CERTCOP
CERTIFIED CYBER COP

Certcop - A Division of Secbay

Certified Cybercop Kali Linux Pentester

CERTCOP
KALI LINUX PENTESTER

About Certcop

We combine the latest cyber tools with original in-house designs to develop customized and advanced cyber security programs to meet the client's requirements. CertCop offers training programs in the areas of pen testing using Kali Linux, Cyber Security Management, Incident Handling & Disaster Recovery, Application Security, Secure Coding, and customized SOC training programs according to client requirements.
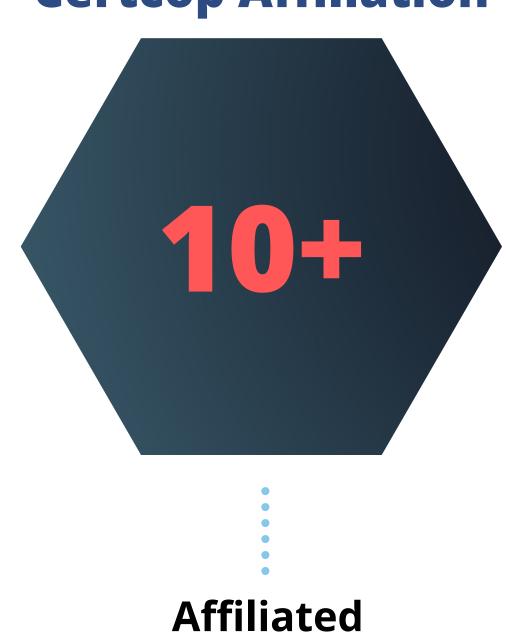
⬡ Certified and highly experienced instructors

⬡ Certcop Flexible Scheduling (Days, evenings, weekends)

Delivery Methods:

⬡ Virtual Live/In-Class/On-site/ 1 on 1/ On-Demand

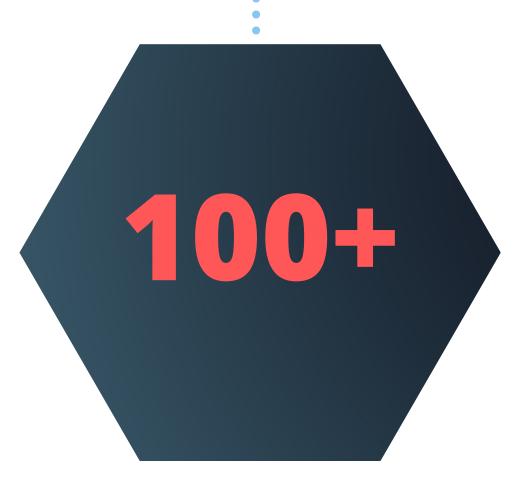⬡ Certcop Curriculum is of High Quality, Extensive, and Industry Standard.

Proud to be one of the
GLOBAL LEADERS in

CERTCOP
CERTIFIED CYBER COP

Certcop Affiliation

Certcop Trainings

Upcoming Cyber Security Training

10+

1000+

100+

Affiliated Certification Vendors

Corporate and Govt. Agencies Trained

Certcop Certcamps

CERTCOP
CERTIFIED CYBER COP

Partial List of Our Clients

EMC²

HARLEY-DAVIDSON MOTOR CYCLES

intel®

United Arab Emirates

DEPARTMENT OF THE NAVY · UNITED STATES OF AMERICA

U.S. DEPARTMENT OF HOMELAND SECURITY

StateFarm

at&t

THE GEORGE WASHINGTON UNIVERSITY

FEDERAL BUREAU OF INVESTIGATION · DEPARTMENT OF JUSTICE

Novell

MOTOROLA

accenture

Morgan Stanley

Microsoft

OUR DELIVERY METHODS

CERTCOP
CERTIFIED CYBER COP

Group Training

Individual Training

Instructor-Led Virtual live

Instructor-Led Classroom

On Demand

About Program

This program is extensively hands-on and will actively engage students in task-focused activities, and lab-based knowledge checks to ensure maximum skill transfer and retention.

This program is designed for IT and Cyber Security professionals new to Kali Linux. This program is extensively hands-on and will actively engage students in task-focused activities and lab-based knowledge checks to ensure maximum skill transfer and retention. In addition, a GUI-based environment will be featured to build on the student's existing technical knowledge. At the same time, command line concepts will be introduced to provide a foundation for students planning to work full-time in pen testing using Kali Linux.

Purpose of the Course:

The materials within this course focus on the knowledge, skills, and abilities identified within the specialty areas like:

- Cyber Defense Analysis
- Systems Analysis
- Technology R&D
- Vulnerability Assessment and Management
- Basic Linux and Security Concepts

Prerequisite

This course requires a basic familiarity with TCP/IP and operating system principles. It's a plus if you're familiar with the Linux command line, network security monitoring, and SIEM technologies. Some fundamental security concepts are expected at this level.

Exam Details

Course Name : Certified CyberCop – Kali Linux PenTester

Course Number : CertCopCKLPT19

Required exam – CKLPT-E019

Number of questions – Maximum of 100

Types of questions – Multiple-choice and performance-based

Length of test – 180 minutes

Passing score – 70% **–** This test has no scaled score; it's pass/fail only.

Languages – English

Retirement – Usually three years after launch

Testing Provider – Online proctoring: ExamIT.com

Certification Exam Voucher – $395 USD

Course Content

1.0 Kali Linux Introduction

- 1.0 A Bit of History
- 1.1 Basics of Linux
- 1.2 Components of Linux
- 1.3 Difference between Windows & Linux OS
- 1.4 Linux Distributions
- 1.5 Why Kali Linux?
- 1.6 Kali Linux Policies
- 1.7 Downloading & Installing Kali Linux
- 1.8 Downloading Kali Linux ISO Images
- 1.9 Installing Kali Linux on Hard-Disk

2.0 Linux Fundamentals

- 2.1 Unifying File Systems
- 2.2 Command Line - Terminal
- 2.3 Basic Linux Commands

3.0 Configure Kali Linux

- 3.1 Configuring the Network
- 3.2 Managing Unix Users And User Grou
- 3.3 Configure Services

4.0 Monitoring and Managing Linux processes

- 4.1 Network Security
- 4.2 Using Firewall for Network Security
- 4.3 Netfilter
- 4.4 Iptables and Rules
- 4.5 Logging
- 4.6 DPKG
- 4.7 IDS (Intrusion Detection System)

5.0 Package Management & Other Repositories

- 5.1 Introduction To Apt (Advanced Packaging Tool)
- 5.2 Kali Repositories
- 5.3 Installing packages
- 5.4 Removing and Purging Packages

6.0 Installing LAMP on Kali Linux

- 6.1 Web server
- 6.2 What are the components of a web server?
- 6.3 Installing and configuring Apache2
- 6.4 Installing and Configure MySQL
- 6.5 Installing NodeJS
- 6.6 Installing MariaDB
- 6.7 Installing & Configure PHP 7.0
- 6.8 Running your first web page on Kali

7.0 Information Gathering

- 7.1 OSINT Framework
- 7.2 UniScan
- 7.3 DirBuster
- 7.4 Nmap
- 7.5 Recon-ng
- 7.6 Maltego
- 7.7 Google Hacking
- 7.8 whois
- 7.9 theHarvester
- 7.10 Shodan

8.0 Vulnerability Assessment

- 8.1 NIKTO
- 8.2 WAPITI
- 8.3 WpScan
- 8.4 JoomScan
- 8.5 Drupwn
- 8.6 OpenVAS
- 8.7 CMSmap
- 8.8 BurpSuite
- 8.9 Netsparker
- 8.10 Nmap for Vulnerability Scanner

9.0 Web Application Exploitation

- 9.1 Introduction to Metasploit
- 9.2 Metasploit Framework Modules
- 9.3 Attacking Web Apps with Metasploit
- 9.4 SQL injection
- 9.5 Cross-site scripting and Types of XSS attacks on a web application
- 9.6 Directory listing
- 9.7 Netcat

10.0 Exploiting Windows / Linux / OSx

- 10.1 Pwning Windows with Meterpreter
- 10.2 ARP Poisoning
- 10.3 ARP Poisoning and MIMT Attacks
- 10.4 XArp
- 10.5 Phishing
- 10.6 Whaling

11.0 Password attacks

- 11.1 Types of Password Attacks
- 11.2 Hashcat
- 11.3 John the Ripper
- 11.4 Hydra
- 11.5 Mitigation of Brute Force Attack using Fail2Ban
- 11.6 Rainbow Table
- 11.7 Md5online, crack station

12.0 Wireless Attacks

- **12.1 Understanding Wireless Network Technologies**
- **12.2 Cracking WEP Network**
- **12.3 Evil Twin Attack**
- **12.4 Wireless Intrusion Prevention System**
- **12.5 Wi-Fi Chalking**
- **12.6 WIFI ANALYZER**
- **12.7 Ghost Framework -- Control Android Devices Remotely**
- **12.8 WLAN Security Countermeasures**
- **12.9 Wireless Intrusion Prevention Systems**
- **12.10 Mobile Security Threats**

13.0 Forensics

- **13.1 Android Debug Bridge (ADB)**
- **13.2 Installation Process of ADB in Different Platforms**
- **13.3 How to back up your android device's data using ADB**
- **13.4 How to restore your Android device's data using ADB**
- **13.5 AFLogical OSE**
- **13.6 Imagining Disk using Kali Linux**
- **13.7 Imaging Disk Using FTK® IMAGER**
- **13.8 Autospy**

Clients Testimonials

Got certified in Cybercop Red Team tutors are just great. They are very practical in their approach and help you learn things faster.
Bark - Security Analyst

The instructor was great and had amazing energy throughout. He also added a lot of additional material and customized the class. I really got what I needed out of this course.
AutoDesk

I enjoyed the Red Team course and want to stick with you guys for more training in the near future for Reconisense, Cloud Security, and Report Writing.
Marcus - Managing Director

CERTCOP
CERTIFIED CYBER COP

50+ Certcamp Location Across the Globe

Certcop - A Division of Secbay

info@certcop.com

CertCop, A Secbay Company
11710 Plaza America Drive Suite 2000
Reston, VA - USA