Government of Pakistan

National Vocational and Technical Training Commission

Prime Minister Hunarmand Pakistan Program,

"Skills for All"

Course Contents/ Lesson Plan

Course Title: Certificate in Cyber Security

Duration: 6 Months

Plot no. 38, Kirthar Road, H-9 Islamabad
051-9044250

Trainer Name	
Course Title	Certificate in Cyber Security
Objective of Course	To prepare the trainees to work as Information Security Professional in a wide variety of computer-related industries and has a strong emphasis on Network related problems
Learning Outcome of the Course	**Knowledge Proficiency Details** • Knowledge of Information technology catering principles and Capabilities with particular -emphasis on the technical support of local area networks. • Knowledge of securing networks, systems, servers and operating Systems with troubleshooting. • Knowledge of the web attacks in modern day servers **Skills Proficiency Details** • Hands on experience in pentesting all network technologies regardingwith local area network. • Perform various tests to detect and provide defense against vulnerabilities. • Practical scenarios to compromise web servers and web applications. • Ability to detect attack vectors, identify attack type and provide continuity of operations. • Ability to recover data from damaged disks to ensure data consistency. • Capable of malware analysis to detect basic working of malwares. • Pentesting mobile devices and applications.
Course Execution Plan	Total Duration of Course: 6 Months (26 Weeks)
	Class Hours: 4 Hours per day
	Theory: 30% Practical: 70%
	Weekly Hours: 20 Hours Per week
	Total Contact Hours: 520 Hours
Companies Offering Jobs in the respective trade	• Trillium • Afinity • NetSole • I2c • Multinet • Nescom • Transworld • Netcom • Systems • Web Work Solution • Purelogics
Job Opportunities	Security Operations Centre (SOC) Engineer • Network Administrator

	• IT Support Officer • Manager / Assistant Manager IT • Network support engineer • Security Analysts • Penetration tester
No of Students	25
Learning Place	Classroom/Lab ITU
Instructional Resources	• Libirary • Elibrary from HEC • Digital Libarary of ITU

Scheduled Week	Module Title	Learning Units	Remarks
Week 1	➢ Introduction	• **Motivational Lecture** • **Course Introduction** • **Success stories** • **Job market** • **Course Applications** • **Institute/work ethics** • Introduction to Cybersecurity • Objectives • Roles • Differences between Information security and cybersecurity • What is Cyberspace? • What is Cyber security? • Why is Cyber security Important? • What is a Hacker?	
Week 2	➢ Footprinting and Reconnaissance	• Describe the elements of information security • Explain information security threats and attack vectors • Describe the hacking concepts, types, and phases • Explain the ethical hacking concepts and scope • Understand the information security controls (information defense-in-depth, policies, procedures, awareness, physical management process, and risk	

		management etc.) • Understand the penetration testing process	
Week 3	➢ Scanning Networks &Enumeration	• Describe the network scanning concepts • Use various scanning tools • Perform scanning to check for live systems and open ports • Perform scanning by using various scanning techniques • Scan beyond intrusion detection system (IDS) and firewall • Perform banner grabbing • Draw network diagrams using network discovery tools • Perform scanning penetration testing • Describe the enumeration concepts • Explain different techniques for Netbios enumeration • Explain different techniques for SNMP enumeration • Explain different techniques for LDAP enumeration • Explain different techniques for NTP enumeration • Explain different techniques for SMTP and DNS enumeration • Explain other enumerations such as IPsec, VoIP, RPC, and Linux/Unix enum • Apply enumeration countermeasures • Perform enumeration penetration testing	
Week 4	➢ Seminar		
Week 5	➢ Vulnerability Analysis	• Describe vulnerability assessment • Describe about vulnerability management life cycle (vulnerability assessment • Understand different approaches of vulnerability assessment solutions • Describe different characteristics of good vulnerability assessment solutions • Explain different types of vulnerability assessment tools • Choose an appropriate vulnerability assessment tools • Understand vulnerability scoring systems • Use various vulnerability assessment tools	

		• Generate vulnerability assessment reports	
Week 6	➢ Systems Hacking	• Describe the Hacking Methodology • Explain different techniques to gain access to the system • Apply privilege escalation techniques • Explain different techniques to create and maintain remote access to the system • Describe different types of rootkits • Explain steganography and steganalysis techniques • Apply different techniques to hide the evidence of compromise • Perform system hacking penetration testing	
Week 7	➢ Malware Threats	• Describe the concepts of malware and malware propagation techniques • Describe the concepts of Trojans, their types, and how they infect systems • Explain the concepts of viruses, their types, and how they infect fi • Explain the concept of computer worms • Perform malware analysis • Explain different techniques to detect malware • Apply malware countermeasures • Perform malware penetration testing	
Week 8	➢ Sniffing&Session Hijacking	• Describe the sniffing concepts • Explain different MAC attacks • Explain different DHCP attacks • Describe the ARP poisoning • Explain different MAC spoofing tracks • Describe the DNS poisoning • Use different sniffing tools • Apply sniffing countermeasures • Apply various techniques to detect sniffing • Perform sniffing penetration testing	
Week 9	➢ Social Engineering	• Describe the social engineering concepts • Perform social engineering using various techniques • Describe insider threats • Perform impersonation on social networking sites • Describe identity theft • Apply social engineering countermeasures	

		• Apply insider threats and identity theft countermeasures • Perform social engineering penetration testing	
Week 10	➢ Denial of Service	• Describe the DoS/DD0S concepts • Perform DoS/DDOS using various attack techniques • Describe Botnets • Describe DoS/DDOS case studies • Explain different DoS/DDoS attack tools • Apply best practices to mitigate DdoS/DD0S attacks • Perform DoS/DDOS penetration testing	
Week 11	➢ Session Hijacking	• Describe the session hijacking concaps • Perform application level sesionhpcing • Perform network lewl session hijacking • Apply different session hijacking tools • Apply session hijacking countermeasures • Perform session hijacking penetration testing	
Week 12	➢ Evading IDS, Firewalls and Honeypots	• Describe IDS, firewall, and honeypot concepts • Use different IDs, firewall and honeypot solutions • Explain different techniques to bypass IDS • Explain various techniques to bypass firewalls • Use different IDS/firewall evading tools • Explain different techniques to detect honeypots • Apply IDS/firewall evasion countermeasures • Perform IDS and firewall penetration testing	
Week 13	➢ Hacking web servers	• Hacking web servers • Describe the web server concepts • Perform various web server attack • Describe about web server attack methodology • Use different web server attack tools • Apply web server attack countermeasures • Describe the patch management concepts • Use different web server security tools • Perform web server penetration testing	

Week 14	➢ Hacking Web Applications&SQL Injection	• Describe web application concepts • Perform various web application attacks • Describe about web application hacking methodology • Use different web application hacking tools • Apply web application attacks countermeasures • Use different web application security testing tools • Perform web application penetration testing • Describe the SQL injection concepts • Perform various types of SQL injection attacks • Describe SQL injection methodology • Use different SQL injection tools • Explain different IDS evasion techniques • Apply SQL injection countermeasures • Use different SQL injection detection tools	
Week 15	Mid-Term Assignment		
Week 16	➢ Hacking Wireless Network	• Describe wireless concepts • Explain different wireless encryption algorithms • Describe wireless threats • Describe wireless hacking methodology • Use different wireless hacking tools • Describe Bluetooth hacking techniques • Apply wireless hacking countermeasures • Use different wireless security tools • Perform wireless penetration testing	
Week 17	➢ Hacking Mobile Platforms	• Understand mobile platform attack vectors • Understand various Android threats and attacks • Understand various iOS threats and attacks • Use various mobile spyware • Describe Mobile Device Management (MDM) • Apply various mobile security countermeasures • Use various mobile security tools • Perform mobile penetration testing	
Week 18	➢ Cloud Computing	• Describe cloud computing concepts • Understand cloud computing threats • Explain cloud computing attacks	

		• Apply cloud computing security measures • Use various cloud computing security tools • Perform cloud penetration testing	
Week 19	➢ Network Security Fundamentals	• Security Through Network Devices ○ Standard Network Devices ○ Network Security Hardware • Security Through Network Technologies ○ Network Address Translation (NAT) ○ Network Access Control (NAC) • Security Through Network Design Elements ○ Demilitarized Zone (DMZ) ○ Subnetting ○ Virtual LANs (VLANs) • Remote Access	
Week 20	➢ Access Control Fundamentals	• What Is Access Control? ○ Access Control Terminology ○ Access Control Models ○ Best Practices for Access Control • Implementing Access Control ○ Access Control Lists (ACLs) ○ Group Policies ○ Account Restrictions • Authentication Services ○ RADIUS ○ Kerberos ○ Terminal Access Control Access Control System (TACACS) ○ Terminal Access Control Access Control System (TACACS) • Security Assertion Markup Language (SAML)	
Week 21	Employable Project/Assignment (6 weeks i.e. 21-26)	● Guidelines to the Trainees for selection of students employable project like final year project (FYP)	

	in addition of regular classes. **OR** On job training (2 weeks)	● Assign Independent project to each Trainee ● A project based on trainee’s aptitude and acquired skills. ● Designed by keeping in view the emerging trends in the local market as well as across the globe. ● The project idea may be based on Entrepreneur. ● Leading to the successful employment. ● The duration of the project will be 6 weeks ● Ideas may be generated via different sites such as: https://1000projects.org/ https://nevonprojects.com/ https://www.freestudentprojects.com/ https://technofizi.net/best-computer-science-and-engineering-cse-project-topics-ideas-for-students/ • Final viva/assessment will be conducted on project assignments. • At the end of session the project will be presented in skills competition • The skill competition will be conducted on zonal, regional and National level. • The project will be presented in front of Industrialists for commercialization • The best business idea will be placed in NAVTTC business incubation center for commercialization. --- **OR** **On job training for 2 weeks:** • Aims to provide 2 weeks industrial training to the Trainees as part of overall training program • Ideal for the manufacturing trades • As an alternate to the projects that involve expensive equipment • Focuses on increasing Trainee’s motivation, productivity, efficiency and quick learning approach.	

Week 22	➢ Business Continuity and DRP	• What Is Business Continuity? • Disaster Recovery ○ Disaster Recovery Plan (DRP) ○ Redundancy and Fault Tolerance ○ Data Backups • Environmental Controls ○ Fire Suppression ○ Electromagnetic Interference (EMI) Shielding ○ HVAC • Incident Response ○ Forensics • Incident Response Procedures	
Week 23	➢ Risk Identification and Mitigation & Incident Handling	• Controlling Risk ○ Privilege Management ○ Change Management ○ Incident Management ○ Risk Calculation • Reducing Risk Through Policies ○ What Is a Security Policy? ○ Balancing Trust and Control ○ Designing a Security Policy ○ Types of Security Policies • Awareness and Training ○ Compliance ○ User Practices ○ Threat Awareness • Training Techniques	
Week 24	➢ Security Audit	• Security Auditing (planning, operations, performance, evaluation) • Ethical Hacking / Penetration testing • Cyber Security Awareness • **Hands-on Lab(s)** ○ Building a machine for penetration testing ○ Perform vulnerability analysis	

		• Secure configurations of devices and systems	
Week 25	➢ Monitoring and Logging	• Firewall logs • System logs • SIEM logs	
Week 26	➢ Entrepreneurship and Final Assessment in project	• Job Market Searching • Self-employment • Freelancing sites • Introduction • Fundamentals of Business Development • Entrepreneurship • Startup Funding • Business Incubation and Acceleration • Business Value Statement • Business Model Canvas • Sales and Marketing Strategies • How to Reach Customers and Engage CxOs • Stakeholders Power Grid • RACI Model, SWOT Analysis, PEST Analysis • SMART Objectives • OKRs • Cost Management (OPEX, CAPEX, ROCE etc.) • Final Assessment	