Ethical Hacking Expert

This Course provides the opportunity to students & IT professionals who are interested to make career in Cyber Security. In this class, Students and Professionals learn about Viruses, Worms, Sniffers, Social Engineering, Denial of Service, Session Hacking, Hacking Web servers, Hacking Web Applications, SQL Injection, Hacking Wireless Networks, Evading IDS, Firewalls and Honeypots, Buffer Overflow, Cryptography etc. An Ethical Hacker is a Security Professional, who applies their Hacking Skills for Defensive Purposes on behalf of the Owners of Information systems. By using various Hacking Techniques and Tools, Ethical Hacker finds the weaknesses and vulnerabilities of Computer and Information Systems by duplicating the Intent and Actions of Malicious Hackers. Ethical Hacker looks what Information/Locations/Systems can an Attacker gain access to, what can an Attacker see on the Target, what can an Attacker do with available Information.

Audience: This course is designed for Students who are interested to make a career in Ethical Hacking/Cyber Security and are passionate to accept challenges with Technology in the IT Industry.

Course Objectives:

In this course, you will learn about:

- Hacking and why one should be Ethical about it.
- Different Attacks associated with Mobile and Cloud Technologies.
- Encrypting and Decrypting the Code.
- Different types of Attacks and how to mitigate them.
- Implementation of Tools to perform Ethical Hacking.

Course Outcome:

After completing this course, you will be able to:

- Discuss Hacking and the need for Ethical Hacking.
- Discuss Types of Attacks and how to Mitigate them.
- Discuss Attacks associated with Mobile and Cloud Technologies.
- Implement tools to perform Ethical Hacking.
- Encrypt and Decrypt the Code.

TOC Outline:

1. Exploring Ethical Hacking.
2. Gathering Information about Target Computer Systems - Foot printing and Investigation.
3. Scanning Computers in the Networks.
4. Enumeration- Listing the Systems/Users and Connecting them.
5. Gaining Access to Systems - Hacking.
6. Exploring Malware Threats and their Counter measures.
7. Monitoring and Capturing Data Packets using Sniffing.
8. Restricting the System Access - Denial of Service (DoS Attack).
9. Tricking People to gather Confidential Information - Social Engineering.
10. Web Servers and Threats associated with it.
11. Web Applications and Threats Associated with it.
12. Controlling User Session with Authenticated TCP Connection - Session Hijacking.
13. Injecting Code in Data Driven Applications: SQL Injection.
14. Hacking Mobile Platforms and Threats associated with it.
15. Encrypting and Decrypting the Code – Cryptography and its Types.
16. Evading IDS, Firewalls and Honeypots.
17. Wireless Networks and Threats associated with it.
18. Cloud Computing and Threats associated with it.
19. IoT Security.
20. Malware Protection.
21. Performing Hacking - LABS.

Exam Information:

Exam Code	:	S09-006	Exam Pattern	:	Multiple Choice
Exam Duration	:	3 Hrs	Exam Delivery	:	AEPTC (ACADEMIC EDUCATION & PROFESSIONAL TESTING CENTER)
Passing Score	:	75%			

Course Duration : 40 Hrs