NETWORKING and CYBER SECURITY

Semester 1

Principles of Computer Networking (NCS1A)

Networking Fundamentals

C 1: Introduction to Networking Concepts

- What is networking? Overview of network types (LAN, WAN, WLAN)
- Basic network terminology: nodes, links, protocols and more
- Understanding the role of networking in computing

C 2: Network Models and Protocols

- Introduction to network models: OSI model, TCP/IP model
- Explanation of each layer in the OSI model and its functions
- Common protocols: HTTP, FTP, TCP, UDP, IP and more

C 3: IP Addressing and Subnetting

- Basics of IP addressing: IPv4 vs. IPv6
- Structure of an IP address: network and host parts
- Introduction to subnetting: subnet masks and CIDR notation

C 4: Networking Devices and Hardware

- Overview of networking hardware: routers, switches, hubs, modems and more
- Functions of each device in a network, at least 15 devices
- Introduction to network cables and connectors

C 5: Network Topologies and Design

- Common network topologies: star, ring, bus, mesh
- Advantages and disadvantages of each topology
- Basic network design principles

C 6: Network Security Basics

- Introduction to network security: threats and vulnerabilities
- Basic security concepts: firewalls, encryption, VPNs
- Importance of securing network infrastructure

Week 2: Network Configuration and Management

C 8: Basic Network Configuration

- Introduction to configuring network settings
- Configuring IP addresses manually and using DHCP
- Basic router and switch configuration

C 9: Understanding DNS and DHCP

- Role of DNS (Domain Name System) in networking
- How DHCP (Dynamic Host Configuration Protocol) works
- Configuring and troubleshooting DNS and DHCP settings

C 10: Introduction to Network Services

- Overview of common network services: email, web hosting, file sharing
- How these services are implemented in a network
- Basic setup and configuration of network services

C 11: Network Monitoring and Troubleshooting

- Introduction to network monitoring tools: ping, tracert, netstat
- Basic troubleshooting steps for network issues
- Understanding network logs and diagnostic information

C 12: Wireless Networking Basics

- Overview of wireless networks: WLAN, Wi-Fi standards (802.11a/b/g/n/ac/ax)
- Configuring and securing wireless networks
- Troubleshooting common wireless network issues

C 13: Network Performance Optimization

- Techniques for optimizing network performance: QoS (Quality of Service), bandwidth management
- Identifying and resolving network bottlenecks
- Tools for performance analysis and improvement

C 14: Review and Practical Assessment

- Comprehensive review of network configuration and management topics
- Practical assessment to test configuration and troubleshooting skills

---

Advanced Networking Concepts

C 15: Network Address Translation (NAT)

- Understanding NAT and its types: static, dynamic, PAT (Port Address Translation)
- How NAT is used to manage IP addresses and improve security
- Configuring NAT on routers

C 16: VLANs and Switching

- Introduction to VLANs (Virtual Local Area Networks)
- Benefits and configuration of VLANs in a network
- Basics of VLAN tagging and trunking

C 17: Routing Protocols and Techniques

- Overview of routing protocols: RIP, OSPF, BGP
- Understanding static vs. dynamic routing
- Basic configuration of routing protocols

C 18: Introduction to IPv6

- Understanding the need for IPv6 and its features
- IPv6 address structure and notation
- Configuring IPv6 addresses and routing

C 19: Network Security Advanced Topics

- Advanced security concepts: IDS/IPS (Intrusion Detection/Prevention Systems), SIEM (Security Information and Event Management)
- Implementing advanced security measures and policies
- Case studies of network security breaches

C 20: Cloud Networking Basics

- Introduction to cloud networking: concepts and models
- Overview of cloud service providers (AWS, Azure, Google Cloud)
- Basics of configuring and managing cloud networks

C 21: Review and Practical Application

- Review of advanced networking concepts

- Practical exercises to apply advanced networking skills

Hands-On Practice and Project Work

C 22: Building a Small Network

- Designing and implementing a small network setup
- Configuring network devices and services
- Testing and validating the network setup

C 23: Network Project Work: Part 1

- Planning and starting a network project
- Assigning roles and tasks for the project

C 24: Network Project Work: Part 2

- Continued work on the network project
- Implementing and configuring network solutions

C 25: Troubleshooting and Optimizing the Network

- Identifying and resolving issues in the network project
- Optimizing network performance and security

C 26: Presentation and Review of Network Projects

- Presentation of completed network projects
- Peer review and feedback on projects

C 27: Introduction to Network Automation

- Basics of network automation and management tools
- Overview of network automation platforms (e.g., Ansible, Cisco DNA)

C 28: Future Trends in Networking

- Emerging trends and technologies in networking
- The impact of IoT (Internet of Things) and 5G on networking

C 29: Final Review and Assessment

- Comprehensive review of all topics covered in the course
- Final assessment to evaluate overall understanding and skills

Cloud Computing and Topologies (NCS1B)

Introduction to Cloud Computing

C 1: Introduction to Cloud Computing

- Definition and core concepts of cloud computing
- Cloud service models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service)
- Benefits and challenges of cloud computing

C 2: Cloud Deployment Models

- Public, private, and hybrid clouds
- Community cloud and its use cases
- Differences and use cases for each deployment model

C 3: Major Cloud Providers and Services

- Overview of major cloud service providers: AWS (Amazon Web Services), Azure (Microsoft), Google Cloud Platform (GCP)
- Key services offered by each provider: compute, storage, databases, networking

C 4: Cloud Architecture and Components

- Understanding cloud architecture: regions, availability zones, data centers
- Key components: virtual machines, storage solutions, networking components

C 5: Cloud Security Fundamentals

- Introduction to cloud security concepts
- Shared responsibility model in cloud security
- Basic security measures: encryption, access control, compliance

C 6: Hands-On: Cloud Service Setup

- Practical setup of cloud services (e.g., creating virtual machines, configuring storage)
- Using a cloud provider's management console (AWS Console, Azure Portal, GCP Console)

C 7: Review and Quiz

- Recap of cloud computing fundamentals
- Knowledge check and quiz on cloud concepts and services

Network Topologies and Technologies

C 8: Introduction to Network Topologies

- Definition and types of network topologies: star, ring, bus, mesh
- Advantages and disadvantages of each topology
- Real-world applications of different topologies

C 9: LAN Technologies and Components

- Overview of LAN technologies: Ethernet, Wi-Fi
- Components of LAN: switches, routers, access points
- LAN configuration and management

C 10: WAN Technologies and Components

- Overview of WAN technologies: MPLS, VPNs, leased lines
- Components of WAN: routers, modems, WAN links
- WAN configuration and management

C 11: Network Protocols and Communication

- Common network protocols: IP, TCP, UDP, HTTP/HTTPS
- Protocol roles in communication and data transfer
- Basics of network packet structure and routing

C 12: Network Design and Planning

- Principles of network design: scalability, reliability, performance
- Designing a network topology for specific needs
- Creating network diagrams and documentation

C 13: Network Security Fundamentals

- Introduction to network security: threats and vulnerabilities
- Basic security measures: firewalls, VPNs, IDS/IPS
- Best practices for network security

C 14: Review and Practical Assessment

- Comprehensive review of network topologies and technologies
- Practical assessment to demonstrate understanding and configuration skills

Cloud Networking and Integration

C 15: Cloud Networking Basics

- Overview of networking in the cloud
- Virtual networks and subnets in cloud environments
- Cloud network security and isolation

C 16: Configuring Cloud Networks

- Setting up virtual private networks (VPNs) in the cloud
- Configuring network security groups and access controls
- Hands-on: Creating and managing cloud virtual networks

C 17: Cloud Storage Solutions

- Types of cloud storage: object storage, block storage, file storage
- Configuring and managing storage solutions
- Integrating storage with compute resources

C 18: Cloud Services Integration

- Integrating cloud services with on-premises systems
- Understanding hybrid cloud architectures
- Tools and technologies for cloud integration

C 19: High Availability and Disaster Recovery

- Concepts of high availability and disaster recovery in the cloud
- Configuring redundancy and failover solutions
- Designing disaster recovery plans

C 20: Monitoring and Managing Cloud Resources

- Tools for monitoring cloud resources (e.g., CloudWatch, Azure Monitor)
- Best practices for resource management and cost optimization
- Setting up alerts and automation for cloud resources

C 21: Review and Practical Application

- Review of cloud networking concepts and configurations
- Practical exercises on integrating and managing cloud services

Advanced Topics and Project Work

C 22: Advanced Cloud Computing Concepts

- Introduction to serverless computing (AWS Lambda, Azure Functions)
- Overview of containerization (Docker, Kubernetes)
- Cloud DevOps practices and tools

C 23: Network Automation and Management

- Basics of network automation: tools and frameworks
- Overview of network management systems
- Automating network tasks and configurations

C 24: Cloud Security Advanced Topics

- Advanced cloud security practices: identity and access management (IAM), security policies
- Compliance and regulatory considerations
- Conducting security assessments and audits

C 25: Building and Managing a Cloud-Based Network

- Designing and deploying a cloud-based network
- Configuring network components and security measures
- Hands-on: Implementing a cloud network solution

C 26: Cloud Network Design

- Planning and developing a comprehensive cloud network solution
- Implementation of design with attention to security, scalability, and integration

C 27: Testing and Optimization

- Testing the cloud network project
- Optimizing performance and resolving any issues
- Preparing the final presentation of the project

C 28: Presentation and Review of Final Projects

- Presentation of final cloud network projects
- Peer review and feedback on project implementations

C 29: Future Trends in Cloud Computing and Networking

- Emerging trends: edge computing, AI in cloud, 5G integration
- Impact of new technologies on cloud and network design

Introduction to Network Security (NCS1C)

Introduction to Network Security

C 1: Introduction to Network Security

- Overview of network security: importance and objectives
- Key concepts: confidentiality, integrity, availability
- Understanding network threats and vulnerabilities

C 2: Network Security Models and Frameworks

- Introduction to network security models: Bell-LaPadula, Biba, Clark-Wilson
- Security frameworks and standards: NIST Cybersecurity Framework, ISO/IEC 27001
- Understanding security policies and procedures

C 3: Threats and Vulnerabilities

- Types of network threats: malware, phishing, denial of service (DoS) attacks
- Common network vulnerabilities: unpatched software, weak passwords, misconfigured devices
- Methods of threat modeling and risk assessment

C 4: Network Security Principles

- Principle of least privilege
- Defense in depth
- Security by design
- Understanding the importance of regular updates and patches

C 5: Network Security Devices and Technologies

- Overview of network security devices: firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs
- Functions and roles of each device
- Introduction to security technologies: encryption, access control, authentication

C 6: Hands-On: Basic Network Security Configuration

- Configuring basic security settings on routers and switches
- Setting up firewalls and VPNs
- Implementing basic access control measures

C 7: Review and Quiz

- Recap of network security fundamentals
- Knowledge check and quiz on basic concepts and devices

Network Security Policies and Management

C 8: Security Policies and Procedures

- Developing network security policies: access control, acceptable use, incident response
- Creating and enforcing security procedures
- Importance of regular policy reviews and updates

C 9: Access Control and Authentication

- Understanding access control models: discretionary, mandatory, role-based
- Authentication methods: passwords, biometrics, multi-factor authentication (MFA)
- Implementing and managing access control mechanisms

C 10: Network Security Monitoring and Logging

- Importance of network monitoring and logging
- Tools for monitoring network traffic and security events
- Setting up and analyzing logs for security incidents

C 11: Incident Response and Management

- Steps in an incident response plan: identification, containment, eradication, recovery
- Roles and responsibilities in incident response
- Developing and testing an incident response plan

C 12: Encryption and Data Protection

- Basics of encryption: symmetric vs. asymmetric encryption
- Implementing encryption for data in transit and at rest
- Understanding data protection regulations and standards (e.g., GDPR, HIPAA)

C 13: Hands-On: Implementing Security Policies

- Creating and enforcing network security policies
- Configuring access controls and authentication mechanisms
- Setting up encryption for secure communications

C 14: Review and Practical Assessment

- Comprehensive review of security policies and management topics
- Practical assessment to demonstrate understanding and configuration skills

Advanced Network Security Topics

C 15: Advanced Threats and Attack Vectors

- Understanding advanced threats: APTs (Advanced Persistent Threats), zero-C attacks
- Attack vectors: network attacks, application attacks, physical attacks
- Strategies for mitigating advanced threats

C 16: Intrusion Detection and Prevention Systems (IDS/IPS)

- Overview of IDS and IPS technologies
- Types of IDS/IPS: network-based, host-based
- Configuring and managing IDS/IPS systems

C 17: Firewalls and Network Segmentation

- Types of firewalls: packet-filtering, stateful, next-generation
- Implementing firewall rules and policies
- Importance of network segmentation and VLANs for security

C 18: Secure Network Design and Architecture

- Principles of secure network design: segmentation, redundancy, monitoring
- Designing networks with security in mind
- Best practices for securing network architecture

C 19: Network Security for Cloud Environments

- Cloud security considerations: shared responsibility model, cloud-specific threats
- Securing cloud networks: firewalls, encryption, access controls
- Best practices for cloud security

C 20: Hands-On: Configuring IDS/IPS and Firewalls

- Implementing and configuring IDS/IPS systems
- Setting up and managing firewall rules
- Designing and configuring network segments for security

C 21: Review and Practical Application

- Review of advanced network security concepts
- Practical exercises to apply advanced security skills

Security Best Practices and Emerging Trends

C 22: Security Best Practices

- Implementing security best practices: patch management, security updates, user training
- Conducting security audits and assessments
- Developing a culture of security within an organization

C 23: Emerging Trends in Network Security

- Overview of emerging trends: AI and machine learning in security, threat intelligence, blockchain
- Impact of new technologies on network security
- Preparing for future security challenges

C 24: Security Compliance and Regulations

- Understanding security compliance requirements: PCI-DSS, SOX, FISMA
- Preparing for audits and compliance assessments
- Implementing controls to meet regulatory requirements

C 25: Hands-On: Security Best Practices and Compliance

- Implementing best practices for network security
- Preparing for a security audit
- Configuring security controls to meet compliance requirements

C 26: Network Security Implementation

- Planning and implementing a comprehensive network security solution
- Configuring security devices and policies
- Testing and validating security measures

C 27: Testing and Review

- Testing the final network security project
- Reviewing and refining security configurations
- Preparing the final presentation

C 28: Presentation and Review of Final Projects

- Presentation of completed network security projects
- Peer review and feedback on implementations

Operating Systems and Network Integration (NCS1D)

Introduction to Operating Systems

C 1: Overview of Operating Systems

- Definition and purpose of an operating system (OS)
- Key functions: process management, memory management, file system management
- Types of operating systems: Windows, Linux, macOS

C 2: Operating System Architecture

- OS components: kernel, shell, file system
- Understanding system calls and APIs
- Differences between monolithic kernels, microkernels, and hybrid kernels

C 3: Process and Memory Management

- Concepts of processes and threads
- Process scheduling and management
- Memory management: paging, segmentation, virtual memory

C 4: File Systems and Storage Management

- Overview of file systems: NTFS, FAT32, ext4, HFS+
- File system structure and management
- Storage management: partitions, logical volumes, RAID

C 5: User and Group Management

- User account and group management: creation, modification, deletion
- File permissions and access control
- Understanding user authentication and authorization

C 6: Hands-On: Basic OS Configuration

- Configuring system settings and preferences
- Managing users and groups
- Basic file system operations

C 7: Review and Quiz

- Recap of operating system fundamentals
- Knowledge check and quiz on OS concepts and configurations

Network Fundamentals and Integration

C 8: Introduction to Networking Basics

- Basic networking concepts: IP addresses, subnets, routers, switches
- Understanding network protocols: TCP/IP, UDP
- Network topologies and architectures

C 9: Network Configuration and Management

- Configuring network settings on different OSes
- Network interfaces and IP configuration: static vs. dynamic IP
- Troubleshooting network connectivity issues

C 10: Network Services and Protocols

- Overview of common network services: DNS, DHCP, HTTP/HTTPS
- Configuring and managing network services on different OSes
- Understanding protocol interactions and data flow

C 11: Introduction to Network Security

- Basics of network security: firewalls, VPNs, encryption
- Implementing basic security measures on networked systems
- Understanding network security best practices

C 12: Network Tools and Utilities

- Overview of network tools: ping, traceroute, netstat, ipconfig/ifconfig
- Using network monitoring and diagnostic tools
- Analyzing network performance and troubleshooting issues

C 13: Hands-On: Network Configuration

- Configuring network settings and services on Windows and Linux
- Setting up basic network security features
- Using network diagnostic tools

C 14: Review and Practical Assessment

- Comprehensive review of network fundamentals and integration
- Practical assessment to demonstrate configuration and troubleshooting skills

Advanced Operating Systems and Network Integration

C 15: Advanced OS Configuration

- Managing system resources and performance tuning
- Configuring and managing system services and daemons
- OS-specific configuration: Windows Services, Linux systemd

C 16: File Sharing and Network File Systems

- Understanding file sharing protocols: SMB, NFS
- Configuring and managing network file systems
- Troubleshooting file sharing issues

C 17: Remote Access and Management

- Overview of remote access methods: SSH, RDP, VNC
- Configuring remote access on different OSes
- Security considerations for remote access

C 18: Integrating OS with Cloud Services

- Overview of cloud integration: IaaS, PaaS, SaaS
- Configuring OS instances on cloud platforms (AWS, Azure, GCP)
- Managing cloud-based storage and services

C 19: Automation and Scripting

- Introduction to automation: benefits and tools
- Scripting languages: PowerShell, Bash
- Automating routine tasks and configurations

C 20: Hands-On: Advanced OS and Network Integration

- Configuring advanced OS settings and services
- Setting up and managing network file systems
- Implementing automation scripts for routine tasks

C 21: Review and Practical Application

- Review of advanced OS and network integration concepts
- Practical exercises to apply advanced configuration and automation skills

Security, Troubleshooting, and Project Work

C 22: OS and Network Security Best Practices

- Implementing security best practices for OS and network integration
- Understanding and mitigating security threats: patch management, access control
- Securing remote access and network services

C 23: Troubleshooting OS and Network Issues

- Common OS issues and troubleshooting steps
- Network troubleshooting: connectivity, performance, security
- Using diagnostic tools and logs for problem resolution

C 24: Final Project Work: OS and Network Integration

- Planning and executing a comprehensive OS and network integration project
- Configuring and securing network services on multiple OSes
- Implementing best practices and automation

C 25: Testing and Optimization

- Testing and validating the final project
- Optimizing performance and security settings
- Documenting the project and preparing for presentation

C 26: Presentation and Review of Final Projects

- Presentation of final OS and network integration projects
- Peer review and feedback on project implementations

C 27: Future Trends in OS and Network Integration

- Emerging trends: containerization, virtualization, hybrid cloud environments
- The impact of new technologies on OS and network integration
- Preparing for future developments and advancements

C 28: Course Review and Final Assessment

- Comprehensive review of all topics covered in the course
- Final assessment to evaluate overall understanding and skills

Routing and Switching (NCS1E)

Introduction to Routing and Switching

C 1: Basics of Routing and Switching

- Overview of routing and switching concepts
- Differences between routers and switches
- Functions and roles of routing and switching in networks

C 2: Network Models and Protocols

- OSI model vs. TCP/IP model: layers and functions
- Introduction to key network protocols: IP, ARP, ICMP
- Understanding Ethernet and VLANs

C 3: Switching Fundamentals

- Basics of Ethernet switching: MAC addresses, frames
- Introduction to VLANs (Virtual LANs) and trunking
- Switching techniques: store-and-forward, cut-through

C 4: Routing Fundamentals

- Basic routing concepts: routing tables, static vs. dynamic routing
- Introduction to routing protocols: RIP, OSPF, EIGRP
- Understanding IP addressing and subnetting

C 5: Hands-On: Basic Switching Configuration

- Configuring VLANs and VLAN interfaces
- Setting up trunk ports and inter-VLAN routing
- Using basic switch configuration commands

C 6: Hands-On: Basic Routing Configuration

- Configuring static routes
- Setting up and verifying dynamic routing protocols
- Understanding routing tables and metrics

C 7: Review and Quiz

- Recap of routing and switching fundamentals
- Knowledge check and quiz on basic concepts and configurations

---

Advanced Switching and Routing Techniques

C 8: Advanced Switching Concepts

- VLAN configuration and management: VLAN assignment, VLAN tagging
- Spanning Tree Protocol (STP): concepts, configuration, and troubleshooting
- Understanding switch stacking and high availability

C 9: Advanced Routing Protocols

- Deep dive into dynamic routing protocols: OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol)
- Configuration of OSPF and EIGRP
- Understanding and troubleshooting routing protocol operation

C 10: Network Address Translation (NAT)

- Introduction to NAT: types and purposes (static, dynamic, PAT)
- Configuring NAT on routers
- Troubleshooting NAT issues

C 11: Access Control Lists (ACLs)

- Understanding ACLs: standard vs. extended
- Configuring and applying ACLs on routers and switches
- Troubleshooting ACLs and their impact on network traffic

C 12: Quality of Service (QoS)

- Introduction to QoS concepts: traffic classification, marking, queuing
- Configuring QoS policies on network devices
- Troubleshooting QoS issues and optimizing performance

C 13: Hands-On: Advanced Switching Configuration

- Configuring and troubleshooting STP, RSTP, and MSTP
- Implementing advanced VLAN features and switch stacking
- Managing switch security features

C 14: Hands-On: Advanced Routing Configuration

- Configuring and troubleshooting OSPF and EIGRP
- Implementing NAT and ACLs
- Configuring and managing QoS policies

Network Design and Implementation

C 15: Network Design Principles

- Principles of network design: scalability, redundancy, performance
- Designing networks for different requirements: small office, enterprise, data center
- Creating network diagrams and documentation

C 16: Implementing Routing and Switching in Different Environments

- Design and configuration of network solutions for various environments: campus, branch, data center
- Integrating routing and switching with other network services (e.g., DHCP, DNS)

C 17: Network Security Considerations

- Implementing security features: VLAN security, ACLs for access control
- Securing routing protocols and network devices
- Understanding network segmentation and isolation

C 18: Troubleshooting Routing and Switching

- Common issues and troubleshooting techniques for routing and switching
- Using diagnostic tools: ping, traceroute, show commands
- Analyzing and resolving configuration problems

C 19: Network Automation and Management

- Introduction to network automation: benefits and tools (e.g., Ansible, Python scripting)
- Basic automation tasks: configuration backup, device management
- Overview of network management systems and their integration

C 20: Hands-On: Network Design and Implementation

- Designing and implementing a network based on specific requirements
- Configuring routing and switching features for the designed network
- Testing and validating network performance and security

C 21: Review and Practical Assessment

- Comprehensive review of routing and switching concepts
- Practical assessment to demonstrate configuration and troubleshooting skills

---

Advanced Topics and Project Work

C 22: Advanced Routing Techniques

- Implementing and troubleshooting advanced routing features: route redistribution, policy-based routing
- Understanding and configuring BGP (Border Gateway Protocol) for inter-domain routing

C 23: Advanced Switching Techniques

- Implementing advanced switching features: EtherChannel, port security, private VLANs
- Troubleshooting complex switching issues and optimizing performance

C 24: Network Performance Optimization

- Techniques for optimizing network performance: load balancing, link aggregation
- Monitoring and analyzing network performance metrics
- Best practices for performance tuning and troubleshooting

C 25: Network Design and Implementation

- Planning and executing a comprehensive network project
- Configuring and integrating advanced routing and switching features
- Implementing security measures and performance optimizations

C 26: Testing and Optimization

- Testing and validating the final network project
- Optimizing configurations and resolving any issues
- Documenting the project and preparing for presentation

C 27: Future Trends in Networking

- Overview of emerging trends: SD-WAN (Software-Defined WAN), network virtualization, 5G
- The impact of new technologies on routing and switching
- Preparing for future developments and advancements

C 28: Course Review and Final Assessment

- Comprehensive review of all routing and switching topics covered
- Final assessment to evaluate overall understanding and skills

NETWORKING and CYBER SECURITY

Semester 2

Principles of Cyber Security (NCS2A)

Introduction to Cybersecurity Fundamentals

C 1: Overview of Cybersecurity

- Definition and importance of cybersecurity.
- Key concepts and terminology.

C 2: Understanding Security Policies

- Purpose and types of security policies.
- Components of effective security policies.

C 3: Developing Security Policies

- Steps to create a security policy.
- Examples of common security policies (e.g., access control, data protection).

C 4: Implementing Security Policies

- Best practices for policy implementation.
- Communicating policies to stakeholders.

C 5: Case Studies

- Review real-world examples of security policies.
- Discussion on policy effectiveness.

C 6: Review and Discussion

- Recap of key concepts from the week.
- Q&A session.

C 7: Practical Exercise

- Draft a basic security policy for a hypothetical organization.

Risk Management

C 8: Introduction to Risk Management

- Definition and importance of risk management.
- Key concepts: risk, threat, vulnerability, and impact.

C 9: Risk Assessment

- Methods for identifying risks (e.g., threat modeling, vulnerability assessments).
- Tools for risk assessment.

C 10: Risk Analysis

- Qualitative and quantitative risk analysis.
- Evaluating risk impact and likelihood.

C 11: Risk Mitigation Strategies

- Risk avoidance, reduction, transfer, and acceptance.
- Implementing mitigation controls.

C 12: Risk Management Frameworks

- Overview of frameworks (e.g., NIST, ISO 27001).
- How to apply these frameworks in practice.

C 13: Review and Discussion

- Recap of risk management principles.
- Q&A session.

C 14: Practical Exercise

- Conduct a risk assessment for a hypothetical scenario.

Compliance

C 15: Understanding Compliance

- Definition and importance of compliance in cybersecurity.
- Overview of relevant regulations and standards (e.g., GDPR, HIPAA, PCI-DSS).

C 16: Compliance Frameworks and Standards

- Detailed look at major compliance frameworks.

- How to align security practices with compliance requirements.

C 17: Implementing Compliance Measures

- Steps to achieve and maintain compliance.
- Common challenges and solutions.

C 18: Audits and Assessments

- Role of audits in maintaining compliance.
- Preparing for and responding to audits.

C 19: Compliance and Security Policies

- How security policies support compliance.
- Integrating compliance into policy development.

C 20: Review and Discussion

- Recap of compliance concepts.
- Q&A session.

C 21: Practical Exercise

- Develop a compliance plan for a hypothetical organization.

Incident Response and Disaster Recovery

C 22: Introduction to Incident Response

- Definition and importance of incident response.
- Key phases of incident response (e.g., preparation, detection, containment).

C 23: Incident Response Planning

- Developing an incident response plan.
- Roles and responsibilities in incident response.

C 24: Incident Response Tools and Techniques

- Tools for detecting and managing incidents.
- Techniques for incident handling and investigation.

C 25: Introduction to Disaster Recovery

- Definition and importance of disaster recovery.
- Key components of a disaster recovery plan.

C 26: Developing a Disaster Recovery Plan

- Steps to create and test a disaster recovery plan.
- Business continuity considerations.

C 27: Incident Response and Disaster Recovery Integration

- How incident response and disaster recovery plans work together.
- Best practices for integration.

C 28: Review and Discussion

- Recap of incident response and disaster recovery concepts.
- Q&A session.

C 29: Practical Exercise

- Create an incident response plan and a disaster recovery plan for a hypothetical organization.

C 30: Final Review and Assessment

- Comprehensive review of all topics covered.
- Assessment quiz or project presentation.

Firewalls and Intrusion Detection (NCS2B)

Introduction to Firewalls

C 1: Overview of Firewalls

- Definition and purpose of firewalls.
- Types of firewalls (e.g., hardware, software, cloud-based).

C 2: Firewall Architecture

- Basic firewall components.
- How firewalls fit into network architecture.

C 3: Types of Firewalls

- Packet Filtering Firewalls
- Stateful Inspection Firewalls
- Proxy Firewalls

- Next-Generation Firewalls (NGFW)

C 4: Designing Firewalls

- Principles of firewall design.
- Creating effective firewall rules and policies.

C 5: Implementing Firewalls

- Deployment strategies.
- Common configuration tasks.

C 6: Review and Discussion

- Recap of firewall concepts.
- Q&A session.

C 7: Practical Exercise

- Design and configure a basic firewall for a hypothetical network.

Advanced Firewall Configuration

C 8: Firewall Management

- Monitoring and maintaining firewalls.
- Handling firewall logs and alerts.

C 9: Firewall Security Best Practices

- Hardening firewalls.
- Preventing common configuration mistakes.

C 10: Firewall Troubleshooting

- Diagnosing and resolving common issues.
- Tools and techniques for troubleshooting.

C 11: Firewall Integration

- Integrating firewalls with other security systems.
- Coordination with intrusion detection systems.

C 12: Case Studies

- Real-world examples of firewall implementations.
- Discussion on challenges and solutions.

C 13: Review and Discussion

- Recap of advanced firewall topics.
- Q&A session.

C 14: Practical Exercise

- Configure advanced firewall features (e.g., VPN, advanced rules) for a hypothetical scenario.

Introduction to Intrusion Detection and Prevention Systems (IDPS)

C 15: Overview of IDPS

- Definition and purpose of IDPS.
- Differences between Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

C 16: Types of IDPS

- Network-Based IDPS (NIDPS)
- Host-Based IDPS (HIDPS)
- Hybrid IDPS

C 17: IDPS Architecture

- Components of an IDPS.
- How IDPS integrates into network architecture.

C 18: Designing IDPS

- Principles of IDPS design.
- Placement and configuration considerations.

C 19: Implementing IDPS

- Deployment strategies for IDPS.
- Basic configuration tasks.

C 20: Review and Discussion

- Recap of IDPS concepts.
- Q&A session.

C 21: Practical Exercise

- Design and implement a basic IDPS setup for a hypothetical network.

Advanced IDPS Configuration and Management

C 22: IDPS Management

- Monitoring and maintaining IDPS.
- Handling IDPS logs and alerts.

C 23: IDPS Tuning and Optimization

- Techniques for reducing false positives/negatives.
- Performance optimization.

C 24: Incident Response Integration

- How IDPS alerts can be used in incident response.
- Coordination with other security measures.

C 25: Case Studies

- Real-world examples of IDPS deployments.
- Discussion on lessons learned and best practices.

C 26: Advanced IDPS Features

- Exploring advanced features (e.g., behavioral analysis, machine learning).
- Use cases and practical applications.

C 27: Review and Discussion

- Recap of advanced IDPS topics.
- Q&A session.

C 28: Practical Exercise

- Configure advanced IDPS features for a hypothetical scenario.

C 29: Final Review

- Comprehensive review of all topics covered.
- Group discussion and Q&A.

C 30: Assessment and Wrap-Up

- Assessment quiz or project presentation.
- Final review and feedback session

Ethical Hacking and Penetration Testing (NCS2C)

Introduction to Ethical Hacking

C 1: Overview of Ethical Hacking

- Definition and objectives of ethical hacking.
- Ethical hacker vs. malicious hacker.
- Legal and ethical considerations.

C 2: Types of Ethical Hackers

- White hat, black hat, and gray hat hackers.
- Roles and responsibilities of ethical hackers.

C 3: Ethical Hacking Tools and Techniques

- Overview of common tools (e.g., Nmap, Metasploit).
- Basic techniques and approaches used in ethical hacking.

C 4: Legal and Ethical Frameworks

- Understanding laws and regulations related to hacking.
- Importance of obtaining proper authorization.

C 5: Setting Up a Penetration Testing Lab

- Creating a virtual lab environment.
- Tools and resources for a penetration testing lab.

C 6: Review and Discussion

- Recap of ethical hacking fundamentals.
- Q&A session.

C 7: Practical Exercise

- Set up and configure a basic penetration testing lab.

Penetration Testing Methodologies

C 8: Introduction to Penetration Testing

- Definition and goals of penetration testing.
- Phases of a penetration test.

C 9: Pre-Engagement Activities

- Scope definition and rules of engagement.
- Gathering information (OSINT, reconnaissance).

C 10: Scanning and Enumeration

- Network scanning techniques (e.g., port scanning, service detection).
- Enumeration of network services and vulnerabilities.

C 11: Vulnerability Assessment

- Identifying and analyzing vulnerabilities.
- Tools and techniques for vulnerability scanning.

C 12: Exploitation Techniques

- Exploiting identified vulnerabilities.
- Understanding exploit frameworks and payloads.

C 13: Post-Exploitation

- Techniques for maintaining access and privilege escalation.
- Information gathering during post-exploitation.

C 14: Review and Discussion

- Recap of penetration testing methodologies.
- Q&A session.

C 15: Practical Exercise

- Perform a basic penetration test on a controlled environment.

Advanced Penetration Testing Techniques

C 16: Web Application Penetration Testing

- Overview of web application vulnerabilities (e.g., SQL injection, XSS).

- Tools and techniques for web application testing.

C 17: Network Penetration Testing

- Techniques for network-based attacks (e.g., man-in-the-middle, network sniffing).
- Tools and methodologies for network penetration testing.

C 18: Wireless Network Penetration Testing

- Identifying vulnerabilities in wireless networks.
- Tools and techniques for testing wireless networks.

C 19: Social Engineering Attacks

- Techniques and methods for social engineering.
- Defending against social engineering attacks.

C 20: Mobile Application Penetration Testing

- Overview of mobile application vulnerabilities.
- Tools and techniques for testing mobile applications.

C 21: Review and Discussion

- Recap of advanced penetration testing topics.
- Q&A session.

C 22: Practical Exercise

- Conduct an advanced penetration test focusing on web, network, or mobile applications.

Reporting and Follow-Up

C 23: Reporting and Documentation

- Creating detailed penetration testing reports.
- Best practices for documenting findings and recommendations.

C 24: Presentation Skills

- Communicating findings to technical and non-technical stakeholders.
- Crafting an effective presentation.

C 25: Remediation and Follow-Up

- Assisting with remediation efforts.
- Verifying and retesting after remediation.

C 26: Ethical Hacking Certifications and Careers

- Overview of certifications (e.g., CEH, OSCP).
- Career paths in ethical hacking and penetration testing.

C 27: Review and Discussion

- Comprehensive review of ethical hacking and penetration testing concepts.
- Q&A session.

C 28: Practical Exercise

- Prepare a complete penetration testing report and presentation based on a hypothetical scenario.

C 29: Final Assessment

- Assessment quiz or project presentation.
- Practical evaluation of penetration testing skills.

C 30: Wrap-Up and Feedback

- Final review of course content.
- Feedback session and next steps for further learning.

Secure Software Development (NCS2D)

Introduction to Secure Software Development

C 1: Overview of Secure Software Development

- Importance of security in software development.
- Key concepts and terminology.

C 2: Security in the Software Development Lifecycle (SDLC)

- Stages of the SDLC (e.g., requirements, design, implementation, testing, deployment).
- Integrating security into each phase of the SDLC.

C 3: Threat Modeling

- Introduction to threat modeling.
- Common methodologies (e.g., STRIDE, PASTA).
- Identifying threats and vulnerabilities.

C 4: Security Requirements and Specifications

- Gathering and defining security requirements.
- Writing secure specifications.

C 5: Secure Design Principles

- Principles for secure software design (e.g., least privilege, defense in depth).
- Security architecture and design patterns.

C 6: Review and Discussion

- Recap of secure software development fundamentals.
- Q&A session.

C 7: Practical Exercise

- Conduct a threat modeling session for a hypothetical application.

Secure Coding Practices

C 8: Introduction to Secure Coding

- Overview of secure coding practices.
- Importance of following coding standards.

C 9: Common Software Vulnerabilities

- Overview of common vulnerabilities (e.g., SQL Injection, Cross-Site Scripting (XSS), Buffer Overflow).
- Examples and impacts.

C 10: Input Validation and Data Sanitization

- Techniques for validating and sanitizing user input.
- Preventing injection attacks.

C 11: Authentication and Authorization

- Secure practices for authentication and authorization.
- Implementing multi-factor authentication (MFA).

C 12: Secure Session Management

- Techniques for secure session management.
- Protecting against session hijacking and fixation.

C 13: Error Handling and Logging

- Best practices for error handling and logging.
- Avoiding information leakage through logs.

C 14: Review and Discussion

- Recap of secure coding practices.
- Q&A session.

C 15: Practical Exercise

- Identify and fix vulnerabilities in a provided codebase.

Secure Development Practices and Tools

C 16: Secure Development Best Practices

- Coding standards and guidelines (e.g., OWASP Secure Coding Practices).
- Code review and static analysis.

C 17: Automated Security Testing

- Introduction to static application security testing (SAST) and dynamic application security testing (DAST).
- Tools and techniques for automated security testing.

C 18: Security Testing in CI/CD Pipelines

- Integrating security into continuous integration and continuous deployment (CI/CD) pipelines.
- Tools for security integration (e.g., GitLab CI, Jenkins with security plugins).

C 19: Penetration Testing for Applications

- Overview of penetration testing for applications.
- Planning and executing an application penetration test.

C 20: Secure Coding for Web and Mobile Applications

- Specific practices for web and mobile app security.
- Tools and techniques for securing web and mobile applications.

C 21: Review and Discussion

- Recap of secure development practices and tools.
- Q&A session.

C 22: Practical Exercise

- Implement security testing in a CI/CD pipeline and review the results.

Advanced Topics and Industry Trends

C 23: Secure Software Development Frameworks

- Overview of security frameworks and standards (e.g., NIST, ISO/IEC 27034).
- How to apply these frameworks.

C 24: Handling Security Incidents and Vulnerabilities

- Responding to security incidents in software.
- Managing and patching vulnerabilities.

C 25: Secure Code Review Practices

- Techniques for performing manual code reviews.
- Tools for code review (e.g., SonarQube).

C 26: Emerging Trends in Secure Software Development

- Trends and future directions (e.g., DevSecOps, zero trust).
- Emerging technologies and their security implications.

C 27: Secure Development Certification and Career Path

- Overview of relevant certifications (e.g., Certified Secure Software Lifecycle Professional (CSSLP)).
- Career development in secure software development.

C 28: Review and Discussion

- Comprehensive review of all topics covered.
- Q&A session.

C 29: Practical Exercise

- Conduct a secure code review and provide remediation recommendations.

C 30: Final Assessment and Wrap-Up

- Assessment quiz or project presentation.
- Final review and feedback session.

Wireless and Mobile Security (NCS2E)

Securing Wireless Networks

C 1: Introduction to Wireless Security

- Overview of wireless networks and their security challenges.
- Basic concepts (e.g., Wi-Fi, Bluetooth).

C 2: Wireless Network Protocols and Standards

- Understanding wireless protocols (e.g., IEEE 802.11, WPA/WPA2/WPA3).
- Differences and improvements in security standards.

C 3: Wireless Network Security Threats

- Common threats and vulnerabilities (e.g., eavesdropping, rogue access points).
- Examples of wireless network attacks.

C 4: Securing Wi-Fi Networks

- Best practices for securing Wi-Fi networks (e.g., strong encryption, secure configuration).
- Configuring WPA2/WPA3.

C 5: Wireless Network Security Tools

- Tools for monitoring and securing wireless networks (e.g., Aircrack-ng, Kismet).
- Introduction to wireless network analyzers.

C 6: Review and Discussion

- Recap of wireless network security concepts.
- Q&A session.

C 7: Practical Exercise

- Configure and secure a wireless network in a lab environment.

Advanced Wireless Security

C 8: Wireless Network Attacks and Defense

- Detailed look at attacks (e.g., deauthentication, man-in-the-middle).

- Techniques for defending against these attacks.

C 9: Wireless Intrusion Detection Systems (WIDS)

- Overview of WIDS.
- Implementing and configuring WIDS solutions.

C 10: Bluetooth Security

- Understanding Bluetooth security risks and vulnerabilities.
- Securing Bluetooth communications.

C 11: Securing IoT Devices

- Security considerations for IoT devices.
- Best practices for IoT security.

C 12: Securing Wireless Network Infrastructure

- Protecting network infrastructure (e.g., routers, access points).
- Security configurations for network devices.

C 13: Review and Discussion

- Recap of advanced wireless security topics.
- Q&A session.

C 14: Practical Exercise

- Perform a security assessment on a wireless network using tools and techniques learned.

Mobile Device Security

C 15: Introduction to Mobile Security

- Overview of mobile devices and their security challenges.
- Types of mobile devices (e.g., smartphones, tablets).

C 16: Mobile Operating Systems and Security Features

- Security features of major mobile operating systems (iOS, Android).
- Differences in security approaches.

C 17: Mobile Security Threats

- Common threats and vulnerabilities (e.g., malware, phishing, app vulnerabilities).

- Examples of mobile security incidents.

C 18: Mobile Device Management (MDM)

- Introduction to MDM solutions.
- Implementing and managing MDM policies.

C 19: Securing Mobile Applications

- Best practices for securing mobile apps.
- Understanding and mitigating app-specific vulnerabilities.

C 20: Mobile Security Tools

- Tools for securing and monitoring mobile devices (e.g., antivirus, app scanners).
- Introduction to mobile security assessment tools.

C 21: Review and Discussion

- Recap of mobile device security concepts.
- Q&A session.

C 22: Practical Exercise

- Configure and secure mobile devices using MDM solutions and security tools.

Advanced Mobile Security and Industry Trends

C 23: Advanced Mobile Security Topics

- Secure coding practices for mobile apps.
- Addressing advanced threats and vulnerabilities.

C 24: Mobile Security Best Practices

- Developing security policies for mobile device use.
- Educating users about mobile security.

C 25: Security for Mobile Payments and Banking

- Overview of mobile payment security.
- Securing mobile banking applications and transactions.

C 26: Emerging Trends in Mobile Security

- Trends and advancements (e.g., biometric security, 5G security).
- Impact of emerging technologies on mobile security.

C 27: Mobile Security Certification and Career Path

- Overview of relevant certifications (e.g., Certified Mobile Security Professional (CMSP)).
- Career opportunities in mobile security.

C 28: Review and Discussion

- Comprehensive review of wireless and mobile security topics.
- Q&A session.

C 29: Practical Exercise

- Conduct a comprehensive security assessment of a mobile application or device.

C 30: Final Assessment and Wrap-Up

- Assessment quiz or project presentation.
- Final review and feedback session.

Semester 3

Advanced Routing and Switching (NCS3A)

Advanced Routing Protocols

C 1: Introduction to Advanced Routing

- Overview of routing protocols and their role in network design.
- Key differences between static and dynamic routing.

C 2: OSPF (Open Shortest Path First) Basics

- Introduction to OSPF and its features.
- OSPF routing algorithm (Dijkstra's algorithm).

C 3: OSPF Configuration

- Configuring OSPF on routers.
- OSPF areas and their types (e.g., backbone, stub, totally stubby).

C 4: OSPF Advanced Topics

- OSPF route summarization.
- OSPF authentication and security.

C 5: OSPF Troubleshooting

- Common OSPF issues and their solutions.
- Tools and techniques for troubleshooting OSPF.

C 6: Review and Discussion

- Recap of OSPF concepts.
- Q&A session.

C 7: Practical Exercise

- Configure OSPF in a lab environment, including different OSPF areas and summarization.

Border Gateway Protocol (BGP)

C 8: Introduction to BGP

- Overview of BGP and its role in the Internet.
- BGP attributes and path selection.

C 9: BGP Configuration

- Basic BGP configuration.
- Understanding BGP neighbor relationships and peering.

C 10: Advanced BGP Features

- BGP route filtering and prefix lists.
- BGP route manipulation (e.g., AS path prepending, MED).

C 11: BGP Troubleshooting

- Common BGP issues and their solutions.
- Tools and techniques for troubleshooting BGP.

C 12: BGP Security

- BGP security best practices.
- Implementing BGP session protection and route validation.

C 13: Review and Discussion

- Recap of BGP concepts.
- Q&A session.

C 14: Practical Exercise

- Configure BGP in a lab environment, including advanced features like route filtering and manipulation.

Layer 3 Switching and Network Optimization

C 15: Introduction to Layer 3 Switching

- Difference between Layer 2 and Layer 3 switching.
- Benefits of Layer 3 switching.

C 16: Layer 3 Switching Configuration

- Configuring VLANs and inter-VLAN routing.
- Implementing Layer 3 switches and routing protocols on switches.

C 17: Advanced Layer 3 Switching

- Understanding and configuring routing protocols on switches (e.g., OSPF, EIGRP).
- Techniques for optimizing Layer 3 switching.

C 18: Network Optimization Techniques

- Overview of network optimization strategies (e.g., load balancing, QoS).
- Implementing Quality of Service (QoS) for optimizing network traffic.

C 19: Network Troubleshooting and Analysis

- Tools and techniques for network troubleshooting.
- Analyzing and optimizing network performance.

C 20: Review and Discussion

- Recap of Layer 3 switching and network optimization topics.
- Q&A session.

C 21: Practical Exercise

- Implement and troubleshoot Layer 3 switching in a lab environment.
- Configure QoS and other optimization techniques.

Advanced Topics and Integration

C 22: Multi-Protocol Label Switching (MPLS) Overview

- Introduction to MPLS and its benefits.
- Basic MPLS concepts and terminology.

C 23: MPLS Configuration and Deployment

- Configuring MPLS on routers.
- MPLS labels and forwarding.

C 24: Integration of Routing Protocols with MPLS

- Using OSPF and BGP with MPLS.
- MPLS VPNs and their applications.

C 25: Network Design Considerations

- Best practices for designing networks with advanced routing and switching.
- Scalability and redundancy considerations.

C 26: Security in Advanced Routing and Switching

- Securing routing protocols and switches.
- Implementing network security measures and best practices.

C 27: Review and Discussion

- Comprehensive review of all topics covered.
- Q&A session.

C 28: Practical Exercise

- Design and implement an advanced network incorporating MPLS, OSPF, BGP, and Layer 3 switching.

C 29: Final Assessment Preparation

- Review key concepts and prepare for final assessment.
- Address any remaining questions or issues.

C 30: Final Assessment and Wrap-Up

- Final assessment quiz or project presentation.
- Review results and provide feedback.

Virtualization and Cloud Security (NCS3B)

Virtualization Fundamentals and Virtual Networks

C 1: Introduction to Virtualization

- Overview of virtualization and its benefits.
- Types of virtualization (e.g., hardware, software, network).

C 2: Virtualization Technologies

- Key technologies (e.g., hypervisors: Type 1 vs. Type 2).
- Common virtualization platforms (e.g., VMware, Hyper-V, KVM).

C 3: Virtual Network Basics

- Concepts of virtual networks (e.g., virtual switches, VLANs).
- Configuring virtual networks in virtualization platforms.

C 4: Virtual Network Configuration

- Creating and managing virtual networks.
- Implementing network segmentation and isolation in virtual environments.

C 5: Virtual Network Security Best Practices

- Securing virtual networks (e.g., network segmentation, firewall rules).
- Implementing security controls in virtualized environments.

C 6: Review and Discussion

- Recap of virtualization and virtual network concepts.
- Q&A session.

C 7: Practical Exercise

- Configure virtual networks and apply security best practices in a lab environment.

Advanced Virtualization Security

C 8: Virtualization Security Threats

- Common threats and vulnerabilities in virtualization (e.g., VM escape, hypervisor attacks).
- Case studies of virtualization security incidents.

C 9: Securing Hypervisors

- Best practices for securing hypervisors.
- Configuring and managing hypervisor security settings.

C 10: Virtual Machine Security

- Securing virtual machines (VMs) and guest operating systems.
- Implementing VM hardening techniques.

C 11: Virtualization Management and Monitoring

- Tools for managing and monitoring virtualized environments.
- Implementing logging and auditing for virtualization.

C 12: Backup and Disaster Recovery for Virtual Environments

- Strategies for backup and disaster recovery in virtualized environments.
- Configuring and testing backup solutions.

C 13: Review and Discussion

- Recap of advanced virtualization security topics.
- Q&A session.

C 14: Practical Exercise

- Implement security measures for hypervisors and virtual machines in a lab setting.

Cloud Security Fundamentals

C 15: Introduction to Cloud Computing

- Overview of cloud computing models (e.g., IaaS, PaaS, SaaS).
- Cloud deployment models (e.g., public, private, hybrid).

C 16: Cloud Service Models and Security

- Security considerations for different cloud service models.
- Understanding shared responsibility models.

C 17: Cloud Security Threats and Risks

- Common threats and vulnerabilities in cloud environments (e.g., data breaches, misconfigurations).
- Examples of cloud security incidents.

C 18: Cloud Security Best Practices

- Implementing security controls in cloud environments.
- Best practices for securing cloud resources (e.g., identity and access management, encryption).

C 19: Cloud Network Security

- Configuring and securing cloud networks.
- Implementing network segmentation and security groups in cloud platforms.

C 20: Review and Discussion

- Recap of cloud security fundamentals.
- Q&A session.

C 21: Practical Exercise

- Configure and secure cloud resources, focusing on network security and access controls.

Advanced Cloud Security and Integration

C 22: Advanced Cloud Security Topics

- Securing cloud storage and databases.
- Implementing advanced security features (e.g., automated security policies, threat intelligence).

C 23: Cloud Compliance and Governance

- Understanding compliance requirements (e.g., GDPR, HIPAA).
- Implementing governance and compliance frameworks in cloud environments.

C 24: Cloud Security Tools and Services

- Overview of cloud security tools (e.g., Cloud Security Posture Management, Cloud Access Security Brokers).
- Evaluating and integrating cloud security services.

C 25: Cloud Incident Response and Management

- Developing an incident response plan for cloud environments.
- Tools and techniques for cloud incident management.

C 26: Cloud Security Certifications and Career Path

- Overview of relevant certifications (e.g., Certified Cloud Security Professional (CCSP)).
- Career development in cloud security.

C 27: Review and Discussion

- Comprehensive review of cloud security topics.
- Q&A session.

C 28: Practical Exercise

- Implement and test cloud security measures, including incident response scenarios.

C 29: Final Assessment Preparation

- Review key concepts and prepare for final assessment.
- Address any remaining questions or issues.

C 30: Final Assessment and Wrap-Up

- Final assessment quiz or project presentation.
- Review results and provide feedback.

Network Forensics (NCS3C)

Introduction to Network Forensics

C 1: Fundamentals of Digital Forensics

- Overview of digital forensics and its importance.
- Key concepts and terminology in digital forensics.

C 2: Digital Forensics Process

- Stages of the digital forensics process (e.g., acquisition, analysis, presentation).
- Legal and ethical considerations in digital forensics.

C 3: Network Forensics Basics

- Introduction to network forensics and its role in cybersecurity.
- Types of network data (e.g., packet data, log files).

C 4: Network Data Collection

- Methods for collecting network data (e.g., packet capture, network logs).
- Tools for network data collection (e.g., Wireshark, tcpdump).

C 5: Data Acquisition Techniques

- Techniques for acquiring network data without altering it.
- Best practices for ensuring data integrity.

C 6: Review and Discussion

- Recap of digital and network forensics fundamentals.
- Q&A session.

C 7: Practical Exercise

- Capture and analyze network traffic using Wireshark or similar tools.

Analyzing Network Data

C 8: Packet Analysis Fundamentals

- Understanding packet structure and protocols.
- Techniques for analyzing packet data.

C 9: Identifying Network Attacks

- Common network attacks (e.g., DDoS, man-in-the-middle, port scanning).
- Recognizing attack patterns in network data.

C 10: Log Analysis

- Importance of log files in network forensics.
- Techniques for analyzing and correlating log data.

C 11: Protocol Analysis

- Detailed analysis of network protocols (e.g., TCP, UDP, HTTP).
- Identifying anomalies and suspicious activity.

C 12: Forensic Tools for Analysis

- Overview of forensic analysis tools (e.g., X1 Social Discovery, NetworkMiner).
- Hands-on use of these tools for network forensic investigations.

C 13: Review and Discussion

- Recap of network data analysis techniques.
- Q&A session.

C 14: Practical Exercise

- Analyze captured network traffic to identify and investigate a simulated attack.

Incident Analysis and Response

C 15: Incident Response Overview

- Overview of incident response and its phases (e.g., preparation, detection, containment).
- Role of network forensics in incident response.

C 16: Incident Detection and Notification

- Techniques for detecting network incidents (e.g., IDS/IPS, SIEM).

- Managing incident notifications and alerts.

C 17: Incident Containment and Eradication

- Strategies for containing and mitigating network incidents.
- Techniques for eradication and remediation.

C 18: Evidence Preservation

- Importance of preserving evidence in network forensics.
- Techniques and tools for evidence preservation.

C 19: Incident Documentation and Reporting

- Documenting incident details and forensic findings.
- Creating and presenting incident reports.

C 20: Review and Discussion

- Recap of incident analysis and response techniques.
- Q&A session.

C 21: Practical Exercise

- Simulate an incident response scenario, including detection, containment, and reporting.

Advanced Topics and Integration

C 22: Advanced Forensic Techniques

- Techniques for advanced network forensics (e.g., deep packet inspection, flow analysis).
- Dealing with encrypted and obfuscated traffic.

C 23: Network Forensics in Cloud Environments

- Challenges and techniques for network forensics in cloud environments.
- Tools and methods for cloud-based network forensic investigations.

C 24: Legal Considerations and Chain of Custody

- Legal aspects of digital and network forensics.
- Ensuring the integrity of evidence through chain of custody procedures.

C 25: Integration with Other Security Measures

- Integrating network forensics with other security practices (e.g., threat hunting, security operations).

- Coordination with law enforcement and other agencies.

C 26: Emerging Trends in Network Forensics

- Latest trends and technologies in network forensics.
- Future directions and challenges in the field.

C 27: Review and Discussion

- Comprehensive review of all network forensics topics.
- Q&A session.

C 28: Practical Exercise

- Conduct a comprehensive forensic investigation, including advanced techniques and reporting.

C 29: Final Assessment Preparation

- Review key concepts and prepare for final assessment.
- Address any remaining questions or issues.

C 30: Final Assessment and Wrap-Up

- Final assessment quiz or project presentation.
- Review results and provide feedback.

Real World Network Application (NCS3D)

Network Design and Planning

C 1: Introduction to Network Design

- Overview of network design principles.
- Understanding network requirements and objectives.

C 2: Network Design Methodologies

- Common methodologies (e.g., Cisco's Design Lifecycle, OSI model).
- Design considerations (e.g., scalability, redundancy).

C 3: Requirements Gathering and Analysis

- Identifying business requirements and goals.

- Analyzing network traffic patterns and usage.

C 4: Designing Network Topologies

- Designing physical and logical network topologies (e.g., star, mesh, hybrid).
- Selecting appropriate hardware and technologies.

C 5: IP Addressing and Subnetting

- Designing an IP addressing scheme.
- Subnetting for efficient use of IP addresses.

C 6: Review and Discussion

- Recap of network design concepts and methodologies.
- Q&A session.

C 7: Practical Exercise

- Design a network topology for a hypothetical organization, including addressing and hardware.

Network Implementation

C 8: Network Hardware and Components

- Overview of network hardware (e.g., routers, switches, firewalls).
- Selecting and configuring network devices.

C 9: Network Configuration Basics

- Configuring network devices (e.g., setting up routers and switches).
- Basic configuration commands and best practices.

C 10: Implementing Network Services

- Configuring essential network services (e.g., DHCP, DNS).
- Setting up and managing VLANs and trunking.

C 11: Advanced Network Configuration

- Implementing advanced features (e.g., Quality of Service (QoS), routing protocols like OSPF and BGP).
- Configuring network redundancy (e.g., HSRP, VRRP).

C 12: Wireless Network Implementation

- Designing and implementing wireless networks.
- Configuring wireless access points and security settings.

C 13: Review and Discussion

- Recap of network implementation concepts.
- Q&A session.

C 14: Practical Exercise

- Implement a network based on the previously designed topology, including configuration of routers, switches, and network services.

Network Security

C 15: Introduction to Network Security

- Overview of network security principles and practices.
- Common security threats and vulnerabilities.

C 16: Securing Network Devices

- Best practices for securing network devices (e.g., routers, switches).
- Implementing access controls and management protocols.

C 17: Firewall and Intrusion Prevention Systems

- Configuring and managing firewalls.
- Implementing intrusion prevention and detection systems (IPS/IDS).

C 18: Network Access Control (NAC)

- Implementing network access control policies.
- Configuring NAC solutions to enforce security policies.

C 19: Virtual Private Networks (VPNs)

- Setting up and securing VPNs.
- Types of VPNs (e.g., site-to-site, remote access) and their configurations.

C 20: Security Monitoring and Logging

- Implementing network monitoring and logging solutions.
- Analyzing logs and detecting anomalies.

C 21: Review and Discussion

- Recap of network security topics and practices.
- Q&A session.

C 22: Practical Exercise

- Secure the previously implemented network, including configuration of firewalls, VPNs, and access control.

Real-World Scenarios and Advanced Topics

C 23: Incident Response and Management

- Introduction to incident response.
- Developing and implementing an incident response plan.

C 24: Security Assessments and Penetration Testing

- Conducting security assessments and penetration tests.
- Tools and techniques for network security testing.

C 25: Disaster Recovery and Business Continuity

- Planning for disaster recovery and business continuity.
- Implementing backup and recovery solutions.

C 26: Integration with Cloud Services

- Securing network infrastructure in cloud environments.
- Configuring cloud-based security services and integrations.

C 27: Emerging Trends and Technologies

- Overview of emerging trends (e.g., SD-WAN, zero trust architecture).
- Assessing the impact of new technologies on network design and security.

C 28: Review and Discussion

- Comprehensive review of all topics covered.
- Q&A session.

C 29: Final Practical Project

- Design, implement, and secure a network infrastructure based on a real-world scenario.
- Include all elements from design to security.

C 30: Final Assessment and Wrap-Up

- Final assessment quiz or project presentation.
- Review results, provide feedback, and discuss next steps for continued learning.

Emerging Trends in Cyber Security (NCS3E)

Current Trends in Cybersecurity

C 1: Overview of Cybersecurity Trends

- Introduction to current trends in cybersecurity.
- Impact of trends on businesses and individuals.

C 2: Ransomware and Extortion

- Understanding the rise of ransomware attacks.
- Case studies of recent ransomware incidents and their impact.

C 3: Threat Intelligence and Threat Hunting

- Importance of threat intelligence in modern cybersecurity.
- Techniques and tools for threat hunting.

C 4: Zero Trust Architecture

- Overview of Zero Trust principles.
- Implementing a Zero Trust model in organizations.

C 5: Cloud Security Trends

- Emerging trends in cloud security.
- Securing cloud environments and cloud-native applications.

C 6: Review and Discussion

- Recap of current cybersecurity trends.
- Q&A session.

C 7: Practical Exercise

- Analyze recent cybersecurity incidents related to trends discussed.

Future Trends in Cybersecurity

C 8: AI and Machine Learning in Cybersecurity

- Role of AI and machine learning in detecting and responding to threats.
- Applications and limitations of AI in cybersecurity.

C 9: Blockchain Technology and Security

- Understanding blockchain and its applications in cybersecurity.
- Potential and challenges of blockchain for securing digital assets.

C 10: Quantum Computing and Its Impact

- Introduction to quantum computing.
- Potential impact of quantum computing on encryption and cybersecurity.

C 11: Internet of Things (IoT) Security

- Security challenges associated with IoT devices.
- Strategies for securing IoT networks and devices.

C 12: Privacy Enhancements and Regulations

- Upcoming privacy regulations (e.g., GDPR, CCPA).
- Future trends in data privacy and protection.

C 13: Review and Discussion

- Recap of future cybersecurity trends.
- Q&A session.

C 14: Practical Exercise

- Explore emerging technologies and their potential impact on cybersecurity.

Industry Best Practices

C 15: Building a Strong Security Culture

- Importance of security awareness and training.
- Developing and maintaining a strong security culture within organizations.

C 16: Risk Management Frameworks

- Overview of risk management frameworks (e.g., NIST, ISO 27001).
- Implementing risk management practices in an organization.

C 17: Incident Response and Management

- Best practices for incident response and management.
- Developing and testing an incident response plan.

C 18: Security Governance and Compliance

- Importance of governance and compliance in cybersecurity.
- Understanding key compliance requirements and frameworks.

C 19: Secure Development Practices

- Incorporating security into the software development lifecycle.
- Best practices for secure coding and application security.

C 20: Review and Discussion

- Recap of industry best practices.
- Q&A session.

C 21: Practical Exercise

- Develop an incident response plan or perform a risk assessment.

Continuous Learning and Professional Development

C 22: Continuous Learning Strategies

- Importance of continuous learning in cybersecurity.
- Resources for staying updated (e.g., blogs, webinars, courses).

C 23: Industry Certifications and Their Value

- Overview of key cybersecurity certifications (e.g., CISSP, CISM, CEH).
- Choosing certifications based on career goals.

C 24: Networking and Professional Development

- Importance of professional networking in cybersecurity.
- Participating in cybersecurity communities and events.

C 25: Emerging Career Opportunities in Cybersecurity

- Exploring new career paths and roles in cybersecurity.
- Skills and qualifications needed for emerging roles.

C 26: Developing a Personal Learning Plan

- Creating a personal plan for continuous learning and career development.
- Setting goals and tracking progress.

C 27: Review and Discussion

- Comprehensive review of continuous learning strategies.
- Q&A session.

C 28: Practical Exercise

- Develop a personal learning plan or create a career development roadmap.

C 29: Final Assessment Preparation

- Review key concepts from trends, best practices, and continuous learning.
- Prepare for final assessment or project presentation.

C 30: Final Assessment and Wrap-Up

- Final assessment quiz or project presentation.
- Review results and discuss next steps for continued growth in cybersecurity.

Semester 4 (Cyber Security Option) only this below for the entire level 4.

Introduction to Ethical Hacking (NCS4D1)

C 1: Understanding Ethical Hacking

- Definition and objectives.
- Differences between ethical hacking and malicious hacking.
- Ethical hacking's role in cybersecurity.

C 2: Legal and Ethical Considerations

- Laws and regulations (e.g., Computer Fraud and Abuse Act, GDPR).
- Importance of authorization and contracts.
- Code of conduct and ethical guidelines.

C 3: Ethical Hacking Frameworks and Standards

- Overview of frameworks (e.g., NIST, OWASP).
- Understanding standards and best practices.

C 4: Tools and Techniques Overview

- Common tools used in ethical hacking (e.g., Nmap, Metasploit, Burp Suite).
- Introduction to basic techniques (e.g., reconnaissance, scanning).

C 5: Setting Up a Penetration Testing Lab

- Creating a safe testing environment using virtual machines.
- Configuring tools and resources.

C 6: Review and Discussion

- Recap of ethical hacking fundamentals.
- Q&A session.

C 7: Practical Exercise

- Set up a basic penetration testing lab environment.

Reconnaissance and Scanning (NCS4D2)

C 8: Reconnaissance (Footprinting)

- Techniques for gathering information (e.g., WHOIS, DNS, social media).
- Tools for reconnaissance (e.g., Maltego, Recon-ng).

C 9: Network Scanning

- Methods for scanning networks (e.g., port scanning, service detection).
- Tools for network scanning (e.g., Nmap).

C 10: Vulnerability Scanning

- Identifying vulnerabilities using automated tools.
- Tools for vulnerability scanning (e.g., Nessus, OpenVAS).

C 11: Enumeration

- Techniques for extracting detailed information about a target (e.g., user accounts, network shares).
- Tools for enumeration (e.g., enum4linux, SNMPWalk).

C 12: OSINT (Open Source Intelligence)

- Techniques for gathering information from open sources.
- Tools and resources for OSINT.

C 13: Review and Discussion

- Recap of reconnaissance and scanning techniques.
- Q&A session.

C 14: Practical Exercise

- Perform a reconnaissance and scanning exercise on a controlled environment.

Exploitation and Post-Exploitation (NCS4D3)

C 15: Exploitation Techniques

- Understanding different types of exploits (e.g., buffer overflow, SQL injection).
- Introduction to exploit frameworks (e.g., Metasploit).

C 16: Metasploit Framework

- Overview of Metasploit functionalities.
- Basic usage and common modules.

C 17: Post-Exploitation

- Techniques for maintaining access (e.g., creating backdoors).
- Privilege escalation methods.

C 18: Web Application Hacking

- Common web vulnerabilities (e.g., XSS, CSRF, SQL Injection).
- Tools for web application testing (e.g., Burp Suite, OWASP ZAP).

C 19: Wireless Network Hacking

- Techniques for attacking wireless networks (e.g., WPA/WPA2 cracking).
- Tools for wireless network testing (e.g., Aircrack-ng).

C 20: Social Engineering

- Techniques for manipulating individuals (e.g., phishing, pretexting).
- Defending against social engineering attacks.

C 21: Review and Discussion

- Recap of exploitation, post-exploitation, and advanced hacking techniques.
- Q&A session.

C 22: Practical Exercise

- Perform exploitation and post-exploitation tasks in a controlled environment.

Reporting and Professional Development (NCS4D4)

C 23: Writing Penetration Testing Reports

- Structure and content of a penetration testing report.
- Best practices for documenting findings and recommendations.

C 24: Presentation Skills

- Communicating findings to different audiences (technical and non-technical).
- Crafting an effective presentation.

C 25: Remediation and Follow-Up

- Assisting organizations with remediation.
- Retesting after fixes have been applied.

C 26: Ethical Hacking Certifications

- Overview of certifications (e.g., CEH, OSCP).
- Certification requirements and preparation tips.

C 27: Career Paths in Ethical Hacking

- Exploring career opportunities.
- Skills and qualifications needed.

C 28: Review and Discussion

- Comprehensive review of ethical hacking concepts and practices.
- Q&A session.

C 29: Practical Exercise

- Prepare and present a complete penetration testing report based on a hypothetical scenario.

C 30: Final Assessment and Wrap-Up

- Assessment quiz or project presentation.
- Final review and feedback session.

Week 1: Current Trends in Cybersecurity (NCS4D5)

C 1: Overview of Cybersecurity Trends

- Introduction to current trends in cybersecurity.
- Impact of trends on businesses and individuals.

C 2: Ransomware and Extortion

- Understanding the rise of ransomware attacks.
- Case studies of recent ransomware incidents and their impact.

C 3: Threat Intelligence and Threat Hunting

- Importance of threat intelligence in modern cybersecurity.
- Techniques and tools for threat hunting.

C 4: Zero Trust Architecture

- Overview of Zero Trust principles.
- Implementing a Zero Trust model in organizations.

C 5: Cloud Security Trends

- Emerging trends in cloud security.
- Securing cloud environments and cloud-native applications.

C 6: Review and Discussion

- Recap of current cybersecurity trends.
- Q&A session.

C 7: Practical Exercise

- Analyze recent cybersecurity incidents related to trends discussed.

Week 2: Future Trends in Cybersecurity (NCS4D6)

C 8: AI and Machine Learning in Cybersecurity

- Role of AI and machine learning in detecting and responding to threats.
- Applications and limitations of AI in cybersecurity.

C 9: Blockchain Technology and Security

- Understanding blockchain and its applications in cybersecurity.
- Potential and challenges of blockchain for securing digital assets.

C 10: Quantum Computing and Its Impact

- Introduction to quantum computing.
- Potential impact of quantum computing on encryption and cybersecurity.

C 11: Internet of Things (IoT) Security

- Security challenges associated with IoT devices.
- Strategies for securing IoT networks and devices.

C 12: Privacy Enhancements and Regulations

- Upcoming privacy regulations (e.g., GDPR, CCPA).
- Future trends in data privacy and protection.

C 13: Review and Discussion

- Recap of future cybersecurity trends.
- Q&A session.

C 14: Practical Exercise

- Explore emerging technologies and their potential impact on cybersecurity.

Week 3: Industry Best Practices **(NCS4D7)**

C 15: Building a Strong Security Culture

- Importance of security awareness and training.
- Developing and maintaining a strong security culture within organizations.

C 16: Risk Management Frameworks

- Overview of risk management frameworks (e.g., NIST, ISO 27001).

- Implementing risk management practices in an organization.

C 17: Incident Response and Management

- Best practices for incident response and management.
- Developing and testing an incident response plan.

C 18: Security Governance and Compliance

- Importance of governance and compliance in cybersecurity.
- Understanding key compliance requirements and frameworks.

C 19: Secure Development Practices

- Incorporating security into the software development lifecycle.
- Best practices for secure coding and application security.

C 20: Review and Discussion

- Recap of industry best practices.
- Q&A session.

C 21: Practical Exercise

- Develop an incident response plan or perform a risk assessment.

Week 4: Continuous Learning and Professional Development (NCS4D8)

C 22: Continuous Learning Strategies

- Importance of continuous learning in cybersecurity.
- Resources for staying updated (e.g., blogs, webinars, courses).

C 23: Industry Certifications and Their Value

- Overview of key cybersecurity certifications (e.g., CISSP, CISM, CEH).
- Choosing certifications based on career goals.

C 24: Networking and Professional Development

- Importance of professional networking in cybersecurity.
- Participating in cybersecurity communities and events.

C 25: Emerging Career Opportunities in Cybersecurity

- Exploring new career paths and roles in cybersecurity.
- Skills and qualifications needed for emerging roles.

C 26: Developing a Personal Learning Plan

- Creating a personal plan for continuous learning and career development.
- Setting goals and tracking progress.

C 27: Review and Discussion

- Comprehensive review of continuous learning strategies.
- Q&A session.

C 28: Practical Exercise

- Develop a personal learning plan or create a career development roadmap.

C 29: Final Assessment Preparation

- Review key concepts from trends, best practices, and continuous learning.
- Prepare for final assessment or project presentation.

C 30: Final Assessment and Wrap-Up

- Final assessment quiz or project presentation.
- Review results and discuss next steps for continued growth in cybersecurity.