to determine the nature of the connections to your system. Student will work with a partner. 	network operating system.
Objectives: 6) To understand security issues with communication protocols.						
Week	Specific Learning Outcome	Teachers Activities	Resources	Specific Learning Outcome	Teachers Act ivies	Resources
7	<ul style="list-style-type: none"> Know what Securing Resources is. Know TCP/IP Security Vulnerabilities. How implementing Security Resources and Services. <ul style="list-style-type: none"> Protecting services. Protect against profiling. Coordinate methods and techniques. Protect services by changing default settings. Remove unnecessary services Protecting TCP/IP Services. <ul style="list-style-type: none"> Specialized accounts. The Web server. Securing IIS. Securing file Transfer Protocol (FTP) servers. 	<ul style="list-style-type: none"> Explaining consistently apply security principles. Describe secure TCP/IP services, including HTTP and FTP. Describe the importance of testing and evaluating systems and services. 	<p>Document and whiteboard</p> <p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White boar</p>	<ul style="list-style-type: none"> Executing arbitrary code in Apache Server. Securing a Windows 2000 Web server. Securing the FTP service. 	<ul style="list-style-type: none"> Explain how to manipulate a flawed CGI script into revealing sensitive information about its host. Describe how change some of the system defaults in IIS. 	A networked Computer Laboratory loaded with an appropriate network operating system.
8	<ul style="list-style-type: none"> Simple Mail Transfer Protocol (SMTP) <ul style="list-style-type: none"> The Internet worm. The Melissa virus E-mail and virus scanning Network-level e-mail scanning Access control measures. Testing and Evaluating <ul style="list-style-type: none"> Testing existing systems Implementing New Systems and Settings. Security Testing Software 	<ul style="list-style-type: none"> Discuss network security management applications, including network scanners, operating system add-ons and log analysis. 	<p>Document and whiteboard</p> <p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board</p>	<ul style="list-style-type: none"> Deploying simple network scanners. Scanning systems using Red Hat Linux. 	<ul style="list-style-type: none"> Explain how to alter the default settings for your DTP server. Describe how deploy a simple network scanner in windows 2000. Describe how using Red Hat Linux to scan systems. 	A networked Computer Laboratory loaded with an appropriate network operating system.

Objectives: 7) Identify firewall types and common firewall terminology.						
Week	Specific Learning Outcome	Teachers Activities	Resources	Specific Learning Outcome	Teachers Act ivies	Resources
9	<ul style="list-style-type: none"> • Know firewalls and Virtual Private Networks. • Introduction to Access Control. • Definition and description of a firewall. • Role of firewall. <ul style="list-style-type: none"> - Implement a company's security policy. - Create a choke point. - Log Internet activity. • Understanding Firewall Terminology <ul style="list-style-type: none"> - Packet Filter. - Proxy Server - Network Address Translation. - NAT considerations. - NAT and vendor terminology. - Bastion host. - Operating system hardening - Securing and choke routers - Demilitarized Zone (DMZ) • Know Firewall Configuration Defaults. • How creating Packet Filter Rules. • Advantages and disadvantages of Packet Filter. • Know how configuring proxy Servers. <ul style="list-style-type: none"> - Recommending a proxy-oriented firewall. - Features and Advantages of Proxy server. 	<ul style="list-style-type: none"> - Describe the role a firewall plays in a company's security policy. - Define common firewall terms. - Describe packet-filtering rules. - Describe circuit-level gateways and their features. 	<ul style="list-style-type: none"> PC connected to an OHP. Power point representation of lecture notes Online lecture notes for the course. White board 	<ul style="list-style-type: none"> - Installing WinRoute in Windows 2000. - configuring packet filtering rules. - Using the ipchains command to create a personal firewall in Linux. 	<ul style="list-style-type: none"> - In this exercise all student and the teacher will install WinRoute onto their systems. The teacher will install WinRoute onto the windows 2000 system acting as a multihomed router. - Explain how to use WinRoute to restrict access to ICMP packets and certain TCP and UDP port. 	<ul style="list-style-type: none"> A networked Computer Laboratory loaded with an appropriate network operating system.
10	<ul style="list-style-type: none"> • Understanding Remote Access and Virtual Private Networks (VPNs) <ul style="list-style-type: none"> - Internet Protocol Security (IPSec) - Security associations (SA) and Internet Key Exchange 	<ul style="list-style-type: none"> -Configure an application-level gateway. -Explain Public Key Infrastructure (PKI) 	<ul style="list-style-type: none"> PC connected to an OHP. Power point representation of lecture notes 	<ul style="list-style-type: none"> - Using the iptables command to create a personal firewall in Linux. - Configuring a proxy server in Windows 2000. 	<ul style="list-style-type: none"> - Explain how to use the ipchains command to create packet-filtering rules for the system, and how to use iptables command to create 	<ul style="list-style-type: none"> A networked Computer Laboratory loaded with an appropriate network

	<ul style="list-style-type: none"> (IKE). - The Point-To-Point Tunneling Protocol (PPTP). - The layer 2 Tunneling Protocol (L2TP). • Public Key Infrastructure (PKI) <ul style="list-style-type: none"> - PKI standards. - PKI terminology • Certificates. 	<ul style="list-style-type: none"> - Discuss the importance of public keys in regards to a Virtual Private network (VPN). - Explain the importance of IPSec in regards to IPv4. 	<p>Online lecture notes for the course.</p> <p>White board</p>		<ul style="list-style-type: none"> packet-filtering rules for the system. - Describe how to configure WinRoute as a proxy server. - 	<p>operating system.</p>
<p>Objectives: 8) Plan a firewall system that incorporates several levels of protection.</p>						
Week	Specific Learning Outcome	Teachers Activities	Resources	Specific Learning Outcome	Teachers Act ivies	Resources
11	<ul style="list-style-type: none"> • Introducing Levels of Firewall Protection. • Know basic Firewall Concepts. • Firewall strategies and goals. • Building a Firewall. <ul style="list-style-type: none"> - Design Principles. • Types of bastion Hosts <ul style="list-style-type: none"> - Single-homed Bastion host - Multi-homed Bastion host - Single-purpose Bastion host - Internal Bastion host • Hardware Issues • Operating system • Services and daemons - 	<ul style="list-style-type: none"> - Describe how to plan a firewall system that incorporates several levels of protection. - Describe all types of firewall system design and their degrees of security - 	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board</p>	<ul style="list-style-type: none"> • All those Labs should led by teacher - Creating an internal network with WinRoute. - Establishing a packet filter. 	<ul style="list-style-type: none"> - Explain how to connect to the WinRoute service running on a host, then configure the service to create an internal and external network. - Describe how to use WinRoute to create a packet filter to forbid ICMP from being passed from one network to another. - 	<p>A networked Computer Laboratory loaded with an appropriate network operating system.</p>
12	<ul style="list-style-type: none"> • Understanding Common Firewall Design <ul style="list-style-type: none"> - Screening routers - Screened host firewall (single-homed bastion) - Screened host firewall (dual-homed bastion) - Screened subnet firewall (demilitarized zone) 	<ul style="list-style-type: none"> - Implement a packet-filtering firewall. - - 	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board</p>	<ul style="list-style-type: none"> - Denying HTTP access. - Configuring an FTP packet-filtering rule for a specific host. • 	<ul style="list-style-type: none"> - Teacher will create a rule that denies external Web access for all hosts. - Teacher will create a rule that disables access for a specific host. 	<p>A networked Computer Laboratory loaded with an appropriate network operating system.</p>
13	<ul style="list-style-type: none"> • Putting It All Together • Detecting and Distracting Hackers. • Understand Proactive Detection. 	<ul style="list-style-type: none"> - Explain how to customize a network to manage hacker activity. - 	<p>PC connected to an OHP.</p> <p>Power point</p>	<ul style="list-style-type: none"> - Filtering zone transfers. - Hardening the firewall operating system. 	<ul style="list-style-type: none"> - Explain how investigate common packet-filtering issues. - Explain how to create a 	<p>A networked Computer Laboratory loaded with</p>

	<ul style="list-style-type: none"> - Automated security scans. - Login scripts. - Automated audit analysis - Checksum analysis. • Understand how Distracting the Hacker. <ul style="list-style-type: none"> - Dummy accounts. - Dummy files - Dummy Password files • Know security tools <ul style="list-style-type: none"> - Tripwires and automated checksums. - Tripwire concerns - Jails • Understand how punishing the Hacker. <ul style="list-style-type: none"> - Know the Methods <ul style="list-style-type: none"> - Log traffic and send e-mail messages. - Conduct reverse scans. - Drop the connection. - Know the tool <ul style="list-style-type: none"> - Sniffers - Personal firewalls - Route - ipchains/iptables - Portsentry - Port Scan Attack detector (PSAD) - Firedaemon • Understand what Problems with Retaliation. 	<ul style="list-style-type: none"> - Explain how to Implement proactive detection. - Describe how distract hackers and contain their activity and how to set traps. 	<p>representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board</p>	<ul style="list-style-type: none"> - Setting a logon tripwire script in Windows 2000. - Using tripwire for Linux. • 	<p>tripwire for the administrator account that alerts a designated host every time an interactive logon occurs.</p> <p>Explain how to install and deploy the tripwire program in Linux.</p>	<p>an appropriate network operating system.</p>
--	--	---	---	--	---	---

Objectives: 9) To Respond appropriately to a security breach, and to Identify security organizations that can help you in case your system is attacked.

Week	Specific Learning Outcome	Teachers Activities	Resources	Specific Learning Outcome	Teachers Act ivies	Resources
14	<ul style="list-style-type: none"> • Understanding Incident Response. • Know how planning for response. • Create a Response Policy. <ul style="list-style-type: none"> - Determining the accounts affected. - Identifying which files 	<ul style="list-style-type: none"> - Explain the respond appropriately to a security breach. - - - Subscribe to respected security alerting 	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture</p>	<ul style="list-style-type: none"> - Subscribing to security mailing lists. 	<ul style="list-style-type: none"> - Explain how to subscribe to respected security mailing lists. 	<p>A networked Computer Laboratory loaded with an appropriate network operating</p>

	<p>have been read, altered, or substituted.</p> <ul style="list-style-type: none"> - Tracing the hacker's activities in the system. - Consulting audit logs. - Determining if any permission have been reset. <p>-</p>	<p>organizations.</p>	<p>notes for the course.</p> <p>White board</p>			<p>system.</p>
15	<ul style="list-style-type: none"> • Decide Ahead of Time. • Document Everything • Assess the Situation. <ul style="list-style-type: none"> - Determine the scope of the breach • Know Execute the Response Plan. <ul style="list-style-type: none"> - Notify affected individuals. - Notify the service provider. - Notify Internet agencies 	<ul style="list-style-type: none"> - Identify some of the security organizations that can help the student in case the system is attacked. - 	<p>PC connected to an OHP.</p> <p>Power point representation of lecture notes</p> <p>Online lecture notes for the course.</p> <p>White board</p>	<ul style="list-style-type: none"> - Subscribing to security mailing lists. - 	<ul style="list-style-type: none"> - Explain how to subscribe to respected security mailing lists. 	<p>A networked Computer Laboratory loaded with an appropriate network operating system.</p>