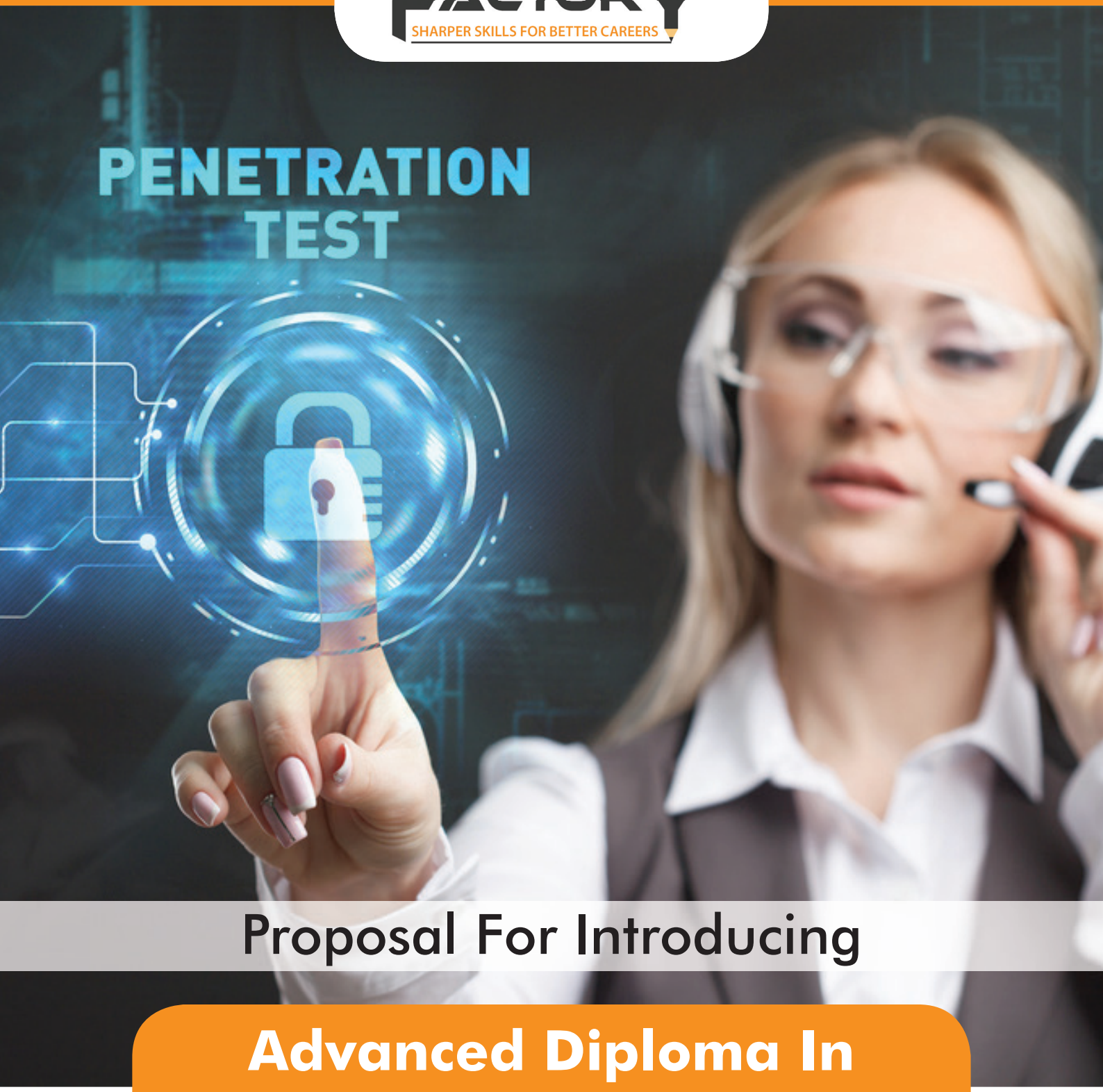
SKILLS FACTORY
SHARPER SKILLS FOR BETTER CAREERS



Proposal For Introducing

Advanced Diploma In Penetration Testing

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: Advanced Diploma In Penetration Testing

1. Aim & Objectives of the Course :

1. To make the students understand the concepts of Penetration Testing tools and concepts used in the evolving cyber threat landscape.
2. To introduce the students to the techniques and tools of penetration testing
3. To introduce the students to various attack simulation techniques using OSINT and Frameworks.
4. To introduce students to various aspects of penetration testing
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 :

Advanced Diploma in Penetration Testing

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 :

Name: Advanced Diploma in Penetration Testing

Course Code: ADPT

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	90	3	100	40	50	20	150	60
Adversary Simulation	Second	90							
Total		180		100	40	50	20	150	60

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

Summary:

Theory in HRS	Theory	Term-Work	Total
180	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 Advanced Diploma in penetration testing 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
ADPT	Section-I Foundation	3	100	40	50	20	150	60
	Section-II Adversary Simulation							

Syllabus for Advanced Diploma in Penetration Testing

Sr. No	Module Name	Topics	Objective	Tools/OS	Free/Open Source	Theory (40 Hrs)	Lab (Practical) 140 Hrs)
1	**Networking**	Overview of Network	Understanding the core concepts of how communication happens using networking devices and protocols.	IP configuration	Free & Open Source Tools	4 Hrs	14 Hrs
		Types of Networks		PING			
		OSI Model		Traceroute			
		TCP/IP Suite		NSlookup			
		IP addressing		SSH			
		MAC addressing		TELNET			
		Ports & Protocols					
2	**GNU/Linux**	Overview of Operating system	Understanding indepth GNU/Linux to efficiently deploy penetration testing frameworks which are primarily functional on unix based OS.	Ubuntu	Open Source OS & Tools	4 Hrs	14 Hrs
		Types of OS		apt			
		Introduction to Client & Server OS		wget			
		Introduction to GNU/ Linux		chmod			
		GNU/Linux Architecture		grep			
		Working with GNU/Linux commands		services			

3	**Foundation**	Introduction to VAPT Difference between VA & PT Importance of VAPT Need of VAPT in Organizations Setting up your LAB	To give a deeper insight into the various facets of VAPT in order to strategize the methodology for performing VAPT	Kali Linux	Open Source OS & Tools	4 Hrs	14 Hrs
4	**Pre-Engagement**	Overview Define Scope Questionnaire Start and End Date Dealing with third parties Goals of VAPT Line of communica-tion Rules of engagement	Understand-ing the overall scope of penetration testing engagement before it begins. Preventing scope creep.	Not Applicable	Not Applicable	4 Hrs	14 Hrs
5	**Intelligence Gathering**	Introduction to Intelligence Gathering Target Selection OSINT Covert Gathering Footprinting Identifying Protection Mechanism	To learn how to analyze the gathered information in order to match its relevance to the target.	Maltego Whois Archive Nmap Masscan Fping	Open Source OS & Tools	4 Hrs	14 Hrs

6	**Threat Modeling**	Introduction Asset Analysis Process Analysis Threat Agents Threat capability analysis Motivation Modeling	To learn how to analyze the information in order to prepare a profile of threat actors and entry points which can compromise an organization.	NA	NA	4 Hrs	14 Hrs
7	**Vulnerability Analysis**	Introduction to VA Active VA Passive VA Validation Research	To identify the vulnerabilities and understand the associated avenues of attack.	Nessus OpenVAS Nexpose Custom Scripts	Free & Open Source Tools	4 Hrs	14 Hrs
8	**Exploitation**	Introduction to Exploitation Basic Exploitation Client-Side Exploitation Social Engineering End-Point Evasion Techniques Customized Exploitation Introduction to ZeroDay	To learn how to gain initial access into an environment and circumvent security controls to achieve the goal.	Metasploit Frame-work John the Ripper Ncrack Setoolkit GoPhish Custom Scripts Air-crack-Ng Suite	Open Source OS & Tools	4 Hrs	14 Hrs

9	**Post-Exploitation (PE)**	Introduction to PE Rules of engagement Infrastructure Analysis Pillaging Privilege Escalation Pivoting Data Exfiltration Persistence Access Cleanup	Locating where sensitive data resides and moving laterally to compromise further systems.	Metasploit Frame-work Ettercap PassThe-Hash Bettrcap Custom Scripts	Open Source OS & Tools	4 Hrs	14 Hrs
10	**Report Writing**	Introduction to Report Writing Importance of Report Report Structure Executive Summary	Learning how to convey to superiors in a clear and unambiguous manner about how penetra-tion testing was conducted and analyzed, so that the superiors can take the appropriate decision.	NA	NA	4 Hrs	14 Hrs