CERTCOP

CERTIFIED CYBER COP

Certcop - A Division of Secbay

Certified Cybercop Red Team

CERTCOP

RED TEAM CERTIFIED - OFFENSIVE SECURITY

CERTCOP
CERTIFIED CYBER COP

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.

CERTCOP
CERTIFIED CYBER COP

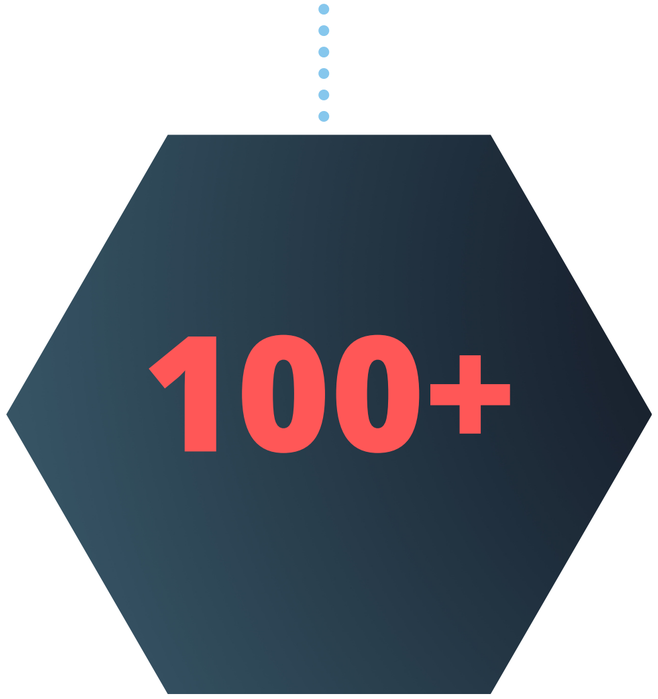
Proud to be one of the GLOBAL LEADERS in

Certcop Affiliation

Affiliated
Certification Vendors

Certcop Certcamps

Upcoming Cyber
Security Training



Certcop Trainings

Corporate and Govt.
Agencies Trained

CERTCOP
CERTIFIED CYBER COP

Partial List of Our Clients

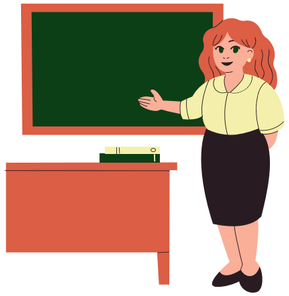
CERTCOP
CERTIFIED CYBER COP

OUR DELIVERY METHODS

Group Training

Individual Training

Instructor-Led Virtual live



Instructor-Led Classroom

On Demand

CERTCOP
CERTIFIED CYBER COP

About Program

The Certified Cybercop Red Team Certified Training is meant to turn you into a powerful Red Team expert who can defend against cyber attacks and conduct successful penetration testing to detect them. Our Red Team Training course is accredited and organized, and it includes all of the tools and strategies you'll need to become a competent Red Team Cyber Security specialist. With the Cybercop Red Team expert training, you will learn to imitate the thought process and attitude of hackers and digital criminals in order to offensively protect sensitive IT infrastructure.

CERTCOP
CERTIFIED CYBER COP

About Program

Target Audience

- 1. IT Professionals
- 2. Bounty Hunters
- 3. Entry Level Red Teamers
- 4. Pentesters
- 5. Cyber Security Analysts
- 6. Incident Responders

Requirements

- 1. Security & Network Basics
- 2. OWASP Top 10
- 3. Basic Incident Response Terminologies.

CERTCOP
CERTIFIED CYBER COP

Exam Details

Course Name : Certified CyberCop – Red Team
Course Number : CertCopRT02
Required exam – CCRT-E023
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

CERTCOP
CERTIFIED CYBER COP

Course Content

1.0 Red Team Methodology

- Intro what is a red team?
- Why do we need a red team?
- What is penetration testing and how is it different?
- What organizations should use Red Teaming-
- What is a Red Team Exercise- Red Team
- Purpose of a Red Team Exercise?
- Red Team Use Cases/Misuse Cases?
- What kind of person should be on a Red Team
- Why is it called Red Team?
- Difference Between Red Team and Blue Team
- How did the concept of Red Team come about?
- What is the goal of a red team?
- What kind of individuals are a good fit for the Red Team

CERTCOP
CERTIFIED CYBER COP

2.0 Legal Laws and Regulations

- Identify Legal Requirements pertaining to Red Team Engagements
- The target of the Engagement (Target of Evaluations)
- How to deal with Sensitive Data
- Client blames pen tester for loss of data
- How to get permission in writing – statement of Intent
- Confidentiality/Non-Disclosure Agreements
- Federally Mandated Red Team reporting
    - PCI, FERPA, HIPAA, HITEC, SOX, GLBA
- State Laws on Hacking
- Authorized Actions vs. Restricted Actions
- Two Person Integrity
- What constitutes a legal incident
- Legal Staff for Red Team engagements

CERTCOP
CERTIFIED CYBER COP

3.0 Recruiting Red Team Members

- Skills required
- Personality Traits
- Outsourcing vs Developing In-House
- Soft Skills
- Interpersonal Skills
- Project Management
- Project Phases
- Team Player
- Leadership

4.0 Scoping and Rules of Engagement

- Open Source Security Testing Methodology Manual (OSSTMM 3)
- Terms and Definitions
- Definition of Scope
- Definition of Rules of Engagement (ROE)
- How to properly Scope a Project
- Identify resources that are “in scope”
- Resources that are “out of scope”
- What happens if there’s a violation of ROE
- What is an Attack Surface

CERTCOP
CERTIFIED CYBER COP

5.0 Reconnaissance

- What is Reconnaissance ?
- What types of information?
- What is OSINT?
- Goals of the Reconnaissance Phase
- Tools
    - OSR Framework
    - UniScan
    - DirBuster
    - Nmap
    - Recon-ng
    - Maltego
    - Hunch.ly
    - Google Hacking Database /Google Dorking
    - OSINT Framework
    - Whois
    - Shodan / Censys
    - Spokeo/ThatsThem
    - DataSploit
    - Recon-ng
    - Sublist3r/TheHarvester
    - Social Media
    - Automater
    - Metagoofil
    - Internet Archive (Wayback Machine)

CERTCOP
CERTIFIED CYBER COP

6.0 Enumeration and Footprinting

- What is enumeration
- Control Enumeration
- Personnel Enumeration
- Footprinting
- Passive Footprinting
- Active Footprinting
- Enumeration of ports/Protocols:
- Services, OS version
- Windows Machines – SMB, NetBIOS, SNMP, LDAP
- Linux commands –
  - Finger
  - Uname
  - Pwd
  - Find
- Cat /etc/group, cat /etc/user cat /etc/shadow
- SNMP enum
- SMTP user enum
- DNS Enum
- Http Enum
- Banner grabbing
- OS Enumeration

CERTCOP
CERTIFIED CYBER COP

7.0 Shell Scripting-Programming Languages

- Introduction to Shell Scripting
- Different types of shells
- Shell commands
- Important Linux Commands
- Text editors
- Bash Scripting
- Python Scripting
- Perl Scripting

8.0 Web Application Penetration Testing

- Intro to Web Applications
- OWASP Top 10
- Why web application Pen tests are done?
- SDLC
- Web Servers
- Apache
- NGINX
- Installation of Web Server
- Enumerating services
- Web Application Penetration Testing Tools

CERTCOP
CERTIFIED CYBER COP

9.0 Cloud

- What Is Cloud Pen Testing
- What is Iaas , SaaS, PaaS (Cloud Service Models)
- Vulnerability Management In Cloud
- Cloud Pen Testing Tools
- Penetration Testing In The Cloud: AWS
- Penetration Testing In The Cloud: Google Cloud
- How To Cloud Platforms Get Compromised?
- Cloud Security
- Biometrics Security And Cloud

10.0 Exploit Frameworks/Exploit Kits

- Intro to Exploits
- Zero-Day Exploit
- Vulnerabilities CVEs
- Vulnerabilities vs Exploits
- Gaining Access
- Maintaining Access
- Covering Tracks
- Intro to Exploit Tools
- vPassword Cracking

CERTCOP
CERTIFIED CYBER COP

11.0 Physical Security

- Physical Security Penetration Testing
- Reconnaissance in Physical Security
- Types of Physical Security Controls
- Lockpicking
- Door Bypass
- Under door technique
- Bump keys
- Rec sensor bypass
- Physical Implant- USB Rubber Ducky, Bash Bunny, Bad USB
- Prox Card Bypass

12.0 Social Engineering

- What is Social Engineering
- How to perform Social Engineering
- Types of Social Engineering
- Examples of Social Engineering
- Preventing Social Engineering
- Social Engineering Tools

CERTCOP
CERTIFIED CYBER COP

13.0 Red Team Report Writing

- Introduction to Report Writing
- Technical Writing
- Knowing your Audience
- Types of Reports
- Controlling Access to Reports
- Working with Various teams on reports
- Report Generation Tools
- Report Template

14.0 Purple Team

- Introduction to Purple Team
- Why is purple teaming important?
- Traditional Approach
- Purple Teaming
- Conducting A Purple Teaming Exercise
- What Does A Purple Team Do?
- When Does An Organization Need A Purple Team?

CERTCOP
CERTIFIED CYBER COP

15.0 Wireless Networking

- Wireless Networking Definitions
- How wireless networking works
- Types of wireless networks
- Wireless networking standards
- Benefits of wireless networking
- Wireless Networking Threats
- Wireless Networking Tools

16.0 Incident Handling

- What is Incident Response
- Incident Handling
- Incident Response Policy/ Personnel/ Team Selection
- What is an incident plan
- Phases of Incident Response
- vIndicators of Compromise (IOCs)
- Incident Response Tools
- Jump Bag- a forensic toolkit
- Evidence Collection

CERTCOP
CERTIFIED CYBER COP

17.0 Internet of Things (IoT)

- What is the Internet of Things?
- How IoT relates to IOT, Cloud, and Big Data
- IoT devices
- Smart home, Smart cars
- Home appliances
- Medical Devices
- Drones
- Industrial Control Systems (ICS)
- SCADA Systems – RTUs, PLCs
- Wearables
- IoT Protocols
- IoT Tools
- OWASP IoT Top 10

18.0 Mobile Device Hacking

- Introduction to Mobile Device Hacking
- OWASP Top 10
- Mobile Application Attack Vectors
- Anatomy of Mobile Attack
- Types of Attack
- Android Device Hacking
- Android Rooting
- IOS Device Hacking
- IOS Jail Breaking

CERTCOP
CERTIFIED CYBER COP

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