At EDUCBA, it is a matter of pride to us to make job oriented hands on courses available to anyone, any time and anywhere.

Learn at a time and place, and pace that is of your choice.

Plan your study to suit your convenience and schedule.

Penetration Testing Certification

Email Contact: info@educba.com

EDUCBA

www.educba.com

Course Overview

It contains many modules that contain Penetration Testing related methods and techniques such as beginner level and advanced level Penetration Testing and different types of malware and handling different types of viruses in different types of operating systems especially Kali Linux.

In-depth knowledge about how actual hacking is done, and how to test an environment and its reliability which people term as highly secure.

Penetration Testing Skills

We learn the following skills:

Ethical hacking, Penetration testing, Footprinting, Reconnaissance, Phishing Attacks, Trojans, Backdoors, Meterpreter, DNS Spoofing, ICMP, Hacking Android, Password Cracking, etc.

This Penetration Testing course is very useful in perspective of ethical hackers to the larger organizations that require safety and protection of their systems having a large number of customers and their personal records to be maintained to provide

Course Features

Course Duration- 21 + Hours

2 Number of Courses

Verifiable Certificates

Lifetime Access

Technical Excellence

About Penetration Testing

Penetration Testing is also called Ethical Hacking or Pent testing. It is an authorized cyber-attack on any computer system to analyze the security levels of the system in order to protect, safeguard, secure and maintain any confidential or sensitive data.

It is a kind of security testing to check the security level of an application.

Penetration Testing Course

This is a Bundle Course that includes complete in-depth Penetration Testing Learning Courses combined into one Complete Course.

This Bundle perfectly meets the requisite of the industry and gives you a better chance of being hired as a Penetration Testing Learning professional.

1 Kali Linux Penetration Testing

Section 1. Introduction

- Introduction to Ethical Hacking
- Penetration Testing

Section 2. Installation and Configuration

- Kali Linux
- Operating ASystems
- Installing Operating Systems
- Installing VMware Tools
- Configuring Kali Linux
- Installing Kali Linux on MacBook

Section 3. Footprinting and Reconnaisance

- What is Footprinting
- Footprinting Objectives
- Footprinting Tools
- Google Hacking
- Database and Query Hacking
- Database and Query Hacking Continue
- WhOIS Lookup

Section 4. Phishing Attacks

- DNS Footprinting
- Gathering Network Information
- Determining Operation System
- Phishing Attacks
- Creating Fake Websites
- Connecting Information Database
- Nmap and ZenMap
- Gathering System Information
- The Harvester
- Gathering Email Ids Using The Harvester
- WHOIS and Dnsenum
- Gathering Subdomain Information
- Urlcrazy and Dnsdict

Section 5. Social Engineering and information Gathering

- Social Engineering
- Types of Social Engineering
- Social Engineering Attacks
- Spear-Phishing Attack
- Phishing Attack
- Fake Page Attacks
- Mass Mailer Attack

Section 6. Trojans and Backdoors

- Types of Computer Malwares
- Different Ways of Infecting Viruses
- Dangerous Viruses of All time
- Melissa Virus and Love Bug
- Installing Rootkit Hunter
- Command Prompt Backdoor
- Backdoor - Gaining Access
- Backdoor - Maitaining Access
- Backdoor - Maitaining Access Continue
- Accessing a Backdoor in Windows 7 Via cmd Prompt
- Meterpreter Backdoor
- I am Root
- Forensic Escaping

Section 7. DNS Spoofing

- PDF Embedded Trojan Horse
- Java Applet Attack Method
- Java Runtime Attack Using Phishing Page
- MITM Attack
- ARP Poisoning
- DNS Spoofing vs DNS Poisoning
- DNS Spoofing
- Using Ettercap
- DHCP Spoofing
- Port Stealing
- ICMP Redirection
- Killing a Network
- Ddosing Unauthorised Network

1 Kali Linux Penetration Testing

Section 8. Denial of Service Attack

- Denial of Service Attack
- DoS vs DDoS
- Levels of Ddos Attacks
- Preventing DDoS Attacks
- Batch file attack
- Unseen DDoS SMB Attack

Section 9. Hacking Android

- Hacking Through Android
- Android Hacking Applications
- Hacking Android via Kali Linux

Section 10. Password Cracking

- Introduction to Password Cracking
- Password Cracking Srategy
- Windows Password Cracking
- Linux Hash Cracking
- Generating wordlist
- CeWL Cracking

Section 11. Wireless Hacking

- WEP and WPA
- WPA2
- 802.1X Standard
- Wireless Cracking Via Kali
- Cracking Networks

Section 12. Meterpreter

- Activating Payloads
- Proccess Module

Section 13. Metasploit

- Msfconsole Explained
- Msfconsole Commands
- Exploits
- Payloads
- Generating Payloads
- Encoders

1 Kali Linux Penetration Testing

Section 14. SQL injection

- SQL Injection
- SQL Injection to Google Dorks
- SQL Mapping via Kali Linux
- Gathering Password and Cracking the Hash

Section 15. Cryptography

- Cryptography
- Hash Func and Oracle Method
- Birthday Theorem and Digital Signature
- Pros and Cons of Cryptography

Section 16. Metasploit Database

- Importing Databases
- Exporting Databases

2 Advanced Penetration Testing

Section 1. Introduction

- Introduction to Pentesting

Section 2. NMAP

- Creating a Virtual Pentesting Lab
- Nmap Scanning
- Advanced Scanning
- Nmap Zombie Scan
- Nmap Timing Options
- Nmap Pre-Existing Scripts
- Simple Nmap Scripts

Section 3. Python Port Scanner

- Python Port Scanner
- SMTP Mail Server
- Samba Exploit
- NFS Exploit
- Grey Box and White Box
- The Malware
- Social Engineering

Section 4. Android Exploitation

- Android Exploitation

Section 5. Hashdump

- Hashdump and Password Phishing
- Automated Handler with Resource

Frequently Asked Questions

Why should I choose this Penetration Testing certification?

Any IT Security Engineer or IT Security Analyst or Security Engineer working on the IT Security Services and Security Operations or Security Testing and who are interested and willing to learn and master the Penetration Testing can also choose this Penetration Testing certification without any other thought.

Would this course add value to my profession?

Yes. this course would definitely add a great value to the learners' profile which would also contain verifiable certifications.

Is this a quick-fix to clear interview or do I still need to practice continuously while learning this Penetration Testing certification?

Yes, this course can be a quick-fix without any other previous knowledge or experience in computers or Penetration Testing or Security Testing or any other related pen testing techniques or security testing roles. This Penetration Testing certification needs to spend a minimum of 21 plus hours to complete.

Customer Reviews

This course is a great resource for entry-level and intermediate Information Security professionals. It is easy to follow and provides the fundamentals to pursue many different paths in Information Security. For entry-level InfoSec professionals, I would recommend taking some sort of networking refresher prior to this course.

Alex Ewin

This Penetration Testing Certification course on Kali Linux can be easily understood by beginners and also the presentation of the software's, tools and utilities as well as the step by step process in the videos are very clear and precise. For a beginner, this course can make you feel comfortable in using the various tools presented in the videos. Nice understanding of the concepts.

Daryll Malicsi

Nice overview of Kali Linux and usage. Learned some new things! I would recommend this course to anyone who is looking for an overview of the usages for Kali Linux.

I would recommend the course get updated to the latest version, as testing the material in my lab resulted in some differences. Great to learn and practice on same.x.

Sean Habing

EDUCBA

Penetration Testing Certification

For Queries please contact:

Email : info@educba.com

www.educba.com