SYLLABI

For

Value Added Course

Certificate Course in Advance Ethical Hacking

Offered by

Department of Information Communication and Technology

TECNIA INSTITUTE OF ADVANCED STUDIES

NAAC ACCREDITED GRADE 'A' INSTITUTE

3 PSP, Institutional Area, Sector – 14, Rohini, Delhi - 110085

Course Module

For

Value Added Course

Course Structure

S.No.	Contents Deliverance	Learning Outcomes
1	Introduction to Network Security (2 Hr)	Identify and exploit various types of vulnerabilities in computer systems, networks, and applications.
2	Advanced Web Application Security (3 Hr)	Understand and apply advanced techniques for reconnaissance, information gathering, and footprinting.
3	Advanced Exploitation Techniques (2 Hr)	Demonstrate proficiency in advanced exploitation techniques, including code injection, privilege escalation, and post-exploitation.
4	Advanced Cryptography (2 Hr)	Conduct advanced penetration testing using industry-standard methodologies and frameworks.
5	Advanced Malware Analysis and Reverse Engineering (3 Hr)	Apply advanced web application security techniques, such as bypassing security controls, exploiting authentication and authorization vulnerabilities, and understanding complex web application architectures.
6	Advanced Social Engineering (2 Hr)	Understand and mitigate wireless network security threats, including attacks against Wi-Fi networks, encryption cracking, and rogue access point detection.
7	Advanced Wireless Security (2 Hr)	Conduct reverse engineering and malware analysis to understand the behavior of malicious software and develop appropriate countermeasures.
8	Cloud Security and Virtualization (2 Hr)	Demonstrate knowledge and skills in network and infrastructure security, including firewall evasion, intrusion detection and prevention, and securing wireless networks.
9	Advanced Incident Response and Forensics (4 Hr)	Apply incident response techniques to effectively handle security incidents, identify root causes, and develop remediation strategies.
10	Red Team Operations (3 Hr)	Understand legal and ethical considerations associated with ethical hacking, including compliance with laws and regulations, obtaining proper authorization, and maintaining confidentiality and integrity of sensitive information.

11	IoT (Internet of Things) Security (3 Hr)	Use specialized tools and technologies for ethical hacking and security testing, such as Kali Linux, Metasploit, Burp Suite, and network sniffers.
12	Mobile Application Security (2 Hr)	Communicate and report findings effectively, both orally and in writing, to technical and non-technical stakeholders.

Reference:

1. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto, Oct 2011.
2. Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni- 15 July 2011.
3. CEH Certified Ethical Hacker All-in-One Exam Guide" by Matt Walker, McGraw-Hill Education,2012.
4. Gray Hat Hacking: The Ethical Hacker's Handbook" by Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, and Michael Baucom.2010.
5. Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman,2014.

Evaluation Pattern: On the basis of practical exam followed by viva.