Six Months Free Course

Certificate in Cybersecurity

Offered by: UET Peshawar Jalozai Campus

Venue: UET Peshawar (Hayatabad Campus/Jalozai campus)

Registration process takes less than two minutes
(See the end of this documents for guidelines)

Trade Name: Certificate in Cybersecurity

Trade Description: Study of Cybersecurity with emphasis on Ethical Hacking and Network Defense

Trade/Course Content:

Module 1: Introduction to Cybersecurity: What is cybersecurity, different domains of cybersecurity (Security Management, Identity and Access Management, Security Engineering, Business Continuity, Compliance, Cryptography, Physical Security, Software Development Security, Security Operations), Brief intro to Cyber Defence technologies, System Design, Administration and Automation, Digital Forensics, Threat hunting and Incident response, Ethical Hacking and Pentesting.

Module 2: Overview of Ethical Hacking: What is Hacking, Hacking versus Ethical hacking, History of Hacking, Phases of Hacking (Reconnaissance, Scanning, Gaining access, Maintaining access, Exfiltrating data and Clearing tracks), different certifications for ethical hackers.

Module 3: Review of relevant networking and Information security concepts: What is a network, Types of network, Network topologies(Physical and Logical), Network Models (OSI Model versus TCP/IP), Network addressing (IP addresses and their parts and types), Network Protocols (HTTP, HTTPS, DNS, FTP, SMTP, DHCP, ICMP, SSH, ARP etc), Routing and Forwarding in Networks, Introduction to Network security, Important concepts and definitions (Threat versus Vulnerability versus Risk, Authenticity, Integrity, Availability, Confidentiality, Non-repudiation, Technology triangle, Defence in depth :Uniform, Protected Enclaves, Information centric and Vector oriented, Ethical hacking versus Pentesting versus Red teaming versus Security Audits versus Vulnerability Assessment etc**)**

Module 4: Categorization of threats and attack vectors: Description of Attack surface and attack vectors, Host based Attacks, Network based attacks, Physical attacks, Application based attacks, Social engineering etc, Introduction to Kill chain, Phases in Kill Chain (Reconnaissance, Weaponization, Payload Delivery, Exploitation, backdoor Installation and Privilege escalation, Setup of Command and control infrastructure, Post Exploitation activity such as Data corruption, Data Exfiltration etc)

Module 5: Phases of Attack (1. Reconnaissance): What is Reconnaissance, Why it is needed, Types of Reconnaissance, Tools of Reconnaissance, Practical Examples, Reconnaissance countermeasures.

Module 6: Phases of Attack (2. Scanning, Enumeration and Vulnerability Assessment) What is network Scanning, Why network scanning, Types of network scanning, Tools and techniques for network scanning (Understanding the 3 way handshake, Understanding different port states, use of nmap in figuring out live systems and their identification, use of nmap for discovering open ports and services that are currently running on the target system/network, Specific nmap scans, why, when and where they are used (Full scans, half scans, XMAS scans, FIN scans, NULL scans, UDP scans, IDLE scans for evading IDS etc) Countermeasures), Banner grabbing and OS fingerprinting (using Telnet and netcat), countermeasures, Enumeration using defaults and NetBIOS, Enumeration using SNMP, Enumeration using LDAP, Enumeration via NTP, Enumeration using SMTP, Enumeration via DNS, Countermeasures.

Module 7: Phases of Attack (3. Gaining access and Post Exploitation Kung-Fu) Methods of gaining access, Social engineering, Client side attacks, Server side attacks, Use of Exploitation platforms (BEEF, Metasploit, COBALSTRIKE, CANVAS etc), Intro to Metasploit, Metasploit Modules (Exploits, Payloads, Encoders, Auxillary, POST, NOPS), Metasploit Payloads (Single, Stagers, Stage) and their examples, Antivirus evasion techniques, Custom Payload Design, Payload Obfuscation, Payload Testing on different architectures and different Operating systems and against different defences such as AV, E2EP, IDS, IPS etc, In-depth study of Msfconsole, Meterpreter and its various scripts, Armitage, Privilege Escalation, Persistence, Use of Command-line, Powershell and wmic etc),

Module 8: Phases of Attack (4. Data Exfiltration and Covering tracks) Different techniques for data exfiltration (Using USB devices, Using email/FTP Servers/Instant Messaging, Using Protocols such as HTTPS/ARP/DNS etc, Using Wireless devices etc), pivoting, hiding malicious files, disabling audits, changing logs etc),

Module 9: Brief intro to Wireless pentesting, Web Application pentesting and Malware Analysis

Module 10: Pentesting of Embedded System such a router/beaglebone black (Understanding the Firmware and its components [bootloader and its stages, Kernel and device tree, Root File system and busybox], Firmware extraction, Firmware analysis and modification, Firmware rebuilding and installation on the target device.

Module 11: Pentesting using python Writing in python: network scanner, protocol spoofers, packet sniffer, vulnerability scanner, payload etc. and finally **Incident Handling and Response.**

Trade/Course Learning Outcomes:

After successful completion of this course, students will have:

- An in-depth understanding of the tools, techniques and procedures used by hackers.
- Hands-on experience of protecting a network against different types of attacks.

Recommended Books:

1) Hands-On Ethical Hacking and Network Defense, Second Edition by Michael T. Simpson, Kent Backman, and James Corley, ISBN:1133935613
2) Hacking the art of exploitation, Second Edition by Jon Erickson, ISBN:1593271442
3) Ethical Hacking and Penetration Testing Guide by Rafay Baloch, ISBN:9781482231625

Registration Process

Step No. 1: Please go to the following link
https://navttc.kamyabjawan.gov.pk/frmCandidateRegistration.aspx

Step No. 2: Enter your NIC and fill the rest of the form.

Step No. 3: Under the heading “Trade Apply For/Fill Attributes”, Select Nowshera for “District” and “UET Peshawar Jalozai Campus” for the “Institute Name”

Step No. 4: Select “Certificate for Cyber Security “ for the “Trade Applied for”

Step No. 5: Fill the rest of the form, and press Save Button.