

## **Course Details:**

### **Name of the course:**

Certificate program in Ethical Hacking & Counter Measures

### **About the course:**

In this course, student will start as a beginner with no previous knowledge about penetration testing or hacking. The first thing they will learn is some basic information about ethical hacking and the different fields in penetration testing. This course is focused on the practical side of penetration testing without neglecting the theory behind each attack. Before jumping into penetration testing, they will first learn how to set up a lab and install needed software to practice penetration testing on their own machine. All the attacks explained in this course are launched against real devices in lab-based sessions.

Course will help students in establishing a strong foundation towards their journey in the cyber security domain. As part of this cyber-security course, they will be learning about the various fundamental concepts and security essentials, cryptography, network security, Application Security, Data & Endpoint Security, Cloud Security, Cyber Attacks and Identity & Access Management.

### **Course Duration:**

8 Weeks – 96 hrs (4Days/week, 3hrs/day)

### **Course Outline:**

#### **Module 1: Introduction to Information Security**

- Why Security?
- The Security, functionality and ease of use Triangle
- Hacking vs. Information Security vs. Cracking
- Can Hacking be Ethical?
- Essential Terminology
- Elements of Security
- What does a Malicious Cracker do?
- Types of Security Professionals
- What do Ethical Hackers/ Information Security Professional do?

#### **Module 2: Masking your System**

- IP Masking
- MAC Masking
- Browser Masking
- OS Making
- Call Masking
- DNS Masking
- URL Masking
- Email Masking and Tracing

#### **Module 3: Exploration and Investigation**

- Defining Foot printing
- Information Gathering Methodology
- IPv4 network range / Mask / subnetting
- How DNS works?
- Tools:  
URL Extractor, Whois, Nslookup, ARIN, Traceroute, VisualRoute Trace, eMailTrackerPro etc...
- Collecting other Information  
Page Rank, Website Value, Tracing Victim IP address, Anonymous Mailing  
Finding people, Domain Lookup, Website Lookup, Email Bombing,  
Website Mirroring etc...

#### **Module 4: Google Dorking**

- Using Basic Operator in Google Dorking
- Searching anonymously any data based on query
- Searches made by using Logical operators
- CCTV searching
- Software search
- Creating new Google searches

#### **Module 5: Social Engineering**

- What is Social Engineering?
- Art of Manipulation
- Human Weakness
- Common Types of Social Engineering
- Human Based Impersonation
- Example of social engineering
- Computer Based Social Engineering
- Reverse Social Engineering
- Policies and procedures
- Security Policies-checklist

#### **Module 6: Scanning Networks**

- Definition of Scanning
- Objectives of Scanning
- Scanning Methodology
- Types of scanning
  - Port Scanning
  - Website Scanning
  - Server Scanning
  - Application Scanning
  - Banner Grabbing
- Tools  
Nmap, Nessus, Acunetix, wire shark etc...

#### **Module 7: System Security**

- Administrator Password Guessing

- Default Password Database
- Introduction to Windows Authentication Process
- Windows Password Cracking
- Cracking LM/NTLM hashes
- Creating Backdoors
- Clearing Password
- Brute Forcing Password
- Linux Password Cracking
- Password Cracking using Live OS
- Introduction to Metasploit
- Steganography

### **Module 8: Trojan and Viruses**

- What is Spy Wares?
- Trojan vs. Virus vs. Worms
- History of Virus/ Worm/ Trojan
- Creating Virus
- Creating Trojans
- Installing Key loggers

### **Module 9: Web Application Security**

- Owasp Top 10 (Open Web Application Security Product)
  - SOL Injection, CSRF, XSS etc.
- Phishing/ Phreaking

### **Module 10: Wi-Fi Attacks**

- How Wi-Fi Packets are Transfer?
- Sniffing Wi-Fi Packets
- Cracking WEP/ WPA/ WPA2 key

### **Module 11: Cryptography**

- Working of Encryption
- Digital Signature
- Digital Certificate
- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Symmetric vs Asymmetric
- Private vs Public Key Cryptography
- RSA (Rivest Shamir Adleman)
- DH Algorithm

### **Module 12: IDS (Intrusion Detection System)**

- Intrusion Detection Systems
- Ways to Detect Intrusion
- Types of Intrusion Detection System
- Intrusion Detection Tools
  - Snort etc.

- How to write rules in snort
- Log Analysis of Snort

**Key Outcomes:**

- Thorough introduction to ethical hacking
- Exposure to threat vectors and countermeasures
- Addresses emerging areas of IoT, cloud and mobile hacking
- Prepares you to combat Trojans, malware, backdoors, and more
- Enables you to hack using mobile