**Week 1-2: Introduction to Network Assets and Threat Analysis**

* Overview of network assets and their significance
* Introduction to threat analysis methodologies
* Identifying common vulnerabilities in network assets
* Risk assessment and risk management in the context of cybersecurity

**Week 3-4: Security Services and Physical/Logical Security**

* Understanding core security services (confidentiality, integrity, availability)
* Implementing physical security measures for network infrastructure
* Configuring logical security measures such as firewalls and intrusion detection systems
* Establishing and enforcing security policies and procedures

**Week 5-6: Protection in Operating Systems**

* Securing various operating systems (Windows, Linux, macOS)
* User account management and access control
* File system security practices
* Patch management, updates, and vulnerability mitigation

**Week 7: Network Access Model and Passwords**

* In-depth exploration of network access control models (RBAC, MAC, DAC)
* Best practices for password policies and management
* Multi-factor authentication and its implementation

**Week 8: Biometrics and Authorization Policies**

* Understanding biometric authentication technologies
* Designing and implementing effective authorization policies
* Role-based access control (RBAC) implementation

**Week 9: Programmed Threats and Database Security**

* Analyzing programmed threats (viruses, worms, Trojans)
* Strategies for securing databases and sensitive information
* Access control and encryption in database security

**Week 10: Private Network Security Policies, Firewalls, and Virtual Private Networks (VPNs)**

* Developing private network security policies
* Configuring and managing firewalls for network security
* Implementing and securing Virtual Private Networks (VPNs)
* Bonus Topics (integrated throughout the course):
* Message Confidentiality
* Message Authentication, Integrity, and Non-repudiation
* Digital signatures and public-key certificates
* Mutual authentication
* Distributed authentication systems (e.g., Kerberos)
* Email Security
* Web Security
* Administering Security
* Legal and Ethical Issues in Cybersecurity