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 regarding with 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

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? • Prerequisites of Cyber security • About Kali Linux • Different flavor of Linux for Hacking and pentesting • Lab Setup • Virtualization and OS installations • Current Security Landscape • Common Security Principles • Security for SOHO, Data Center, Cloud and virtual environment	**Home Assignment**

Week 2	➢ Prerequisites ➢ Kali Linux ➢ Window CMD	**Motivational Lecture (***For further detail please see Page No: 3& 4)* • Kali and Parrot Linux • Directory Structure • Basic and admin commands • Variables and User Profiles • Windows CMD commands • PowerShell • Windows Registry • Commands Alias and Links • Secure Access Management • Compare In-band and out-of-band management • Protection/Hardening of management plane • Configure and verify secure access through SNMP v3	• **Task 1** • **Task 2** • **Task 3** • **Task 4** • **Task 5** *Details may be seen at Annexur e-I*
Week 3	➢ User ➢ Permission ➢ SMB ➢ FTP	**Success stories (** *For further detail please see Page No: 3& 4)* • User manage management in window • Linux User and groups • File and folder permission in Linux • ACL and Special Permissions • NTFS permissions in Windows • Data Sharing with SMB • Cisco ASA Product Family Overview and Design • Introducing the Cisco ASA 5500-X Series Next Generation Firewalls • Introducing Cisco ASAv New Features • Installation of ASA 9.61v and its management via Cisco ASDM	• **Task 6** • **Task 7** • **Task 8** • **Task 9** • **Task 10** • **Task 11** *Details may be seen at Annexur e-I*

Week 4	➢ Services MGT ➢ Automation ➢ Firewall	**Motivational Lecture (***For further detail please see Page No: 3& 4)* • Service management with systemctl • Automate jobs with Crontab and window scheduler • Windows Defender and real time Virus protection Linux and Window Firewall • Window Defender and Real time Virus protections • Iptables firewall and inbound and outbound traffic rules • Ipforwarding and MASQUERADE • New firewall (Firewalld) • /etc/security and TCP Wrapper • Selinux Booleans and Rules • Password Policy with PAM • Traffic redirections rules • Cisco ASA Firewall Technologies • Basic Firewall initialization using CLI and ASDM • Firewall Access Control	• **Task 12** • **Task 13** • **Task 14** • **Task 15** • **Task 16** • **Task 17** • **Task 18** • **Task 19** • **Task 20** • **Task 21** • **Task 22** *Details may be seen at Annexur e-I*

		• Generate vulnerability assessment reports	
Week 5	➢ LVM SWAP ➢ Widows Disk MGT ➢ Rescue	**Success stories (***For further detail please see Page No: 3& 4)* • Disk Management • SWAP and LVM Partitions • Windows Disk MGT tool • Basic T.Shoot of Linux • NAT on ASA (IPv4 / IPv6) • Object/Auto NAT • Manual or Twice NAT • Source Based vs Destination based NAT • NAT traversal	• **Task 23** • **Task 24** • **Task 25** *Details may be seen at Annexur e-I*
Week 6	➢ Scripting ➢ Python ➢ PHP	**Motivational Lecture (***For further detail please see Page No: 3& 4)* • Windows CMD commands • PowerShell • Linux Shell and variables • .bat Script • .sh Script • Basic python scripts and • Basic of PHP • Routing on ASA • Static / Default • Dynamic Routing protocols • VLANs and sub-interfaces in ASA • Secure DMZ Design & implementation	• **Task 26** • **Task 27** *Details may be seen at Annexur e-I*
Week 7	➢ Server Apps	**Success stories (***For further detail please see Page No: 3& 4)* • Data sharing Apps • DHCP Server and Clients • DORA process • DNS Server and clients • DNS Record Types • Virtualization / Context in ASA • Firewall Deployment Modes • Routed / Layer 3 design • Transparent mode	• **Task 28** • **Task 29** *Details may be seen at Annexur e-I*

Week 8	➢ Web Server ➢ Mail Server	**Motivational Lecture (***For further detail please see Page No: 3& 4)* • Apache and Nginx Web Server • IIS Web Server • XAMP and LAMP • Mail Server with SMTP/POP/IMAP • ASA Firewall High Availability • Active-Passive deployment • Active-Active deployment • Redundant Interfaces • Aggregated Interfaces	• **Task 30** • **Task 31** • **Task 32** • **Task 33** • **Task 34** *Details may be seen at Annexur e-I*

Week 9	➢ Cryptography ➢ Steganography ➢ CIA	**Success stories (***For further detail please see Page No: 3& 4)* • Encryption, Decryption • Encoding, Decoding • Hashing • Public and Private Key • SSL , TLS, PKI • Email Encryption • About steganography and Homography • Hide data with in picture and video • Hide payload with in picture and .pdf documents • Executable .bat script hide with in and documents and pictures • Concepts of Homography • Homography attack with Phishing • Countermeasures • Modular Policy Framework • ASA Clustering • Spanned-EtherChannel • Interface mode	• **Task 35** • **Task 36** • **Task 37** • **Task 38** • **Task 39** *Details may be seen at Annexur e-I*
Week 10	➢ Password Break ➢ SAM Password ➢ Linux/SHA512	**Motivational Lecture (***For further detail please see Page No: 3& 4)* • Windows Password Break • Windows Password Cracking • Linux Password Break and Cracking • .pdf and .rar file Password Cracking • Bios Password • Mobile Password Breaking • Cisco ASA FirePOWER / Cisco FTD • Evolution • Deployment Models • Initial Setup / Boot strapping	• **Task 40** • **Task 41** • **Task 42** • **Task 43** • **Task 44** *Details may be seen at Annexur e-I*

Week 11	➢ Footprinting and Reconnaissance	**Success Stories (***For further detail please see Page No: 3& 4)* • 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 • Understand the penetration testing process • Fire POWER Traffic flow • FirePOWER Access Policy Components • Security Zones • Creating Individual Objects and Groups	• **Task 45** • **Task 46** • **Task 47** *Details may be seen at Annexur e-I*
Week 12	➢ Scanning Networks ➢ &Enumeration	**Motivational Lecture (***For further detail please see Page No: 3& 4* • 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	• **Task 48** • **Task 49** • **Task 50** • **Task 51** *Details may be seen at Annexur e-I*

		• 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 • Pre-filter policy in Cisco FTD • Filtering based on Networks / Ports • Filtering based on Web URLs • Filtering based on Applications (AVC)	

Week 13	Mid-Term Assignment		• **Task 52** • **Task 53** • **Task 54** • **Task 55** *Details may be seen at Annexure-I*
Week 14	➢ Vulnerability Analysis	• Success stories (For further detail please see Page No: 3& 4) • 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 tool • Understand vulnerability scoring systems • Use various vulnerability assessment tools • File Blocking • SSL Decryption • Advanced Malware Protection (AMP) • AMP for Network • AMP for Content • AMP for Endpoint • Security Intelligence	• **Task 56** • **Task 57** • **Task 58** *Details may be seen at Annexur e-I*

Week 15	➢ Systems Hacking	• Motivational Lecture(For further detail please see Page No: 3& 4) • 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 • Correlation Policy in FTD • Intrusion Detection and Prevention (IPS) / SNORT Rules • FirePOWER Reporting • Real-time events & Logging	• **Task 59** • **Task 60** • **Task 61** *Details may be seen at Annexur e-I*
Week 16	➢ 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 • Cisco Web Security Appliance (WSA) • Features and Functionality • Install and Verify the Cisco WSA in various deployment scenarios • Deploying WSA Proxy Services	• **Task 62** • **Task 63** • **Task 64** *Details may be seen at Annexur e-I*
Week 17	➢ Sniffing & Session Hijacking	• Motivational Lecture(For further detail please see Page No: 3& 4) • Describe the sniffing concepts • Explain different MAC attacks • Explain different DHCP attacks • Describe the ARP poisoning	• **Task 65** • **Task 66** *Details may be*

		• 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 • Utilizing WSA Authentication • Configuring WSA Policies • Enforcing Acceptable Use • Defending Against Malware • Data Security Features	*seen at Annexur e-I*

Week 18	➢ Social ➢ Engineering	• Success stories (For further detail please see Page No: 3& 4) • 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 • Cisco Email Security Appliance (ESA) • Features and Functionality • Deployment Options • Administering the Cisco Email Security Appliance • Email Security Pipeline	• **Task 67** • **Task 68** *Details may be seen at Annexur e-I*
Week 19	➢ Denial of Service	• Motivational Lecture(For further detail please see Page No: 3& 4) • 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 • Controlling Sender and Recipient Domains • Controlling Spam with Cisco SensorBase and Antispam • Using Antivirus, Advanced Malware Protection, and Virus Outbreak Filter • Using Mail Policies • Using Content Filters • Preventing Data Loss	• **Task 69** • **Task 70** • **Task 71** *Details may be seen at Annexur e-I*

Week 20	➢ Session Hijacking	• Success stories (For further detail please see Page No: 3& 4) • 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 • Cisco Identity Services Engine • Cisco ISE Architecture • ISE Deployment Models • Implementation / Bootstrapping • Identity Management	• **Task 73** • **Task 74** *Details may be seen at Annexur e-I*
Week 21	➢ iOT	• Concept of iOT • iOT Hardware • Project with Arduino • Ducky Scripts • iOT Hacking • Cisco ISE Policy • Cisco ISE as a TACACS+ Server for Device Administration with Command Authorization • Cisco ISE BYOD Process / Flow	

Week 22	➢ Evading IDS, Firewalls and Honeypots	• Motivational Lecture(For further detail please see Page No: 3& 4 • 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 • Configuring My Devices Portal Settings • Configuring Certificates in BYOD Scenarios • High Availability Distributed deployment	

Week 23	➢ Hacking web servers ➢ Hacking Wireless Network ➢	• Success stories (For further detail please see Page No: 3& 4) • MDM Integration • ISE Profiling Services • Endpoint compliance services • 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 • Motivational Lecture(For further detail please see Page No: 3& 4) • 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 24	➢ Monitoring and Logging ➢ Hacking Mobile	• Motivational Lecture(For further detail please see Page No: 3& 4) • Firewall logs • System logs • Logs Server • Monitoring Tools • Motivational Lecture(For further detail please see Page No: 3& 4) • 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 • Client posture services and provisioning • Web Authentication and Guest services	
Week 25	➢ Entrepreneurship and Final Assessment in project	• Job Market Searching • Self-employment • Freelancing sites • Entrepreneurship • Final Assessment	

Week 26	➢ Dark Web	NAVIGATING THE DEEP & DARK WEB ➢ Exploring the Surface, Deep & Dark Web ➢ Ethics and Legality ➢ The Onion Router (TOR) ➢ The Hidden Internet Project (I2P) ➢ Deep & Dark Web Search Engines CRIME ON THE DARK WEB ➢ The Hidden Wiki ➢ Dark Markets ➢ Drugs on the Dark Web ➢ Weapons & Hitmen on the Dark Web ➢ Fake Documents on the Dark Web ➢ Human Trafficking & Sexual Exploitation on the Dark Web DIGITAL CURRENCY ➢ Cryptocurrencies ➢ Blockchain / Bitcoin	

Tasks For Certificate in Cyber Security *Annexure-I*

Task No.	Task	Description	Week
Cyber Security			
1	**Open Source Information Gathering using Windows Command Line Utilities**	As a professional Ethical Hacker or Pen Tester, your first step will be to check for the reachability of a computer in the target network. Operating systems offer several utilities that you can readily use for primary information – gathering. Windows command-line utilities such as ping nslookup. And tracert gather important information like IP address, maximum Packet Fame size, etc., about a target network of system that form a base for security assessment and pen test.	**Week-2 & 3**
2	**Finding Company's Sub – domains using Sublist3r**	As a professional ethical hacker, you should be able to extract information on the target using an automated tool such as Sublist3r. It uses multiple search engines to gather the subdomains of a target domain. This lab will demonstrate extracting information using Sublisør.	
3	**Gathering Personal Information using Online People Search Services**	During information gathering you need to gather personal information about employees working on critical positions in the target organization such as Network Administrator, Help Desk Employees, and Receptionist etc. The information collected can be useful in performing social engineering. This lab will demonstrate how you can search for personal information using online people search services.	
4	**Gathering Information from LinkedIn using In Spy**	As a professional ethical hacker, you should be able to extract information on the target using an automated tool such as InSpy. It uses Google to extract valuable information about the employees of an organization through their twitter profiles.	

Task No.	Task	Description	Week
5	**Collecting Information About a Target Website using Firebug**	Collect information on the target website and extract the source code of the web pages built in HMII, Java Script, CSS script etc. This activity may reveal potential vulnerabilities in the web application that can be exploited later in the security assessment phases. This lab will demonstrate bow to reveal source code and collect information about a target website.	
6	**Extracting a Company's Data using Web Data Extractor**	Extract information from the organization website. You are required to perform web data extraction in order to gain useful information from the website. This lab will show you how to perform web data extraction on the target website	
7	**Mirroring Website using HTTrack Web Site Copier**	Difficult to perform foot printing on a live website. Need to mirror the target website. This mirroring of the website helps you to footprint the web site thoroughly on your local system.	
8	**Preparation of EVE-NG based test bed for defensive and Offensive security**	Use of Emulated Virtual Environment – Next Generation for simulating defensive security devices	
9	**Management plane Hardening**	Configure and verify management plane hardening features for L2/L3 devices	
10	**Securing Management Access**	Configure and verify secure access through SNMPv3	
11	**Cisco ASAv Features**	Installation of ASA 9.61v and its management via Cisco ASDM	
12	**Collecting Information About a Target by Tracing Emails**	An attacker may send malicious emails to a victim in order to carry out an attack on a target organization. As a professional ethical hacker, you should be able to trace out information about such malicious email. It involves analyzing the email headers of suspicious email to extract information such as the date that an email was received or opened, geographical information, etc.	**Week-4**

13	**Gathering IP and Domain Name Information using Whois Lookup**	WHOIS foot printing the target domain name or IP addresses. It involves gathering information on the target IP and domain obtain during previous information gathering steps.	

Task No.	Task	Description	Week
14	**Advanced Network Route Tracing using Path Analyzer Pro**	With the IP address, hostname, and domain obtained in the previous information gathering steps, your nest task will be to trace the route of the target network in order to detect the trusted routes, firewall, and network topology used in the network. This lab will demonstrate how to demonstrate tracing on the target network.	
15	**Foot printing a Target using Maltego**	The information gathered in the previous steps might not be sufficient to reveal potential vulnerabilities of the target. There could be more information available that could help in finding loopholes in the target. As an ethical hacker, you should look for as much information as possible about the target. This lab will demonstrate what other information you can extract from the target.	
16	**Performing Automated Network Reconnaissance using Recon – ng**	As an ethical hacker or pen tester, you should also perform host discovery on the target to get information about additional domains. This activity will enable you to find all the hosts present on the target. This lab will demonstrate how to discover additional hosts from the target	
17	**Using Open – source Reconnaissance Tool Recon – ng to Gather Personnel Information**	During information gathering, you are required to discover personal information on the target. This personal information can be used later to perform other attacks such as social engineering attacks. So as a professional ethical hacker or pen tester, you should be able to discover the personal information of a target company. This lab will demonstrate how to discover personal information about the target organization	
18	**Collecting Information from Social Networking Sites**	Lab Scenario For a security assessment, you can gather information about social networking data such as tweets, profiles, pictures, etc. At a specified location. As a	

Task No.	Task	Description	Week
	using Recon – ng Pushpin	professional ethical hacker should be able to extract such social networking information from a specified geographical location. This lab will demonstrate how to collect information from social networking sites from a specific geographical location	
19	**Automated Fingerprinting of an organization using FOCA**	Useful information may reside on the target organization's website in the form of pdf documents, Microsoft Word files, etc. As an ethical hacker, you should be able to extract valuable data including metadata and hidden information from such documents. This lab will demonstrate how to extract valuable information from website archives.	**Week-4**
20	**Open Source Intelligence Gathering Using OSR Framework**	As a professional ethical hacker, you should be able to extract information on the target using an automated tool such as Usuf.py. It extracts the user aliases from multiple social media platforms. This lab will demonstrate extracting information using Usuf.py.	
21	**Information Gathering Using Metasploit**	As a professional ethical hacker, you should be able to extract information on the target using an automated tool such as Metasploit. Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. This lab will demonstrate extracting information using Metasploit Framework.	**Week-4**
22	**Information Gathering using the Harvester**	As a professional ethical hacker, you should be able to extract information on the target using an automated tool such as The Harvester. It uses Google, Bing, SHODAN, etc. To extract valuable information from the target domain. This lab will demonstrate extracting information using TheHarvester.	

	Cisco ASA Firewall Initialization	Basic Firewall initialization using CLI/ASDM and Firewall access control.	
23	**Scanning the Network**	During network – scanning phase, you are required to	**Week-5,6,7**

Task No.	Task	Description	Week
	using the Colasoft Packet Builder	perform network scanning to detect a live host on the network. As an expert ethical hacker or as a penetration tester, you should be aware of the different tools used to perform network scanning. This lab will demonstrate how to perform network scanning using ARP Ping Scanning techniques.	
24	**UDP and TCP Packet Crafting Techniques using HPING3**	During network scanning, your first task will be to scan the target network to determine all possible open ports, live hosts, and running services. Knowledge of packet – crafting techniques may help you to scan the network beyond the firewall or intrusion detection system (IDS).	
25	**Basic Network Troubleshooting using MegaPing**	During the security assessment – scanning phase, you should not limit your scanning attempts by number or type. It is important to try different tools and techniques to detect line host and open ports of the system. This lab will demonstrate how to detect live hosts and open ports in the target network.	
26	**Understanding Network Scanning using Nmap**	Nmap is network – scanning utility that most of the security professionals use during security assessment. It supports various types of network – scanning techniques. During security assessment, you will be asked to perform network scanning using Nmap. Therefore, as a professional ethical hacker or a penetration tester, you should be able to perform nawork scanning using Nmap. This lab will show you how to perform network scanning using Nmap.	

27	**NAT on Cisco ASA**	Configuring Object NAT and manual NAT with source & destination based schemes.	
28	**Routing on ASA and Secure DMZ Design**	Configuring Routing protocols and implementation of Secure DMZ design near perimeter firewall.	
29	**Virtualization on Cisco ASA. Various deployment modes**	Configuring context on Cisco ASA. Implementation of Routed and transparent mode firewalls.	
30	**Performing Man – in – the Middle Attack using Cain & Abel**	You learned in the previous lab how to obtain user name and passwords using Wireshark. By merely capturing enough packets, attackers can extract the username and password if victims authenticate themselves in public	**Week –8**

Task No.	Task	Description	Week
		networks, especially on unsecured websites. Once a password is hacked, an attacker can simply log into the victim’s email account or use that password to login to their PayPal and drain the victim’s bank account. They can even change the password for the email.	
31	**Spoofing MAC Address using SMAC SMAC**	MAC duplicating or spoofing attack involves sniffing a network for MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then the attacker spoofs his or her own MAC address with the MAC address of the legitimate client. Once the spoofing is successful, the attacker an receive all traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of a network user. If an administrator does not have the working packet sniffing skills, it is hard to defend intrusions. So, as an Expert Ethical Hacker and Penetration Tester, you must spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing and DNS poisoning.	**Week –8**
32	**Sniffing Passwords using Wireshark**	Data traversing an HTTP channel is prone to MITM attacks, as it flows in plain-text format. Network administrators can use sniffers to troubleshoot network problems, examine security problems and debug protocol implementations. However, an attacker can use the tools such as Wireshark and sniff the traffic flowing between the client and the server. This traffic obtained by the attacker might contain sensitive information such as login credentials, which can be used to perform malicious activities such as user-session impersonation.	

Task No.	Task	Description	Week
33	**Analyzing a Network using Capsa Network Analyzer**	Capsa is a portable network analyzer application for both LANs and WLANs which performs real-time packet capturing capability, 24/7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It goes one step ahead of sniffing by intuitively analyzing network packets and generating meaningful information Network administrators can use Capsa's comprehensive high – level window view for monitoring the entire network, for a quick insight into network administrators or network engineers that allows rapid pinpointing and resolving application problems.	
34	**High Availability Options on Cisco ASA**	Configure Active/Passive and Active/Active designs for HA. Implementation of Redundant and aggregated interfaces.	
35	**Detecting phishing using Netcraft**	As you are an expert Ethical Hacker and Penetration Tester, you must be aware of phishing attacks occurring on the network, and implement anti-phishing measures. In an organization, proper training must be provided to the people, to help them deal with phishing attacks. In this lab, you will be learning to detect phishing using Netcraft.	**Week-9**
36	**Detecting Phishing using PhishTank**	PhishTank is a collaborative clearinghouse for data and information regarding Internet phishing.	

37	**Sniffing Facebook Credentials using Social Engineering Toolkit (SET)**	The Social Engineering Toolkit (SET) is an open – source Python – driven tool designed for penetration testing	
38	**Phishing User Credentials using SpeedPhish Framework (SPF)**	Social Engineering attacks are used to compromise companies every day. They are an increasing threat to organizations all over the globe. Even though there are many hacking tools available throughout hacking communities, SpeedPhish Framework (SPF) is freely available and applicable to Spear – phishing attacks, website attacks, and many others. Attackers can draft email messages, attach malicious files, and send them to numerous people using SPF	
39	**Modular Policy Framework**	Configuring MPF with security filtering. Implementation of ASA clustering with spanned ether-channel and interface mode.	

Task No.	Task	Description	Week
40	**SYN Flooding a Target Host using Metasploit**	A SYN flood is a form of denial – of – service attack in which an attacker sends a succession of SYN requests to a target machine in an attempt to exhaust its resources and make it unresponsive to legitimate in incoming traffic	**Week-10**
41	**SYN Flooding a Target Host using hping3 hping3**	A SYN flood is a form of denial – of – service attack in which an attacker sends a succession of SYN requests to the target's system to consume enough server resources to make the system unresponsive to legitimate traffic. Hs A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either not send the expected ACK, or spoof the source IP address in the SYN, causing the server to send the SYN – ACK to a falsified IP address – which will not send an ACK because it "knows" that it never sent a SYN. The server will wait for the acknowledgment for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of half – open connections will bind resources on the server until no new connections is made , resulting in a denial of service to legitimate traffic, Some systems may also malfunction badly or even crash	
42	**Performing Distributed Denial of Service Attack Using HOIC**	A distributed denial of service (DdoS) attack involves a group of compromised systems usually infected with Trojans used to perform a DoS attack on a target system or network.	
43	**Detecting and Analyzing Dos Attack Traffic using KFSensor and Wireshark**	KF Sensor is a Network Intrusion Detection Tool that is equipped with several mechanisms to counter DOS attacks. The tool allows you to determine the maximum number of connections to the machine per IP address.	
44	**Deployment of Cisco Firepower/ Cisco FTD**	Initial setup for Cisco NGFW and its bootstrapping	

45	**Session Hijacking using the Zed Attack Proxy (ZAP) The Zed Attack Proxy (ZAP)**	ZAP is an Intercepting Proxy. It allows you to see all the requests you make to a web app and all the responses you receive from it. Amongst other things, this allows you to see AJAX calls that may not otherwise be obvious. You can also set break points, which allow you to change the requests and responses on the fly.	**Week-11**

Task No.	Task	Description	Week
46	**Perform sslstrip and Intercept HTTP Traffic through BetterCAP**	Attackers can use session hijacking to launch various kinds of attacks, such as man in – the middle (MITM) attack. An MTM attack one in which the attacker places himself between the client and server. Session hijacking enables the attackers to place themselves between the authorized client and the web server, so that all information – traveling in either direction must pass through them. An ethical hacker or a penetration tester, you must know the working of an MITM attack to protect your organization's sensitive information from the attack.	
47	**FirePower Access Policy**	Configuring various components of firepower access control policy with security zones, objects and groups.	
48	**Detecting Intrusions using Snort**	The goal of the Intrusion Detection Analyst is to find possible attacks against a network. The past few years have witnessed a significant increase in DdoS attacks on the Internet, making network security a great concern. Analysts must do this by examining IDS logs and packet captures and corroborating them with firewall logs, known vulnerabilities, and general trending data from the Internet. IDS attacks are becoming more cultured, automatically reasoning the attack scenarios in real time and categorizing them has become a critical challenge	**Week-12**

49	**Detecting Malicious Network Traffic using HoneyBOT HoneyBOT**	A honeypot makes a protected domain in which to capture and interact with spontaneous movement on a system. HoneyBOT is a simple – to – use arrangement perfect for system security research or as a feature of an early – warning IDS. As a penetration tester, you will come across systems behind firewalls that block you from accessing the information you want. Thus, you will need to know how to avoid the firewall rules in place and discover information about the host. This step in a penetration testing is called	

Task No.	Task	Description	Week
		Firewall Evasion Rules	
50	**Pre-filter policy**	Configuring pre-filter policy on FTD. Perform filtering based on networks/ports, Web URLs and AVC	
51	**Detecting Intruders and Worms using KFSensor Honeypot IDS**	Intrusion detection plays a key role in ensuring the integrity of a system’s security. Network Intrusion Detection Systems (NIDSs) have long been the best method for identifying assaults. KFSensor is an NIDS that is casy to install and configure. No special hardware is required, and its efficient design enables it to run even on low specification Windows machines. To become an expert Penetration Tester and Security Administrator, you must possess sound knowledge of network IPSs and IDSs, identify network malicious activity and log information, and stop or block malicious network activity.	
52	**Performing Web Server Reconnaissance using Skipfish Skipfish**	Every attacket tries to collect as much information as possible about the target web server. The attacker gathers the information and then analyzes the information in order to find lapses in the current security mechanism of the web server.	**Week-13**

53	**Footprinting a Web Server using the httprecon Tool**	Web applications can publish information, interact with Internet users, and establish an e-commerce / e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats. Although the threats in cyberspace remain largely the same as in the physical world (e.g., fraud, theft, vandalism, and terrorism), they are far more dangerous. Organizations can face monetary losses, damage to reputation, or legal action if an intruder successfully violates the confidentiality of their data. DoS attacks are easy for attackers to attempt because of the number of possible attack vectors, the	

Task No.	Task	Description	Week
		variety of automated tools available, and the low skill level needed to use the tools.	
54	**Footprinting a Web Server using ID Serve**	Pen testers must be familiar with banner grabbing techniques to monitor servers and ensure compliance and appropriate security updates. This technique also helps in locating rogue servers or determining the role of servers within a network. In this lab you will learn the banner grabbing technique to determine a remote target system using ID Serve. In order to be an expert ethical hacker and pen tester, its important to understand how to footprint a webserver.	
55	**Uniscan Web Server Fingerprinting in Kali Linux**	Webserver fingerprinting is an essential task for any penetration tester. Before proceeding to hacking / exploiting a webserver, it is critical for the penetration tester to know the type and version of the webserver as most of the attacks / exploits are specific to the type and version of the server being used by the target. These methods help any penetration tester to gain information and analyze their target so that they can perform a thorough test and can deploy appropriate methods for mitigation of such attacks on the server.	
56	**Build your CV**	Download professional CV template from any good site (https://www.coolfreecv.com or relevant) • Add Personal Information • Add Educational details • Add Experience/Portfolio • Add contact details/profile links	**Week-14 & 15**
57	**Exploiting Parameter Tampering and XSS Vulnerabilities in Web Applications**	Though web applications enforce certain security policies, they are vulnerable to attacks such as SQL injection, cross-site scripting, and session hijacking.	

Task No.	Task	Description	Week
58	**Performing Cross – Site Request Forgery (CSRF) Attack**	Cross – Site Request Forgery (CSRF) is an attack which enforces a user to run unknown activities on a web application in which they're currently logged in.	
59	**Enumerating and Hacking a Web Application using WPScan and Metasploit**	WPScan is a black – box WordPress vulnerability scanner. It is a regular part of most of the penetration testers' assessment toolkit. According to Web Technology Surveys, WordPress is used by 60.4% of all known content management system websites, and 23.8% of all websites. WPScan provides great help in assessing the security of target organizations with WordPress sites.	
60	**SSL Decryption and File Blocking**	Configuration of Advanced Malware Protection with security intelligence. Implementation of Correlation policy.	
61	**Cisco Web Security Appliance**	Bootstrapping Cisco WSA and deploy proxy services	

62	**SQL Injection Attacks on MSSQL Database**	SQL Injection is one of the most common and perilous attacks that website's software experience. This attack is performed on SQL databases that have weak codes and this vulnerability can be used by an attacker to execute database queries to collect sensitive information, modify the database entrics or attach a malicious code resulting in total compromise of the most sensitive data. As an Expert Penetration Tester and Security Administrator, you need to test web applications running on the MS SQL Server database for vulnerabilities and flaws.	**Week-16**
63	**WiFi Packet Sniffing using Microsoft Network Monitor and Wireshark**	Wireless networks aanbe open to active or passive attacks. These attacks include Dos, MITM, spoofing, jamming, war driving, network hijacking, packet sniffing, and many more. Passive attacks that take place on wireless networks are common and are difficult to detect since the attacker usually just collects information. Active attacks happen when a hacker has gathered information about the network after a successful passive attack. Sniffing is the act of monitoring the network traffic using legitimate network analysis tools.	**Week-16**

Task No.	Task	Description	Week
		Hackers can use monitoring tools, including AiroPeck, Ethercal, TCPDump, or Wireshark, to monitor the wireless networks. These tools allow hackers to find an unprotected network that they can hack. Your wireless network can be protected against this type of attack by using strong encryption and authentication methods In this lab, we use Microsoft Network Monitor, a tool that an sniff network using a wireless adapter. Because you are the cthical hacker and a penetration tester of an organization, you need to check the wireless security and evaluate weaknesses present in your organization	
64	**Create an account profile on Fiverr (at least two gigs) and Upwork**	Create an account by following these steps: **Step 1:** Personal Info **Step 2:** Professional Info **Step 3:** Linked Accounts **Step 4:** Account Security	**Week-16**
65	**Creating Binary Payloads using Kali Linux to Hack Android**	With advancement in technology and implementation of BYOD policies, there is a radical increase in smartphone usage in the workplace. Though companies offer robust network security, attackers / insiders attempt to hack into employees' mobile phones to obtain sensitive information related to the company or the employee. As an ethical hacker, you should be familiar with all the exploits and payloads available in Kali Linux to perform various tests for vulnerabilities on the devices connected to a network.	**Week-17**

66	**WSA Authentication and Enforcing Acceptable use**	Configuring WSA policies to enforce data security features and defending against Malware.	
67	**Harvesting Users' Credentials using the Social Engineering Toolkit The Social Engineering Toolkit (SET)**	Social engineering is an ever-growing threat to organizations all over the world. Social engineering attacks are used to compromise companies every day. Even though there are many hacking tools available with underground hacking communities, a social engineering	**Week-18**

Task No.	Task	Description	Week
		toolkit is a boon for attackers, as it is freely available to use to perform spear - phishing attacks, website attacks, and so on. Attackers can draft email messages and attach malicious files and send them to a large number of people using the spear-phishing attack method. Also, the multi attack method allows utilization of the Java applet, Metasploit browser, Credential Harvester / Tabnabbing, and others all at once.	
68	**Cisco Email Security Appliance**	Administering Cisco Email Security appliance and email security pipeline	
69	**Building a Cloud using ownCloud and LAMPServer**	OwnCloud is an open - source application used to sync documents and provides tools to users, as well as substantial undertakings and administration suppliers working. OwnCloud gives protected secure, and consistent record = view synchronization, and imparting arrangement on servers that you control. As an expert Security Professional and Penetration Tester, you should possess knowledge of building a cloud server, creating user accounts, and assigning user rights to each of them in accessing files and directories. You also need to know about sharing files online and offline using ownCloud Desktop Client	**Week-19**

70	**Securing ownCloud from Malicious File Uploads using ClamAV ClamAV**	Cloud is a very lucrative and sought - after platform for the hackers as the gains from an exploited cloud platform is tremendous. Since there are numerous users active on a cloud platform at any given time, it makes it that much more necessary and harder to protect all that data from getting hacked. One way to prevent malicious files from getting into the cloud server is to filter them at the time of upload. This command can be performed with the help of an antivirus configured to scan and protect the system and	

Task No.	Task	Description	Week
		stop any malicious files from getting uploaded. As a security executive, it is your duty to make sure that the cloud stays uninfected and safe for the clients to use it at their ease without worrying about their privacy.	
71	**Using Virus Outbreak Filters**	Implement mail policies, content filters, data loss prevention and virus outbreak filters.	
72	**Calculating One - way Hashes using HashCalc EY HashCalc**	Message digests or one - way hash functions distill the information contained within a file (small or large) into a single fixed - length number, typically between 128 and 256 bits in length. If any given bit of the function's input is changed, every output bit has a 50% chance of changing. Given an input file and its corresponding message digest, it should be nearly impossible to find another file with the same message digest value, as it is computationally unfeasible to have two files with the same message digest value. Hash algorithms are widely used in a wide variety of cryptographic applications, and are useful for digital signature applications, file integrity checking and storing passwords.	**Week-20**

73	**How to search and apply for jobs in at least two labor marketplace countries (KSA, UAE, etc.)**	• Browse the following website and create an account on each website ▪ Bayt.com – The Middle East Leading Job Site ▪ Monster Gulf – The International Job Portal ▪ Gulf Talent – Jobs in Dubai and the Middle East • Find the handy ‘search’ option at the top of your homepage to search for the jobs that best suit your skills. • Select the job type from the first ‘Job Type’ drop-down menu, next, select the location from the second drop-down menu. • Enter any keywords you want to use to find suitable job vacancies. • On the results page you can search for part-time jobs only, full-time jobs only, employers only, or agencies only. Tick the boxes as appropriate to your	**Week 20 onwards**

Task No.	Task	Description	Week
		search. • Search for jobs by: ▪ Company ▪ Category ▪ Location ▪ All jobs ▪ Agency ▪ Industry	
74	**Cisco Identity Services Engine**	Implementing next generation NAC solution with Identity management, profiling, posturing, BYOD access control and guest services	

Annexure-II

SUGGESTIVE FORMAT AND SEQUENCE ORDER OF MOTIVATIONAL LECTURE.

Mentor

Mentors are provided an observation checklist form to evaluate and share their observational feedback on how students within each team engage and collaborate in a learning environment. The checklist is provided at two different points: Once towards the end of the course. The checklists are an opportunity for mentors to share their unique perspective on group dynamics based on various team activities, gameplay sessions, pitch preparation, and other sessions, giving insights on the nature of communication and teamwork taking place and how both learning outcomes and the student experience can be improved in the future.

Session- 1 (Communication):

Please find below an overview of the activities taking place Session plan that will support your delivery and an overview of this session's activity.

Session- 1 OVERVIEW
Aims and Objectives:
• To introduce the communication skills and how it will work

- Get to know mentor and team - build rapport and develop a strong sense of a team
- Provide an introduction to communication skills
- Team to collaborate on an activity sheet developing their communication, teamwork, and problem-solving
- Gain an understanding of participants' own communication skills rating at the start of the program

Activity:	**Participant Time**	**Teacher Time**	**Mentor Time**
Intro Attend and contribute to the scheduled.			
Understand good communication skills and how it works.			
Understand what good communication skills mean			
Understand what skills are important for good communication skills			
Key learning outcomes:	**Resources:**		**Enterprise skills developed:**
• Understand the communication skills and how it works. • Understand what communication skills mean • Understand what skills are important for communication skills	• Podium • Projector • Computer • Flip Chart • Marker		• Communication • Self Confidence • Teamwork

Schedule	**Mentor Should do**
Welcome: **5 min**	Short welcome and ask the **Mentor** to introduce him/herself. Provide a brief welcome to the qualification for the class.

	Note for Instructor: Throughout this session, please monitor the session to ensure nothing inappropriate is being happened.
Icebreaker: **10 min**	Start your session by delivering an icebreaker, this will enable you and your team to start to build rapport and create a team presentation for the tasks ahead. The icebreaker below should work well at introductions and encouraging communication, but feel free to use others if you think they are more appropriate. It is important to encourage young people to get to know each other and build strong team links during the first hour; this will help to increase their motivation and communication throughout the sessions.
Introduction & Onboarding: **20mins**	Provide a brief introduction of the qualification to the class and play the "Onboarding Video or Presentation". In your introduction cover the following: 1. Explanation of the program and structure. (Kamyab jawan Program) 2. How you will use your communication skills in your professional life. 3. Key contacts and key information – e.g. role of teacher, mentor, and SEED. Policies and procedures (user agreements and "contact us" section). Everyone to go to the Group Rules tab at the top of their screen, read out the rules, and ask everyone to verbally agree. Ensure that the consequences are clear for using the platform outside of hours. (9am-8pm) 4. What is up next for the next 2 weeks ahead so young people know what to expect (see pages 5-7 for an overview of the challenge). Allow young people to ask any questions about the session topic.
Team Activity Planning: **30 minutes**	MENTOR: Explain to the whole team that you will now be planning how to collaborate for the first and second collaborative Team Activities that will take place outside of the session. There will not be another session until the next session so this step is required because communicating and making decisions outside of a session requires a different strategy that must be agreed upon so that everyone knows what they are doing for this activity and how. • "IDENTIFY ENTREPRENEURS" TEAM ACTIVITY • "BRAINSTORMING SOCIAL PROBLEMS" TEAM ACTIVITY" *As a team, collaborate on a creative brainstorm on social problems in your community. Vote on the areas*

	you feel most passionate about as a team, then write down what change you would like to see happen. Make sure the teams have the opportunity to talk about how they want to work as a team through the activities e.g. when they want to complete the activities, how to communicate, the role of the project manager, etc. Make sure you allocate each young person a specific week that they are the project manager for the weekly activities and make a note of this. Type up notes for their strategy if this is helpful - it can be included underneath the Team Contract.
Session Close: **5 minutes**	**MENTOR:** Close the session with the opportunity for anyone to ask any remaining questions. **Instructor:** Facilitate the wrap-up of the session. A quick reminder of what is coming up next and when the next session will be.

MOTIVATIONAL LECTURES LINKS.

TOPIC	SPEAKER	LINK
How to Face Problems In Life	**Qasim Ali Shah**	**https://www.youtube.com/watch?v=OrQte08Ml90**
Just Control Your Emotions	**Qasim Ali Shah**	**https://www.youtube.com/watch?v=JzFs__yJt-w**
How to Communicate Effectively	**Qasim Ali Shah**	**https://www.youtube.com/watch?v=PhHAQEGehKc**
Your ATTITUDE is Everything	**Tony Robbins** **Les Brown** **David Goggins** **Jocko Willink** **Wayne Dyer** **Eckart Tolle**	**https://www.youtube.com/watch?v=5fS3rj6eIFg**
Control Your EMOTIONS	**Jim Rohn** **Les Brown** **TD Jakes** **Tony Robbins**	**https://www.youtube.com/watch?v=chn86sH0O5U**
Defeat Fear, Build Confidence	**Shaykh Atif Ahmed**	**https://www.youtube.com/watch?v=s10dzfbozd4**
Wisdom of the Eagle	**Learn Kurooji**	**https://www.youtube.com/watch?v=bEU7V5rJTtw**
The Power of ATTITUDE	**Titan Man**	**https://www.youtube.com/watch?v=r8LJ5X2ejqU**
STOP WASTING TIME	**Arnold Schwarzenegger**	**https://www.youtube.com/watch?v=kzSBrJmXqdg**
Risk of Success	**Denzel Washington**	**https://www.youtube.com/watch?v=tbnzAVRZ9Xc**

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

Annexure-III

SUCCESS STORY

S. No	Key Information	Detail/Description
1.	**Self & Family background**	**Seemant Sehgal**, Founder and CEO of BreachLock Inc. is a promising Cyber Security Entrepreneur in the EU and USA tech scene. His venture BreachLock has been listed amongst Top 10 Vulnerability Management Solution providers for 2019 and is listed in Top 10 Vulnerability Assessment Solutions by Gartner Peers insights. He is an ardent supporter of RED Teaming philosophy. Seemant is a regular speaker at international conferences and also an author for the ISACA Journal since 2015. In January 2015, Seemant's paper on "**Effective Cyber Threat Management – Evolution And Beyond**" was published in the ISACA Journal
3.	**Post-training activities**	His areas of expertise include cyber resilience, payment security (PSD2, PCI DSS), ISO 27001, Cyber defense and SOC. He is a proud contributor/supporter for Threat Intelligence Based Ethical Red teaming (TIBER) initiative.He has been recently engaged with organizations such as ING Group, Capital One Bank, IBM, COMODO Security Solutions (UK) and Cisco Systems offering them his expertise in various domains of Information Security. He has also achieved various certifications including SANS GSNA, CISM, CISA, CEH, ISO 27001 Lead Implementer.
4.	**Message to others** **(under training)**	Take the training opportunity seriously Impose self-discipline and ensure regularity Make Hard work pays in the end so be always ready for the same.

<u>Note:</u> Success story is a source of motivation for the trainees and can be presented in several ways/forms in a NAVTTC skill development course as under: -

1. To call a passed out successful trainee of the institute. He will narrate his success story to the trainees in his own words and meet trainees as well.
2. To see and listen to a recorded video/clip (5 to 7 minutes) showing a successful trainee Audio-video recording that has to cover the above-mentioned points.*
3. The teacher displays the picture of a successful trainee (name, trade, institute, organization, job, earning, etc) and narrates his/her story in the teacher's own motivational words.

** The online success stories of renowned professional can also be obtained from* ***Annex-II***

Annexure-IV:

Workplace/Institute Ethics Guide

Work ethic is a standard of conduct and values for job performance. The modern definition of what constitutes good work ethics often varies. Different businesses have different expectations. Work ethic is a belief that hard work and diligence have a moral benefit and an inherent ability, virtue, or value to strengthen character and individual abilities. It is a set of values-centered on the importance of work and manifested by determination or desire to work hard.

The following ten work ethics are defined as essential for student success:

1. **Attendance:**

   Be at work every day possible, plan your absences don’t abuse leave time. Be punctual every day.

2. **Character:**

   Honesty is the single most important factor having a direct bearing on the final success of an individual, corporation, or product. Complete assigned tasks correctly and promptly. Look to improve your skills.

3. **Team Work:**

   The ability to get along with others including those you don’t necessarily like. The ability to carry your weight and help others who are struggling. Recognize when to speak up with an idea and when to compromise by blend ideas together.

4. **Appearance:**

   Dress for success set your best foot forward, personal hygiene, good manner, remember that the first impression of who you are can last a lifetime

5. **Attitude:**

   Listen to suggestions and be positive, accept responsibility. If you make a mistake, admit it. Values workplace safety rules and precautions for personal and co-worker safety. Avoids unnecessary risks. Willing to learn new processes, systems, and procedures in light of changing responsibilities.

6. **Productivity:**

   Do the work correctly, quality and timelines are prized. Get along with fellows, cooperation is the key to productivity. Help out whenever asked, do extra without being asked. Take pride in your work, do things the best you know-how. Eagerly focuses energy on accomplishing tasks, also referred to as demonstrating ownership. Takes pride in work.

7. Organizational Skills:

Make an effort to improve, learn ways to better yourself. Time management; utilize time and resources to get the most out of both. Take an appropriate approach to social interactions at work. Maintains focus on work responsibilities.

8. Communication:

Written communication, being able to correctly write reports and memos. Verbal communications, being able to communicate one on one or to a group.

9. Cooperation:

Follow institute rules and regulations, learn and follow expectations. Get along with fellows, cooperation is the key to productivity. Able to welcome and adapt to changing work situations and the application of new or different skills.

10. Respect:

Work hard, work to the best of your ability. Carry out orders, do what’s asked the first time. Show respect, accept, and acknowledge an individual’s talents and knowledge. Respects diversity in the workplace, including showing due respect for different perspectives, opinions, and suggestions.

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