# NETWORK AND CYBER SECURITY
# ENCT 463

**Lecture : 3** **Year : IV**
**Tutorial : 1** **Part : II**
**Practical : 1.5**

**Course objectives:**
The main objective of this course is to provide fundamental understandings of networks and cyber security. Students will learn about network and cyber security principles, risk management, cryptographic techniques and defensive measures against cyber threats. The course aims to equip students with the necessary skills to design secure network systems and implement effective security strategies.

**1. Basics of Network and Cyber Security (5 hours)**
- 1.1. Introduction to Network and Cyber Security
- 1.2. Basic security requirements: Confidentiality, Integrity, Availability
- 1.3. Security threats and attacks
- 1.4. Security services and mechanisms
- 1.5. Risk management and vulnerabilities
- 1.6. Cyber Security Frameworks (NIST, ISO/IEC 27001)

**2. Cryptography (7 hours)**
- 2.1. Cryptography, its importance, plain text and cipher text
- 2.2. Type of ciphers: Symmetric and Asymmetric ciphers, Block and Stream ciphers
- 2.3. Traditional ciphers: Substitution (Mono-alphabetic, Polyalphabetic) and Transposition ciphers
- 2.4. Symmetric Block Ciphers: DES, AES
- 2.5. Asymmetric ciphers: RSA, ECC
- 2.6. Message digest, Hash functions (MD5, SHA)
- 2.7. Message authentication, Digital Signatures and Certificates
- 2.8. Public Key Infrastructure (PKI) and its importance

**3. Network Security Measures (7 hours)**
- 3.1. Transport Layer Security (TLS/SSL)
- 3.2. Virtual Private Networks (VPNs)
- 3.3. Network Traffic Analysis, Packet Capture
- 3.4. DNS Security
- 3.5. Network Access Control (NAC), Router Access Control List (ACLs)
- 3.6. Firewalls and Proxy Servers
- 3.7. Intrusion Detection and Prevention Systems (IDS/IPS)
- 3.8. System Protection (User Accounts, Access Permissions, Least Privilege, Multifactor Authentication, Secure Configuration and Patch Management)

**4. Securing Wireless and Mobile Networks (5 hours)**

4.1. Wireless Security Protocols (WEP, WPA, WPA2, WPA3)
4.2. Wireless Network Security Mechanisms (Authentication, Encryption and Secure Configuration, Hotspot Security, IEEE 802.1X)
4.3. Threats in Wireless Networks (Rogue Access Points, Sniffing)
4.4. Mobile Device Security (Device Encryption, Authentication, Application Permissions and Security Updates)
4.5. Wireless Access Control and Security Measures (MAC Filtering, SSID Security, Guest Networks, Network Segmentation and Secure Access Point Configuration)

**5. Malware and Cyber Attacks (7 hours)**

5.1. Types of Malwares (Viruses, Worms, Trojans, Ransomware)
5.2. Social Engineering Attacks (Phishing, Spear Phishing, Vishing, Quishing)
5.3. Denial of Service (DoS) and Distributed DoS (DDoS) Attacks, Man-in-the-Middle Attacks, Password Attacks
5.4. Zero-Day Exploits, Reconnaissance Attacks (IP probes, port scans, vulnerability scans)
5.5. Web Application Security (XSS, CSRF/XSRF, SQL injection, Authentication, Authorization, Validation, Secure Session)

**6. Incident Response and Risk Management (7 hours)**

6.1. Incident Response Planning and Management
6.2. Incident Identification and Classification
6.3. Security Monitoring and Log Analysis (System, Application, Firewall and Authentication Logs, Indicators of Compromise, Alert Investigation)
6.4. Incident Triage and Escalation (Event Correlation and Detection Rules)
6.5. Risk Assessment and Vulnerability Scanning
6.6. Digital Forensics and Evidence Handling (Preservation of Logs and Digital Evidence, Basic File and Log Examination, Evidence Integrity, Documentation and Chain of Custody)
6.7. Post-Incident Analysis, Reporting and Disaster Recovery Planning

**7. Ethical and Legal Aspects of Cyber Security (7 hours)**

7.1. Cyber Law and Regulations (e.g., GDPR, CCPA)
7.2. Security Policy Framework (SPF), MITRE ATT&CK Framework
7.3. Security Auditing and Compliance
7.4. Penetration Testing and Vulnerability Scanning
7.5. Ethics in Cyber Security
7.6. Ethical Hacking and Responsible Disclosure
7.7. Privacy Concerns and Data Protection
7.8. Intellectual Property and Digital Rights Management
7.9. Cyber law in the context of Nepal

**Tutorials: (15 hours)**

1. Security principles, CIA triad, threat identification and attack-scenario analysis

2. Classical ciphers, encryption/decryption exercises, hashing and digital signatures
3. Risk assessment, risk matrix, asset valuation and vulnerability prioritization
4. Firewall rules, router ACLs, proxy servers and IDS/IPS scenarios
5. Packet analysis using Wireshark: TCP handshakes, DNS queries and TLS traffic
6. Wireless security: compare WEP, WPA2 and WPA3; analyze secure configuration choices
7. Malware classification, phishing analysis and social engineering case studies
8. DoS/DDoS, MITM, password attacks and reconnaissance: attack scenarios and defenses
9. Web application vulnerabilities: SQL injection, XSS and CSRF; identify appropriate fixes
10. Vulnerability assessment: interpret a sample scan report and prioritize remediation
11. Incident response: identification, triage, escalation, containment and reporting
12. Digital forensics, evidence integrity, chain of custody and ethical/legal case studies

**Practical: (22.5 hours)**

1. Network Configurations (using simulator e.g., Cisco Packet Tracer)
2. Cryptography Algorithms Implementation
3. Network traffic analysis
4. Setting up Access Control, Firewalls and IDS/IPS
5. Vulnerability Assessment using tools (e.g., Nmap, Wireshark)
6. Simulating and Analyzing DDoS Attacks
7. Log analysis and incident response

**Evaluation Scheme:**

The questions will cover all the chapters of the syllabus. The evaluation scheme will be as indicated in the table below:

| Chapters | Hours | Marks distribution* |
|---|---|---|
| 1 | 5 | 6 |
| 2 | 7 | 10 |
| 3 | 7 | 9 |
| 4 | 5 | 6 |
| 5 | 7 | 9 |
| 6 | 7 | 10 |
| 7 | 7 | 10 |
| **Total** | **45** | **60** |

*There may be minor deviation in marks distribution

**References:**

1. Baloch, R. (2015). Ethical hacking and penetration testing guide. CRC Press.

2. Bishop, M. (2019). Computer security: Art and science (Latest ed.). Pearson Education.
3. Meeuwisse, R. (2017). Cybersecurity for beginners (Latest ed.). CyberGuard GmbH.
4. Murdoch, D. (2014). Blue team handbook: SOC, SIEM and threat hunting use cases (notes from the grid). CreateSpace Independent Publishing Platform.
5. Simpson, M. T., & Antill, N. (2017). Hands-on ethical hacking and network defense (3rd ed.). Cengage Learning.
6. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
7. Stallings, W. (2017). Network security essentials: Applications and standards (Latest ed.). Pearson Education.
8. Stallings, W. (2017). Cryptography and network security: Principles and practice (latest ed.). Pearson Education.
9. Stuttard, D., & Pinto, M. (2011). The web application hacker's handbook: Finding and exploiting security flaws (Latest ed.). Wiley.