

HIGHER NITEC IN CYBER & NETWORK SECURITY (2 YEARS)

CERTIFICATION

Credits required for certification:

Sector Foundation Modules	: 3
Cluster Core Modules	: 18
Specialisation Modules	: 26
Life Skills Modules	: 9
Cross Disciplinary Core Modules	: 6
Electives	: 6
Total	: 68

COURSE STRUCTURE

Module Title	Credits
SECTOR FOUNDATION MODULES	
Networking Fundamentals	3
CLUSTER CORE MODULES	
System Software Essentials	3
Computer Maintenance	3
Networking Technology	3
Enterprise Networking	3
System Administration	3
System Hardening & Infrastructure Services	3
SPECIALISATION MODULES	
Container Security	3
Cloud Security	3
Infrastructure Security	3
IT Security	3
Security Operations	3
Security Vulnerability Testing	3
Internship Programme	8
ELECTIVES (GENERAL) AND LIFE SKILLS MODULES	
For details, click here	

Note: The offer of electives is subject to the training schedule of respective ITE Colleges. Students are advised to check with their Class Advisors on the availability of the elective modules they intend to pursue.

MODULE OBJECTIVES

Sector Foundation Modules

Networking Fundamentals

On completion of the module, students should be able to set up, configure, set up and troubleshoot wired and wireless network system for small office environment. They should be able to provide network support and configure network devices.

Cluster Core Modules

System Software Essentials

On completion of the module, students should be able to install and configure operating system (OS) and application software on end user computing devices. In addition, they should also be able to perform OS maintenance and troubleshooting.

Computer Maintenance

On completion of the module, students should be able to perform installation and configuration of hardware components and peripherals of end user computing devices. In addition, they should also be able to perform end user computing devices maintenance and troubleshooting of hardware problems.

Networking Technology

On completion of the module, students should be able to apply the fundamentals of computer networking in relation to the OSI model. They should also be able to configure and set up wired and wireless local area network (LAN) including network segmentation. Students will also be able to perform network documentation and monitor network performance.

Enterprise Networking

On completion of the module, students should be able to configure and set up a switched and routed network with Virtual LANs (VLANs) as well as set up a wide area network (WAN), implement access control lists and troubleshoot common network issues and problems.

System Administration

On completion of the module, students should be able to set up server operating systems and perform system administration tasks such as user management, resource management and performance monitoring. Students should also be able to configure file server services and implement basic system security.

System Hardening & Infrastructure Services

On completion of the module, students should be able to perform server security hardening and manage infrastructure services. Students should also be able to automate server administration and implement high-availability systems.

Specialisation Modules

Container Security

On completion of the module, students should be able to administer container and virtualisation platforms and its associated services, as well as to monitor resource utilisation, diagnose and resolve performance and connectivity issues, and to secure containerised infrastructures.

Cloud Security

On completion of the module, students should be able to administer cloud platform and its associated services, monitor resource utilisation on the hypervisor, troubleshoot performance and connectivity issues as well as secure the cloud resources. They will also be introduced to commercially available cloud services, including containers and be able to utilise them.

Infrastructure Security

On completion of the module, students should be able to configure firewall appliances, intrusion detection and prevention systems, firewall policies and configure edge network

security. They should also be able to implement appropriate technologies to protect against security attacks such as spams, spyware and worms/viruses including the set-up of end-point security measures.

IT Security

On completion of the module, students should be able to implement detection, manage, and monitor security threats by configuring firewall, wireless LAN, extracting system logs, setting up a Certificate Authority server, and managing privilege identity access.

Security Operations

On completion of the module, students should be able to take up tasks in the Security Operations Centre (SOC) environment including monitoring and identifying security risks, analysing and classifying security risks through security monitoring systems. They should also be able to apply appropriate counter measures to mitigate identified threats.

Security Vulnerability Testing

On completion of the module, students should be able to perform system and network scanning, vulnerability assessment and documentation of identified vulnerabilities. They should also be able to perform basic penetration testing and prepare appropriate test documentation.

Internship Programme

On completion of the modules, students should be able to integrate and apply a cluster of key technical, social and methodological competencies related to their field of study.

Electives (General) and Life Skills Modules

For details, click [here](#).