IIT KANPUR
Indian Institute of Technology Kanpur

PROFESSIONAL CERTIFICATE PROGRAM IN

CYBERSECURITY - RED TEAM

Powered by simplilearn

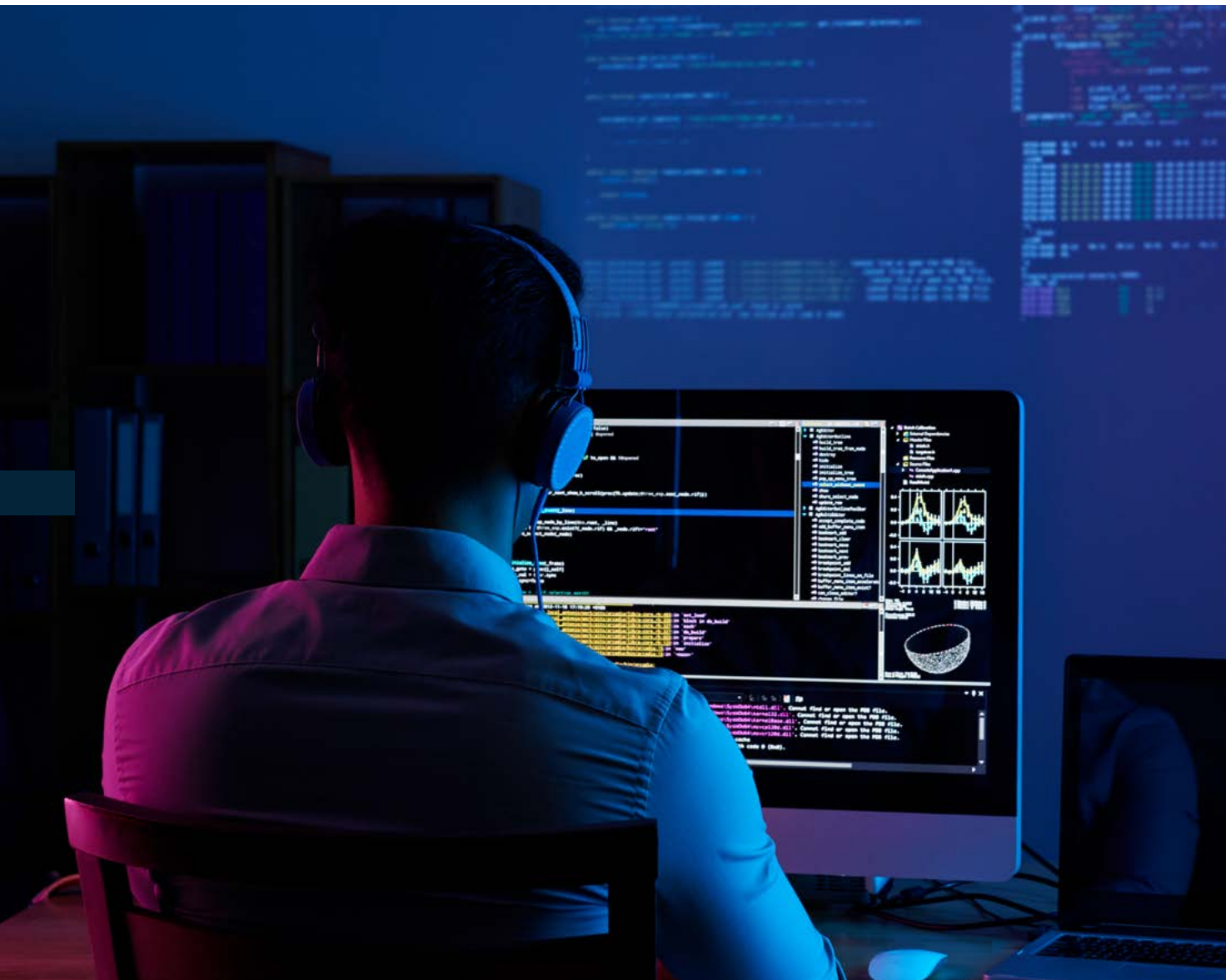


Table of Contents

About the Professional Certificate Program in Cybersecurity- Red Team

Cybersecurity skills are now among the most sought-after and highly-compensated skills as the business world has shifted towards a digital operational framework, and business data and organizational assets face an enhanced risk of cyber violations and cyberattacks. This Professional Certificate Program in Cybersecurity- Red Team equips you with the skills needed to become an expert in this rapidly growing domain.

This program features a mix of theory, case studies, and extensive hands-on practice to prepare you for an exciting career in cybersecurity. The program provides comprehensive education, leveraging IIT Kanpur's academic excellence. You will learn how to protect your infrastructure by securing data and information, conducting a risk analysis, architecting cloud-based security, and achieving compliance. You will also understand how to use ethical hacking and become an expert in analyzing vulnerability and penetration testing on various prototypes.

Key Features of the Program

Program Certificate

Program completion certificate from IIT Kanpur and Simplilearn

Top Instructors

Masterclasses from IIT Kanpur faculty

Capstone Project

Get hands-on experience with a capstone on industry-relevant use cases

Career Service

Simplilearn Career Service helps you get noticed by top hiring companies

Sandboxed Labs

Seamless access to integrated labs on Simplilearn's LMS

About Indian Institute of Technology Kanpur

IIT Kanpur is among the most prestigious and oldest educational institutes in India that offers various undergraduate, postgraduate, and integrated research programs in the field of engineering, science, management, and design.

You will receive training in the newest tools, technologies, methodologies, and concepts in cyber security through this curriculum, which was created in collaboration with IIT Kanpur. Get ready to successfully navigate the evolving cyber security world.

About Simplilearn

Simplilearn is the world's #1 online Bootcamp provider, enabling learners across the globe with rigorous and highly specialized training offered in partnership with world-renowned universities and leading corporations. We focus on emerging technologies and skills, such as data science, cloud computing, programming, and more, that are transforming the global economy. Our training is hands-on and immersive, including live virtual classes, integrated labs and projects, 24x7 support, and a collaborative learning environment. Over two million professionals and 2000 corporate training organizations across 150 countries have harnessed our award-winning programs to achieve their career and business goals.

Program Eligibility Criteria and Application Process

Eligibility Criteria

- Should have a bachelor's degree in a relevant discipline
- Do not require prior work experience
- Basic programming knowledge is not necessary

Application Process

There are three simple steps to gain admission to the Professional Certificate Program in Cybersecurity- Red Team:

STEP 1
SUBMIT AN APPLICATION

Complete the application and include a brief statement of purpose. The latter informs our admissions counselors why you're interested and whether you're qualified for the Bootcamp.

STEP 2
APPLICATION REVIEW

A panel of admissions counselors will review your application and statement of purpose to determine whether you qualify for acceptance.

STEP 3
ADMISSION

An offer of admission will be made to qualified candidates. You can accept this offer by paying the program fee.

Talk to an Admissions Counselor

We have a team of dedicated admissions counselors who are here to help guide you in the application process and related matters. They are available to:

- Address questions related to the application
- Assist with financial aid (if required)
- Help you resolve your questions and understand the program

Program Outcomes

At the end of this Professional Certificate Program in Cybersecurity- Red Team, you will:

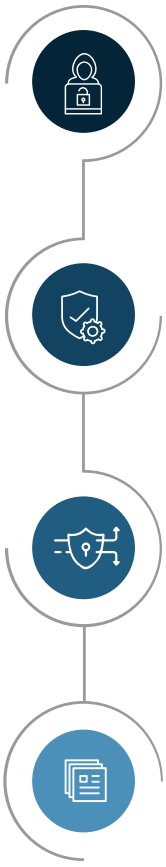
- Discover vulnerabilities from an attacker's perspective to address any shortcomings
- Adhere to ethical security behavior for risk analysis and mitigation
- Understand security in cloud computing architecture
- Implement cloud data storage architectures and security strategies and utilize them to analyze risks
- Create a secure network to counter security breaches
- Detect and respond to vulnerabilities and minimize exposure to security breaches
- Equip yourself with the tools and strategies to lead successful penetration testing initiatives
- Kickstart your tech career as a cybersecurity expert in top IT companies

Who Should Enroll in this Program?

This program caters to those who are hoping to enter the world of cybersecurity or want to update their skills as it is designed and structured to accommodate various professional backgrounds. Although there are no prerequisites for taking this training program, individuals in the following roles and disciplines are ideal for this course:

- Information Security Analyst
- Security Analyst
- Certified Ethical Hacker
- Security Consultant
- Information Security Manager
- Penetration Tester
- Vulnerability Tester
- Vulnerability Assessment Analyst
- Network Security Operations
- Application Security Vulnerability
- Cyber Penetration Testing Engineer
- CyberSecurity Applications Engineer
- Security Architect
- Security Administrator
- Pentest Security Engineer
- Cyber Penetration Testing Engineer
- CyberSecurity Applications Engineer
- Security Administrator

Learning Path Visualization



01 Ethical Hacking

02 Vulnerability Assessment

03 Penetration Testing

04 Capstone Project

Electives

Academic masterclass: Cybersecurity

Ethical Hacking

You will learn more about the concepts, consequences, distinctions, and limitations of ethical hacking in this course. You will assist an organization in the task of implementing new hack-prevention strategies and technologies to safeguard systems from becoming a target of hackers.

Key Learning Objectives

- Learn how to use online open-source intelligence applications for passive reconnaissance
- Execute footprinting and reconnaissance, a crucial pre-attack part of the ethical hacking process using the most recent methods and technologies
- Master multiple scanning techniques using NMAP and NPING, and conduct scanning on the target network outside of IDS and firewall
- Understand the workings of web applications and web servers, their vulnerabilities, and how to prevent attacks

Course Curriculum

- **Introduction to Ethical Hacking**
  - Ethical Hacking
  - Concepts & Outcome
  - Differences & Limitations
- **Introduction To Cyber Kill Chain®**
- **Footprinting & Reconnaissance**
  - Introduction to Reconnaissance
  - Passive Reconnaissance
  - Active Reconnaissance
  - Counter Measures

Scanning Networks

- Network Scanning Concepts
- Scanning Tools
- Port Scanning Techniques
- IDS/Firewall Evasion Techniques
- Banner Grabbing
- Draw Network Diagram

Enumeration

- What is Enumeration
- LDAP Enumeration
- NetBIOS Enumeration
- DNS Enumeration
- Enumeration Defence

Vulnerability Identification & Exploit Selection

- Vulnerability Assessment
- Vulnerability Assessment Solutions
- Vulnerability Scoring System
- Exploit DB

System Hacking

- System Hacking Introduction
- Password Cracking
- Privileged Escalation
- Executing Applications
- Data Hiding
- Covering Tracks

Malware

- Malware Concepts
- Viruses and Worms
- Trojans
- Malware Analysis
- Anti-Malware Software

Sniffing

- Sniffing Concepts
- Sniffing Techniques
  - MAC Attack
  - ARP Positioning
  - Spoofing Attack
  - DNS Poisoning
- Sniffing Tools
- Defending and Countermeasures Techniques Against Sniffing

Social Engineering

- Social Engineering Concepts
- Social Engineering Attacks
- Insider Threats
- Social Networking Sites
- Identity Theft
- Assisted Demo: Getting Email IDs Available in the Public Domain using the Harvester

Denial of Service

- DoS/DDoS Concepts
- DoS/DDoS Attack Techniques

Session Hijacking

- Session Hijacking Concepts
- Application-level Session Hijacking
- Network-level Session Hijacking
- Countermeasures

Evading IDS, Firewalls, and Honeypots

- IDS/IPS - Basic Concepts
- Firewalls - Basic Concepts
- Honeypots
- How to Detect a Honeypot

Hacking Web Servers

- Webserver Concepts
- Web Server Attack Methodologies
- Web Server Attacks
- Patch Management
- Web Server Security

Hacking Web Applications

- Web Application Concepts
- Web App Threats
- Hacking Methodologies
- Hacking Tools
- Countermeasures

SQL Injection

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Tools
- Countermeasures

Hacking Wireless Networks

- Concepts and Terminology
- Wireless Encryption
- Wireless Hacking
- Wireless Attacks
- Wireless Encryption Attacks
- Protecting Wireless Networks

Hacking Mobile Platforms & IoT

- Mobile Platform Hacking
- Countermeasures
- Mobile Attacks
- Improving Mobile Security
- IoT Concepts
- IoT Technology Protocols
- IoT Operating Systems
- IoT Communication Models
- IoT Vulnerabilities and Attacks
- IoT Hacking Methodology
- Countermeasures

Cryptography

- Cryptography Concepts
- Encryption Algorithms
- Hashes
- Public Key Infrastructure
- Disk Encryption
- Email Encryption
- Cryptanalysis
- Countermeasures

Cloud Computing

- Cloud Computing Concepts
- Cloud Computing Threats
- Cloud Computing Attacks
- Cloud Security Control Layers
- Cloud Security Tools

Vulnerability Assessment

In this course, you will learn how to analyze security flaws in an information system systematically. Determine whether the system is susceptible to any known vulnerabilities, rate the seriousness of those vulnerabilities, and, as necessary, make recommendations for mitigation or for managing risk.

Key Learning Objectives

- Build a safe and secure system and gain knowledge of the principles of vulnerability assessment and reconnaissance to protect your infrastructure and web presence
- Utilize practical exploits and assess how they affect your systems
- Evaluate the risk assessment and perform threat modeling of a web application architecture
- Create a successful vulnerability management strategy

Course Curriculum

- **Lesson 1: Fundamentals of Vulnerability Assessment**
  - Introduction
  - Scanning and Exploits
  - Assisted Demo
- **Lesson 2: Analyzing Vulnerabilities and Exploits**
  - Uncovering Infrastructure Vulnerabilities
  - Attacks Against Analyzers and IDS
  - Exposing Server Vulnerabilities
  - Assisted Demo
  - Revealing Desktop Vulnerabilities
- **Lesson 3: Configuring Scanners and Generating Reports**
  - Implementing Scanner Operations and Configurations
  - Creating and Interpreting Reports
  - Assisted Demo

- **Lesson 4: Assessing Risks in a Changing Environment**
  - Researching Alert Information
  - Identifying Factors that Affect Risk
- **Lesson 5: Risk Calculation**
  - Risk Standard
- **Lesson 6: Managing Vulnerabilities**
  - The Vulnerability Management Cycle
  - Vulnerability Controversies

Penetration Testing

In this course, you will execute an attack on a computer system to evaluate its security. You will examine whether a system is robust enough to withstand attacks from authenticated and unauthenticated positions, as well as a range of system roles.or for managing risk.

Key Learning Objectives

- Examine the organization's risk exposure on both local and wide area networks
- Conduct penetration testing on web applications to secure and stabilize a system
- Simulate a variety of attacks that could threaten a business
- Creating custom packets using Netcat

Course Curriculum

- **Introduction to Penetration Testing**
  - Penetration Testing
  - Setting up a Hacking Lab
  - Phases of Penetration Testing
- **Introduction to Kali Linux**
- **Reconnaissance**
  - Introduction to Reconnaissance
  - Passive Reconnaissance
  - Active Reconnaissance
- **Scanning Networks**
  - Network Scanning Concepts
  - Scanning Tools
  - Port Scanning Techniques
- **Vulnerability Analysis**
- **Web Application Penetration Testing**
  - Exploit Identification
  - Web Application Concepts
  - Web App Threats
  - Web Application PT
  - Assisted Demo
- **System Penetration Testing**
  - Exploiting and Gaining Access
  - Setting up Metasploitable
  - Exploitation
  - Assisted Demo
  - Windows 10 Exploit
- **Gaining Access**
- **Post Exploitation**
- **Anonymity**

Certification

INDIAN INSTITUTE OF TECHNOLOGY KANPUR
Centre for Continuing Education

Certificate of Completion

This is to certify that

Jordan Smith

has successfully completed the

Professional Certificate Program in Cybersecurity- Red Team

Held during from 01/11/2022 to 01/05/2023

Certificate ID: 51190127

https://success.simplilearn.com/33a69d51-c7a0-4fd4-9c79-bbda7be5cbfc

Dr. Sandeep Shukla
IIT Kanpur

Prof. BV Ratish Kumar
Head CCE, IIT Kanpur

Program delivered by simplilearn

Advisory Board Members

Sandeep Shukla

Professor, Computer Science and Engineering at Indian Institute of Technology, Kanpur

Sandeep Shukla is the Coordinator, Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructure, IIT Kanpur. He has a Ph.D. and MS in Computer Science from the State University of New York and 28+ years of experience as a technology professional and revered academic.

simplilearn

USA

Simplilearn Americas, Inc.
201 Spear Street, Suite 1100, San Francisco, CA 94105
United States
Phone No: +1-844-532-7688

INDIA

Simplilearn Solutions Pvt Ltd.
53/1 C, Manoj Arcade, 24th Main, Harlkunte
2nd Sector, HSR Layout
Bangalore - 560102
Call us at: 1800-212-7688

www.simplilearn.com