PROFESSIONAL MODULE - ETHICAL HACKING

This Professional Module - Ethical Hacking program will immerse participants in an interactive environment where they will learn to think and act like ethical hackers. Through practical labs, students will learn how to scan, test, and secure networks using real-world attack and defense techniques. The course covers essential concepts such as penetration testing, vulnerability assessment, and security auditing. Participants will gain hands-on experience in identifying security threats, exploiting vulnerabilities, and implementing countermeasures to protect systems and networks. By the end of the training, participants will have a comprehensive understanding of ethical hacking methodologies and hands-on expertise in cybersecurity defense mechanisms.

Audience : This course is designed for IT professionals, system administrators, cybersecurity enthusiasts, students, penetration testers, and law enforcement experts. It provides hands-on training in ethical hacking, security defense, and forensic analysis to strengthen cybersecurity skills.

Key Benefits : At the end of the training, participants will establish and govern minimum standards for credentialing professional information security standards in the security domain.

Duration : 6 months

Course Content

A+ : Basics of Computer Hardware

- Motherboard – Purpose, components, form factors.
- Processor – Types, functions, clock speed, cores.
- Storage Devices – HDD, SSD, NVMe, external storage.
- Memory Devices – RAM types, cache, memory hierarchy.
- Video Technologies – GPUs, display interfaces, refresh rates.
- Other Components – Cooling systems, expansion cards, peripherals.
- Virtualization & Monitoring – Hypervisors, resource allocation, PSU intro.
- Power Supply & Troubleshooting – Wattage, connectors, failure diagnosis.
- Wireless & Mobile Components – Wi-Fi cards, webcams, mobile displays.
- Live Lab Practice – Hands-on with hardware.
- Assignments & A+ Assessment

N+ : Basics of Computer Networks

- Command Prompt & OS – Basic networking commands, OS types.
- Operating System – Network settings, command-line networking tools.
- Network Types & Topology – LAN, WAN, MAN, bus, star, mesh.
- Transmission Media & Devices – Ethernet, fiber optics, switches, routers.
- Service Models & Wireless Networks – 2G-5G, cloud services.
- DSL & ONT – Broadband types, Wi-Fi analyzers.

- Cloud & Virtualization – SaaS, PaaS, IaaS, desktop virtualization.
- Protocols & Encryption – HTTP, FTP, TLS, VNC basics.
- Remote Management – RMM, MSRA, third-party tools.
- Load Balancers & Troubleshooting – Network congestion, common issues.
- Assignments & N+ Assessment

CCNA : Routing & Switching

- OSI & TCP/IP Model – Layers, functions, protocols.
- TCP & UDP – Differences, use cases.
- IP Addressing – IPv4/IPv6, classes, subnet masks.
- Subnetting – CIDR, VLSM, hands-on practice.
- Routers – Intro, Packet Tracer (PT) practice.
- Routing – Static vs. Dynamic, configuration in PT.
- Switches & VLANs – Basics, setup in PT.
- Port Security & ACLs – Standard ACL configuration.
- Extended ACL & BGP – Advanced filtering, routing.
- NAT & Telnet – Address translation, remote access.
- DHCP & PAT – IP allocation techniques.
- Router & Switch Lab – Real-time configuration.
- Modem Lab – Practical modem setup.
- Network Protocols – FTP, SMTP, SSH, SMB, SNMP.
- Firewall & Security – Configuring basic firewalls.
- DNS & VPN – Name resolution, secure tunnels.
- Networking Concepts – MTU, MSS, GRE Tunneling.
- CDN & DNS – Load balancing, fast flux DNS.
- Streaming & Video Encoding – HLS, MPEG-DASH.
- Network Security & Tools – Common threats, mitigation.
- Seminar & Assignment Submission
- Assessment 1 - Theory
- Assessment 2 - Practical

MCSE (Latest - Windows Server)

- Installing and configuring Windows Server.
- Managing Windows Server roles and features.
- Configuring virtualization with Hyper-V.
- Implementing Active Directory Domain Services (AD DS).
- Managing users, groups, and organizational units in AD DS.
- Configuring Group Policy for security and automation.
- Implementing DHCP, DNS, and IP Address Management (IPAM).
- Managing file and storage solutions.
- Configuring remote access and VPN solutions.
- Implementing Windows Server security features.
- Configuring high availability with clustering and load balancing.
- Managing Windows Server updates and patching.
- Monitoring and optimizing server performance.

- Implementing backup, disaster recovery, and failover strategies.
- Integrating Windows Server with cloud services (Azure AD, hybrid setups).

Linux Fundamentals

- Introduction to Linux – OS comparison, distros.
- Installation & Boot Process – GRUB, startup sequence.
- Filesystem & Directories – /home, /etc, /var, permissions.
- Basic Commands – Navigation, file handling, search.
- User & Group Management – Adding, deleting, modifying users.
- Process & Job Management – Monitoring, killing, scheduling.
- Git & GitHub – Setup, commits, CLI usage.
- Python & Package Management – Pip, virtual environments.
- XAMPP & Web Hosting – Apache, MySQL, PHP setup.
- Web Servers (Nginx & Apache) – Hosting, SSL, reverse proxy.
- File Sharing (Samba & FTP) – Network file transfers.
- Software Management – Package installation via apt, yum, dnf.
- Linux Security – Firewalls, SSH hardening, fail2ban.
- Backup & Storage – Disk partitioning, rsync, tar.
- Automation & Scripting – Bash scripts, cron jobs.

Ethical Hacking

- Introduction to Ethical Hacking.
- Footprinting and Reconnaissance techniques.
- Scanning networks for vulnerabilities.
- Enumeration of system resources.
- Exploiting system vulnerabilities (System Hacking).
- Understanding Trojans and Backdoors.
- Identifying and analyzing Viruses and Worms.
- Packet sniffing and network monitoring (Sniffers).
- Social Engineering attack techniques.
- Conducting Denial of Service (DoS) attacks.
- Exploiting and preventing Session Hijacking.
- Attacking and securing web servers.
- Hacking and securing web applications.
- Performing SQL Injection attacks.
- Attacking and securing wireless networks.
- Hacking vulnerabilities in mobile platforms.
- Evading IDS, Firewalls, and Honeypots.
- Understanding and applying Cryptography.
- Conducting penetration testing methodologies.
- Reporting and documenting security assessments.