HIGHER NITEC IN CYBER & NETWORK SECURITY (2 YEARS)

Core 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 devices such as switches and wireless access points.

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.

Virtualisation Fundamentals
On completion of the module, students should be able to set up virtualisation server and environment. They should also be able to perform backup and recovery of VMs for fault tolerance. They should be able to perform basic troubleshooting with hypervisor and VMs.

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

Specialisation Modules

Infrastructure Security
On completion of the module, students should be able to configure firewall appliances, intrusion detection and prevention systems, firewall policies and set up Virtual Private Networks. 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 perform network intrusion detection, prevention and mitigation through the implementation of intrusion detection system. They should also be able to implement a secure network using Public Key Infrastructure technologies and set up a secure wireless network, as well as perform privilege identity management support functions.

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.

Industry Attachment

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.