Certificate Course on Cyber Security Essentials

Detailed Curriculum

Name of Unit of Qualification	**:**	System Security and Safety
Duration	**:**	10 Hours
Topics	**:**	Over View of Cyber Security, Policies, Procedures, Standards, and Guidelines, System Level Security Measures, Threats and Vulnerabilities, Common Cyber Attacks and Counter Measures.

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
1. Understanding of Cyber Security background	Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.	2
2. Understanding of Operational and Organizational Security	Policies, Procedures, Standards, and Guidelines - Security Awareness and Training - Interoperability Agreements - The Security Perimeter - Physical Security - Environmental Issues - Wireless - Electromagnetic Eavesdropping - People—A Security Problem - People as a Security Tool	2
3. Understanding of Linux OS	Explain basics of Linux Architecture and Importance of LinuxFile systems.	1
4. AAA (in Security) and Security in Remote Access	User, Group, and Role Management Password Policies - Single Sign-On - Security Controls and Permissions - Preventing Data Loss or Theft - The Remote Access Process - Remote Access Methods.	1
5. Understanding of Cyber Threats, Vulnerabilities and Common Attacks	Over View of Cyber Threats and Vulnerabilities, Discussion of common cyber Attacks and counter Measures.	1
6. Understanding of Windows OS	Explain basic of Windows Security and File System.	1
7. Systems Security	Authentication,Policy,Secure Design Principles, Information Flow	2

Name of Unit of	**:**	Web and Network Security

Qualification		
Duration	**:**	11 Hours
Topics	**:**	Web Security-Threats-Vulnerabilities, Role of Cryptography in Security, Security Measures using Network Protocols, Cyber Security Measures in Social Media or Social Networking

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
1. Understanding of Cyber Security in Web Infrastructure.	Introduction of Cyber Security in Web infrastructure, discussion on tools and techniques of Web security implementation and testing,	1
2. Understanding of Network Protocols Security	Roles of Networking Protocols (TCP/IP, UDP, DNS, ARP, DHCP, ICMP) in Cyber Security, Transport and Network Layer Security, Data Link Layer Security.	2
3. OS Hardening	Hardening of OS – Windows and Linux	1
4. Role of Cryptography in Security background	Introduction to Cryptography: Its Types and benefits, Cryptographic Functions, Cryptographic Types, Digital Signature, Types of Cryptographic algorithms, Techniques for cryptography, Attacks on Cryptographic Techniques.	2
5. Knowing of web Application based Threats and Vulnerabilities with counter measures	Cyber Threats and Vulnerabilities of Web Application, tools and Techniques, Examples and counter Measures, Current Security in Web Applications.	1
6. Cyber Security issues in Social Media and Social Networking	Cyber Security Issues in Social Media and Social Networking, Types of Cyber threats and vulnerabilities in social media and networking, Counter Measures of Cyber threats and vulnerabilities while handling social media applications, Tool and Techniques in this domain.	1
7. Usability of Wireshark	Wireshark Techniques – Tool Interface, Packet Capturing, Packet Filtering, Protocol Analysis, Matrix and Statistics	1
8. Cyber Ethics And Laws	Introduction to cyber laws, E-Commerce and E-Governance, Certifying Authority and Controller, Offences under IT Act, Computer Offences and its penalty under IT Act 2000, Intellectual Property Rights in Cyberspace.	1
9. Understanding of Defensible Network Architecture	Discuss the Defensive mechanism of Networks, Tools used, DMZones, Proxy Server, VLANs, IDS and IPS	1

Name of Unit of Qualification	**:**	Demonstration of few Attack Methods and practices
Duration	**:**	9 Hours
Topics	**:**	Demonstration of Kali Linux Tools and malware, SQL Injection and Cross Site Scripting, Scanning, Spoofing, Sniffing etc.

Performance Criteria (OUTCOME) No.	**Contents**	**Hrs.**
1. Demonstration of ARP Poisoning and SYN Flood	Demonstration of Kali Linux tools – ARP Poisoning and SYN Flood	1
2. Understanding of Virtual Environment	Environment Setup for Practical Exercises and OS & Tool Installations and configurations	1
3. Demonstration of DNS spoofing	Demonstration of Kali Linux tools – DNS Spoofing&Nmap Scanning	1
4. Understanding of Digital Signature and SSL	Demonstrations – Digital Sign a Document Apache Web Server Integration (Self-sign SSL)	1
5. Understanding of working of Malicious tools	Viruses, WORMS and Trojans and related Tools	2
6. Understanding of SQL Injections and Cross Site Scripting	SQL Injection techniques and Cross Site Scripting, Tools responsible	2
7. Open Source Firewall installation and its benefits	Step by step Installation of Firewall, discuss benefits of open source firewall	1

Note: After completion of course there is a final qualifying exam will be there which is not included in the course duration, for that an extra 1 or 2 days will be given to do the final assessment.