Subject: Advance Network Security								
Program: M.Sc. in CyberSecurity				**Subject Code:**			**Semester: II**	
Teaching Scheme				**Examination Evaluation Scheme**				
Lecture	**Tutorial**	**Practical**	**Credits**	**University Theory Examination**	**University Practical Examination**	**Continuous Internal Evaluation (CIE)-Theory**	**Continuous Internal Evaluation (CIE)-Practical**	**Total**
3	**0**	**2**	**4**	**40**	**40**	**60**	**60**	**200**

COURSE OBJECTIVES:

1. Explain the objectives of information security
2. Explain the importance and application of each of confidentiality, integrity, authentication and
3. availability
4. Understand various cryptographic algorithms.
5. Understand the basic categories of threats to computers and networks
6. Describe public-key cryptosystem.
7. Describe the enhancements made to IPv4 by IPSec
8. Understand Intrusions and intrusion detection
9. Discuss the fundamental ideas of public-key cryptography.
10. Generate and distribute a PGP key pair and use the PGP package to send an encrypted email message.
11. Discuss Web security and Firewalls

Content

Course Content

W - Weightage (%) , **T -** Teaching hours

Sr.	**Topics**	**W**	**T**
1	**UNIT 1 – Introduction to Network Security** What is network security? The importance of network security Common network security threats The role of network security in modern computing **Network Security Fundamentals:** CIA triad (Confidentiality, Integrity, Availability) Security policies and procedures Risk assessment and management	**20**	**10**
2	**UNIT 2-Network Protocols for Authentication:** RADIUS (Remote Authentication Dial-In User Service) TACACS+ (Terminal Access Controller Access Control System Plus) LDAP (Lightweight Directory Access Protocol) Kerberos OAuth and OpenID Connect **Secure Authentication Protocols:** Secure Socket Layer/Transport Layer Security (SSL/TLS)	**20**	**9**

	Secure Shell (SSH) for remote access Extensible Authentication Protocol (EAP) OAuth 2.0 and OpenID Connect Security Assertion Markup Language (SAML)		
3	**UNIT – 3 Public Key Cryptography** Need and Principles of Public Key Cryptosystems RSA Algorithm Key Distribution and Management Diffie-Hellman Key Exchange Digital Signatures	**20**	**7**
4	**UNIT-4 Network Perimeter Security:** Firewalls and their types (e.g., stateful, stateless) Intrusion Detection and Prevention Systems (IDS/IPS) Demilitarized Zones (DMZ) Network segmentation and isolation Virtual Private Networks (VPNs)	**20**	**7**

TEXT BOOKS:

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition
2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition

REFERENCE BOOKS:

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
2. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition
3. Information Security, Principles, and Practice: Mark Stamp, Wiley India.
4. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH
5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning
6. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning

Video Lectures

1. http://nptel.ac.in/courses/106105031/lecture by Dr. Debdeep MukhopadhyayIIT Kharagpur
2. https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-033-computer-system-engineering-spring-2009/video-lectures/ lecture by Prof. Robert Morris and Prof. Samuel Madden MIT.

List of Practical’s:

1. Learn to use commands like tcpdump, netstat, ifconfig, nslookup and traceroute. Capture ping
2. and trace route PDUs using a network protocol analyzer and examine.
3. Write a HTTP web client program to download a web page using TCP sockets.
4. Applications using TCP sockets like: a) Echo client and echo server b) Chat
5. Simulation of DNS using UDP sockets.
6. Use a tool like Wireshark to capture packets and examine the packets
7. Implement Caesar Cipher Encryption-Decryption in Python
8. Implement Playfair Cipher Encryption-Decryption on paper
9. Implement Polyalphabetic cipher (rolling cipher) Encryption-Decryption in Python
10. Implement Atbash Cipher Encryption-Decryption in Python
11. Implement RSA Encryption-Decryption in Python
12. Implement RSA Encryption-Decryption on Paper
13. Perform Diffie Helmen Key exchange on Paper
14. Write a program to generate SHA-1 Hash