DISCIPLINE SPECIFIC ELECTIVE COURSE: Network Security

Credit distribution, Eligibility and Pre-requisites of the Course

Course title & Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course (if any)
		Lecture	Tutorial	Practical/ Practice		
Network Security		**3**	**1**	**0**	Pass in Class XII	DSC 04 Object Oriented Programming with C++/ GE 1a Programming using C++ / GE1b Programming with Python/ DSC 01 Programming using Python/ GE 3b: Java Programming

Learning Objectives

This course will provide students with an understanding of the fundamental concepts, principles, and techniques of network security. Students will learn how to assess, design, and implement secure networks using various tools and technologies.

Learning outcomes

On successful completion of the course, students will be able to:

- Describe the importance of network security and the principles of the CIA triad (confidentiality, integrity, and availability), types of security threats and attacks
- Describe the basics of cryptography, including symmetric and asymmetric encryption, hash functions, digital signatures, and public key infrastructure (PKI).
- Apply authentication and access control techniques, including password-based, token-based, and biometric authentication, as well as authorization models and single sign-on (SSO).
- Design and implement secure networks using network segmentation, security zones, and VPNs for remote access.

- Implement and manage firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to protect network resources, secure wireless networks,
- Implement endpoint security and malware protection measures, including antivirus, patch management, and host-based firewalls.

SYLLABUS OF DSE

Unit 1 (10 hours)

Introduction to Network Security and Network Fundamentals: Importance of network security, Confidentiality, integrity, and availability (CIA) triad, Types of security threats and attacks. OSI and TCP/IP models. IP addressing and subnetting. Networking devices (hubs, switches, routers, firewalls). Network protocols and services (HTTP, HTTPS, FTP, SSH, etc.).

Unit 2 (12 hours)

Cryptography Basics, Authentication and Access Control, Secure Network Design: Symmetric and asymmetric encryption, Hash functions and digital signatures, Public key infrastructure (PKI), Common cryptographic algorithms (AES, RSA, SHA, etc.). Authentication techniques (passwords, tokens, biometrics), Authorization and access control models (RBAC, ABAC, MAC, DAC), Single sign-on (SSO) and multi-factor authentication (MFA). Defense-in-depth strategy, Network segmentation and isolation, Security zones and DMZ, VPNs and secure remote access.

Unit 3 (12 hours)

Firewalls and Intrusion Detection/Prevention Systems, Wireless Network Security: Types of firewalls (packet filtering, stateful inspection, application layer), IDS and IPS concepts and deployment, Signature-based and anomaly-based detection, Honeypots and honeynets. Wireless standards and technologies (802.11, Bluetooth, RFID), Wireless security protocols (WEP, WPA, WPA2, WPA3), Rogue access points and wireless attacks, Securing wireless networks.

Unit 4 (8 hours)

Endpoint Security and Malware Protection, Security Monitoring and Incident Response: Antivirus and antimalware solutions, Patch management and software updates, Host-based firewalls and intrusion detection, Mobile device management (MDM). Security Information and Event Management (SIEM) systems, Log management and analysis, Incident response process and procedures, Forensic analysis and evidence handling.

Unit 5 (3 hours)

Network Security Best Practices and Compliance: Security policies and procedures, Risk assessment and management, Security awareness training, Regulatory compliance (HIPAA, GDPR, PCI-DSS, etc.).

Essential/recommended readings

1. Behrouz Forouzan, Cryptography and network security. 3rd edition (2015), McGraw Hill Education.

2. Stallings, W. (2021). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.
3. Harris, S. (2018). All-in-One CISSP Exam Guide (8th Edition). McGraw-Hill Education.
4. Atul Kahate, Cryptography and Network Security, McGraw-Hill; Fourth edition (8 May 2019); McGraw Hill Education (India).

Additional References

i. Conklin, W. A., White, G., Williams, D., Davis, R., & Cothren, C. (2021). Principles of Computer Security: CompTIA Security+ and Beyond (6th Edition). McGraw-Hill Education.
ii. Chapple, M., & Seidl, D. (2020). Network Security For Dummies. Wiley.
iii. Gibson, D. (2021). CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide. YCDA Publishing.

Online Additional Reference Materials:

1. NIST Special Publications: https://csrc.nist.gov/publications/sp
   a. SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
   b. SP 800-82: Guide to Industrial Control Systems (ICS) Security
   c. SP 800-115: Technical Guide to Information Security Testing and Assessment
2. ISO/IEC 27000 series: Information Security Management Systems (ISMS)
   a. ISO/IEC 27001: Information Security Management
   b. ISO/IEC 27002: Code of Practice for Information Security Controls
   c. ISO/IEC 27005: Information Security Risk Management
3. Center for Internet Security (CIS) Critical Security Controls: https://www.cisecurity.org/controls/
   a. A prioritized set of actions to improve network security.
4. OWASP Top Ten Project: https://owasp.org/www-project-top-ten/
   a. A list of the most critical web application security risks.
5. SANS Institute Reading Room: https://www.sans.org/reading-room/
   a. A collection of whitepapers and articles on various network security topics.
6. Vendor documentation and best practices guides (Cisco, Juniper, Palo Alto Networks, etc.)