SKILLS FACTORY
SHARPER SKILLS FOR BETTER CAREERS

Proposal For Introducing

Certificate In Cyber Security

Venkateshwara House, 1st Floor, Office # 3, Opp. Kalinga Hotel,
Near Sharada Centre, Off Karve Road, Pune 411004 (India)

Phone: 020 2545 1488 / 25464656
Web: www.iqspl.com

Table of contents

Course: Certificate In Cyber Security

1. Aim & Objectives of the Course :

1. To make the students understand the concepts of cyber security tools and concepts used in the evolving cyber landscape.
2. To introduce the students to the techniques and tools of Cyber security
3. To introduce the students to various attack simulation techniques using OSINT and Frameworks.
4. To introduce students to various aspects of Cyber Security.
5. To train IT personnel, how to protect information from adversaries.
6. To train people to design threat model.
7. To train people to write technical and non-technical reports.
8. To prepare students to take up higher specialized courses in Information security.

2. Title of the course :

Certificate in Cyber Security

3. Academic year in which course is to be initiated :

Academic year	For students of	Examination
2019-20	Open to all	End of academic year

4. Eligibility criterion for admission to the course :

Knowledge of Networking & Operating System

5. Teaching scheme & Structure of the course Course :

Course Name: Certificate In Cyber Security

Course Code: CCS

Duration of Course: Two Semesters

Name of Subject	Section	Teaching Scheme	Examination Scheme							
		TH/PR	Paper HRS	TH		TW		Total	
				MAX	MIN	MAX	MIN	MAX	MIN
Foundation	First	28	3	100	40	50	20	150	60
Adversary Simulation	Second	32							
Total		60	--	100	40	50	20	150	60

Abbreviations: TH - Theory OR - Oral, TW – Term-work, PR – Practical

Summary:

Theory in HRS	Theory	Term-Work	Total
60	100	50	150

Note: The detailed syllabus of the course is given as an Appendix at the end. Please refer the appendix.

6. Standard of passing & Rules of re-appearing the examination :

1. Passing or failure in this examination will not affect the regular academic examinations.
2. Students will be awarded grades in the following manner
3. Failure in any of the heads of the examination will not entail detention. Students will be allowed to carry forward and reappear in case of failure.
4. The examination will be conducted for all modules once a year i.e. at the end of the academic year.

7. Award of grades :

Marks	Grade
90 and more	A+
80 to 89	A
70 and 79	B
51 and 69	C
50 and less	D

8. Basis for allocation of marks :

A. Internal Assessment: 50 marks.

B. University Examination (External Evaluation): 100 marks.

9. Procedure for conducting internal assessment :

a. Assignment

b. Online Exam

10. Examination system :

On successful completion of examination, students will be awarded Certificate in Cyber Security by the college and Skills Factory Learning Private Limited jointly.

The examination pattern for this module is as follows:

Name of Paper	Section & Subject Covered	Examination Scheme						
		Paper HRS	TH		TW		Total	
			MAX	MIN	MAX	MIN	MAX	MIN
CCS	Section-I Foundation	3	100	40	50	20	150	60
	Section-II Adversary Simulation							

Syllabus for Certificate In Cyber Security

Sr. No.	Module Name	Objective	Theory/ Practical	Duration
1	**Introduction to Cyber Security**	The objective of this chapter is to understand the concept of cyber security along with its need in day to day life. Layered-security approach is about maintaining appropriate security measures and procedures at five different levels within your IT environment.	**Theory**	**2 Hrs**
	Defining cyber security			
	Need for cyber security.(case studies)			
	Statistics			
	Layered approach to cyber security			
	Latest Technological Trends	By including IoT and BYOD student will get an insight into the latest technological advancement in cyber security as well as in technology. Also the student will understand the role of cyber security in pointing out threats.	**Theory**	**2 Hrs**
	Introduction to IoT			
	How the Internet of Things (IoT) Is Changing the Cyber security Landscape?			
	Threats and Countermeasures of IoT and BYOD			
	Cyber security concerns and solution in Smart City & Home Automation			
	Basics of Networking	To get familiarize with an OS and its basic settings, file management in OS. To learn difference between Linux and Windows OS	**Theory and Practical**	**10 Hrs**
	GET MAC,NCPA.CPL, cmd line			
	Obtaining IP address from DHCP Server			
	IP address: types and classes			
	IPV4 and IPV6 address			
	Sharing Files and Folders			
	Virtualization and installation of OS on virtual Box.	To get introduced to virtual application system and the sequence of booting file. To learn basic concepts of networking,		
	• Introduction to virtualization.			
	• Installation of virtual box			
	• Installation of OS.			

2	**Passwords** • Understanding password • Types of passwords. – BIOS password – System password • Administrator password. • User password. • Passwords storage – windows and Linux • Types of password attacks	This chapter will give some idea of passwords and its importance in security policy	**Theory and Practical**	**5 Hrs**
	Web browser security • Understanding web browsers. • Security features of web browsers. – Internet Explorer – Google Chrome – Firefox Mozilla – Opera	This chapter will give complete understanding of web browsers. This will explain security settings and features of different web browsers which will be very useful for users to secure his web browsing activities.	**Theory and Practical**	**5 Hrs**
	Firewall And UTM Understanding the Firewall Understanding Unified Threats Use of Firewall and UTM Advantages and Disadvantages of UTM	This chapter covers the firewall as a security measure and its types. Different firewall techniques which are useful for data protection. One can select the technique as per own requirement. UTM is single hardware platform blended with layers of threat protection.	**Theory**	**1 Hrs**
3	**Physical Security** • Understanding physical security • Need for physical security	The objective of this chapter is to understand physical security and its need. For application of physical security we are going to study some security equipment's like CCTV cameras and biometrics system. This will help to implement physical security in any organization.	**Theory**	**1 Hrs**
	• Physical security equipment's			
	Closed circuit television cameras (CCTV)			
	– Analogue cameras			
	– Digital cameras			
	Biometrics			
	– Fingerprint			
	– Iris			

	– Retina			
	– Face			
	– Security tokens			
	– Smart card			
	Mobile Security	This chapter covers different mobile platforms. Different applications used for mobile security. How to create mobile hotspots.	**Theory and practical**	**2 Hrs**
	• Different Mobile platforms.			
	• Mobile security features.			
	• Applications of mobile security			
	• Different security options in mobile like encryption etc.			
	Case studies.			
4	**Email Security**	This chapter covers details of electronic mail. How E-mail works and its types. E-mail Tracing includes how to identify fake mail through Email header analysis. Email security includes how to secure emails by setting spam filters, by using encryption etc.	**Theory and practical**	**4 Hrs**
	• What is E-mail?			
	• Understanding how Email works.			
	• Types of Email.			
	• Email Security –			
	– Set up spam filters			
	– Preventing Phishing			
	– Use encryption.			
	Keep your computer updated			
	Malware	In this topic students will be able to understand different types of malwares. This chapter includes very important area that how to secure yourself from Malwares?	**Theory and practical**	**2 Hrs**
	Understanding Malwares			
	Different types of Malwares like viruses, Worms, Trojans, Adwares, Spywares,			
	Ransomware Rootkits, and Keyloggers etc.			
	Securing system from malware			
5	**Cryptography**	Students will learn to identify different types of malware & understand how to secure the system against each malware	**Theory and practical**	**5 Hrs**
	• Understanding cryptography			
	• Goals of cryptography			
	• Cryptographic methods			
	– Rotation			
	– Substitution			
	• Mono-alphabetic substitution			
	• Poly-alphabetic substitution			
	– Transposition			

	• Types of cryptography			
	• Symmetric key cryptography			
	• Asymmetric key cryptography			
	• Use of Hash function in cryptography			
	Digital Signature in cryptography			
6	**Wireless Security**	Students will learn security parameters for 802.11 protocol	**Theory and practical**	**2 Hrs**
	• Concept of Wireless Networks			
	• Security Features of Wi-Fi			
	• Wireless Encryption Protocols			
	1. WEP			
	2. WPA			
	3. WPA2			
	• Wireless Attacks and Countermeasures			
7	**Ethical Hacking**		**Theory and practical**	**5 Hrs**
	• Concept of Ethical Hacking	The objective of this topic is to differentiate between ethical hacking and illegal hacking. Using ethical hacking techniques to understand vulnerabilities in platforms like web or system.		
	• Ethical hacking process			
	– Reconnaissance			
	1. Active reconnaissance			
	2. Passive reconnaissance			
	– Scanning			
	1. Port scanning			
	2. Network scanning			
	3. Vulnerability scanning			
	– Gaining Access			
	– Maintaining Access			
	– Covering Tracks			
	Google Hacking	Google hacking involves using To learn how to use google advanced special operators.	**Theory and practical**	**2 Hrs**
	• Google hacking techniques.			
	– Anonymity with Caches			
	– Using Google as a proxy server			
	– Directory listings			
8	**Virtualization and Cloud Computing**		**Theory and practical**	**2 Hrs**
	• Basic Concept of Virtualization			

	– Types of Virtualization	Virtualization is latest technology. With knowledge of Virtualization, one physical server can be made to act as many virtual servers. It offers a range of benefits, which is reducing the number of physical servers an organization needs.		
	– Benefits			
	• Data Center Virtualization			
	• Desktop Virtualization			
	• Virtualizing Enterprise Application			
	• Network Virtualization			
	• Server Virtualization			
	• Load Balancing with Virtualization			
	Cloud computing:	To understand how cloud works and how it can used to deliver various services.		
	• Definition of cloud			
	• Cloud Architecture			
	• Advantages of cloud			
	• Risks involved in cloud computing.			
	Cloud Storage			
	Cloud Services			
	• Software As Service (SAS)			
	• Platform As Service (PAS)			
	• Infrastructure As A Service			
	Public Cloud Environment			
9	**Cyber Crime and Cyber Laws**	This chapter will educate the Give a comprehensive understanding of different categories of cyber crime, how they can be identified and precautions required therein. Safety measures to be adopted for online banking.	**Theory**	**2 Hrs**
	• Defining cyber-crime			
	• Types of cyber-crimes			
	– Password related crimes			
	– Email related crimes			
	– Desktop related crimes			
	– Social networking sites related crimes			
	– Website related crimes			
	– Network related crimes.			
	Social engineering related crimes			
	– Categories of Cyber Crime			
	– Individual			
	– Property			
	– Government			
	– Online Banking			
	– Online banking frauds			
	Safety tips for online banking			

	Cyber laws (Information Technology Act 2000 & 2008) • Understanding cyber law • Evolution of cyber law in India. • Jurisdiction of IT Act • Penalties under IT Act. • Difference between civil law and criminal law. • Offences under IT Act- some sections. Section 43, Section 65, Section 66, Section 67, Section 72, Section 69, Section 79. Intellectual Property Rights (IPR).	This chapter will enable students to match different sections of the IT act to various kinds of cyber crimes and the penalties of such crimes.	**Theory**	**2 Hrs**
10	**ISO 27001** • Introduction to ISO 27001 • General requirements for ISO standardization. Methodological requirements Security control requirements. • Different corporate policies. Implementation and establishment of ISMS	The student learns how to establish and implement a specified predetermined security management system.	**Theory**	**2 Hrs**
11	**IP based communication: (VOIP)** • Introduction • Working of VOIP • Requirements and Availability • Service Limitation • Threat or Risk • Countermeasures Media gateway control Protocol SIP (Session Initiation Protocol)	This topic will enable the student to understand the application and function of VOIP for fast, reliable and secure Internet communication.	**Theory**	**2 Hrs**

12	**Protection of information Assets, Planning and implementation of BC/DR** • Defining Disaster. • Types of Disaster. • Consequences of Disaster • Disaster recovery. • Elements of BC • Planning of BC • Benefits of BCP and DRP • BCP Process Steps • Development of Business Continuity Plan	This chapter will enable students to understand what constitutes a disaster and what steps are needed to recover from the disaster. It also educates student on the steps required to ensure business continuity despite disasters and how to prepare for contingencies.	**Theory**	**2 Hrs**
			Total	**60 Hrs**