



# Certified Cybersecurity Professional

**Learn from the best in the industry**

**4 Months Training**

**6 Months Internship**

**Career in the most  
in-demand IT stream**

A programme by




**StrongBox IT**

Security | Performance | Automation

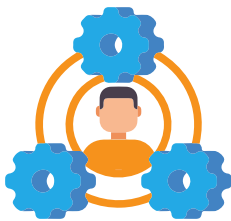


**If you think you know-it-all  
about cybersecurity,  
this discipline was probably  
ill-explained to you.**

- Stephane Nappo 

Cyberattacks and Data breaches are rapidly rising, along with the costs associated with recouping from a cyberattack. Organizations globally are increasing their budgets to build advanced cyber security measures to combat this and to avoid losing billions of dollars.

Global enterprises are preparing for this challenge by consistently upskilling their employees, hiring skilled cyber security professionals, and partnering with leading cybersecurity organizations like StrongBox IT.



**GLOBAL SKILLS SHORTAGE**

3.4 Million more professionals needed to cover a gap that has increased by 26% in 2021 compared to 2020.

- Infosecurity-Magazine, Oct 2021



**2MILLION JOBS**

Will still go unfulfilled in 2022.

-Tech Target, August 2022



**\$2.6 BILLION**

will be spent on cyber risk management by Indian users in 2022.

Cybersecurity professionals find weaknesses in databases, networks, hardware, firewalls and encryption. Cybersecurity professionals are responsible for protecting their company's information and data from attacks by hackers, viruses, or other cyber threats

The Certified Cyber Security Professional training program equips you with the skills that the industry seeks most, an offensive and a defensive approach to security. The program is ideal for professionals and final year students, with a background in IT related streams and an exposure to programming/networking. This program is a pathway to create a successful career in the one of the highest paying professions in Information Technology.



# Programme Highlights

At StrongBox IT, we are in a constant race to better ourselves in terms of technical expertise and our delivery excellence. This program is specifically designed to expand our team with a set of professionals who are at par with the best in the world. With real world exposure to how web and mobile applications, infrastructure and connected devices can be hacked and the advisories that are given to secure them, you as a participant will be a ready and through cybersecurity professional at the end of this training. What's more! You will directly join our team of white hat hackers or choose a place of your liking.



A comprehensive curriculum to become industry-ready



Interactive live mentorship with industry experts



Incentives for further certifications



Lab sessions to gain hands-on experience



Internship and Training in real projects



The curriculum is designed to cater to various professional needs. Whether you're an early-career professional looking to build a career in cyber security or a mid-level IT professional looking to transition into a career in cyber security, this programme will help you align your learning to your professional goals.



## Young professionals

Learn the core concepts of cyber security and build a solid foundation using the in-demand market skills. You will benefit from this if you are:

- ➔ A professional looking to transition into a career in cyber security
- ➔ A fresh graduate wanting to break into the cyber security domain
- ➔ An IT infrastructure manager wanting to upskill with cyber security



## Mid-level Professionals

In addition to the concepts, the programme gives you a high-level strategic overview of the best cyber defence practices, enabling you to analyse the threat landscape and strategise towards appropriate cyber security measures. You will benefit from this if you are:

- ➔ A mid-level manager involved in cyber security governance and decision making for your organisation

**Successful completion of this program will qualify you for various roles in cyber security, including:**



Cyber Security Analyst



Information Security Specialist



Cyber Threat Intelligence Analyst



Cloud Security Analyst



# Programme Outcomes

The program also helps in preparing learners for the Offensive Security and EC-Council certifications.



1. Develop the Security Mindset



2. Perform security validations on enterprise infrastructure inline with SANS and NIST standards. Assess the risk and respond. Write clear and world-class incident reports



3. Familiarize yourself with the Standards and Frameworks such as: MITRE ATT&CK, Center for Internet Security (CIS) Benchmarks



4. Perform web application penetration testing following the OWASP TOP 10 threat vector models



5. Interact with a global customer base understanding their cybersecurity needs and appropriate it to their business requirements



6. Become an expert in vulnerability assessment, penetration testing and red teaming

The program also helps in preparing learners for the Offensive Security and EC-Council certifications.



# Curriculum

The programme is designed to start strong with the foundations of cyber security, where you learn the basics of protocols, transmission, cryptography, operating systems, and technology stacks. You then delve into the various types of cyberattacks. After you've mastered the attacks, you'll learn how to carry them out on target infrastructure as well as web and mobile applications. Understanding how these can be hacked into and compromised, you start to learn how these attacks can be prevented. You also learn how the attack patterns and recommendations can be reported to the clients as per globally accepted standards, interact with clients to help them understand the findings and implement secure controls to safeguard their IT assets.



## **MODULE 1:**

### **CYBER SECURITY FUNDAMENTALS | 4 WEEKS**

Learn the fundamentals of Cyber Security, Kali Linux, Windows OS, networking, and cryptography.



## **MODULE 2:**

### **INFRASTRUCTURE SECURITY | 4 WEEKS**

Learn about the various stages of an infrastructure attack, like information gathering, target scanning, and enumeration to gain access, perform privilege escalation, and exploitation.



### **MODULE 3:**

#### **SHELL SCRIPTING | 2 WEEKS**

Learn about shell scripting, write custom rules, and custom tool to perform penetration testing.



### **MODULE 4:**

#### **SERVER SECURITY | 4 WEEKS**

Learn to configure different services like HTTP, database, FTP, and SSH servers and harden these services in both a Linux and Windows environment.

Learn to use the Incident Response Playbook to defend against an ongoing cyber-attack and protect critical digital resources in this situation.



### **MODULE 5:**

#### **WEB APPLICATION SECURITY | 6 WEEKS**

Learn about the web application architecture and how to use the latest web hacking tools and techniques to perform different attacks such as XSS, injection, and privilege escalation on web applications. You will also learn about the latest defensive countermeasures used to make the application more resistant to cyberattacks.



### **MODULE 6:**

#### **MOBILE APPLICATION SECURITY | 4 WEEKS**

Learn about the Android System Architecture and how to root Android devices and bypass SSL pinning using the most up-to-date mobile hacking tools and techniques. Learn to deeply analyse the mobile app, operating system, and supporting components. Learn about the defensive techniques that can be used to harden your mobile application and make it more resistant to cyber-attacks.

## TOPICS

- ✓ CIA Triad
- ✓ Authentication, authorization, and accounting
- ✓ Zero Day Attacks
- ✓ TCP/IP and the OSI Model
- ✓ Wireshark
- ✓ Routing and Switching
- ✓ Firewall
- ✓ VPN
- ✓ Windows Fundamentals
- ✓ Linux Fundamentals

## KEY TAKEAWAYS

- Understand the fundamental principles of cyber security, like CIA, AAA, and cryptography.
- Understand the fundamentals of networking and network security.
- Understand the workings of network devices like routers, switches, firewalls, and VPNs.
- By the end of the course, you will be able to understand the various phases of hacking, networking protocols, and be proficient in using Kali for various hacking engagements.








## TOPICS

- Network Exploitation
- Reconnaissance
- Packet crafting
- NMAP
- Testing Firewall
- Hacking application services
- Wireless Network Hacking
- Nessus, Netcat
- Hacking passwords






## KEY TAKEAWAYS

- Understand the different phases of a cyberattack.
- Perform reconnaissance of the target network and devices.
- Craft packets to evade network security devices like firewalls and perform DDOS attacks.
- Attack services using the information gained during the reconnaissance.
- Perform an attack on the wireless network.
- Perform reconnaissance of the target network and devices.
- At the end of the module, the student will be fluent in performing different network-based attacks, cracking passwords, and hacking wireless networks.











**TOPICS**

-  Introduction to Shell Scripting
-  Using variable in Shell scripting.
-  Basic commands
-  Writing Custom tool.
-  Piping

**KEY TAKEAWAYS**

-  Understand and write your own shell script.
-  Write custom scanner scripts.
-  Create custom encrypted and decrypted files.
-  Write a custom password generator.
-  At the end of the module, the student will be able to write custom tools and scripts to perform different types of reconnaissance or attack activity.

**TOPICS**

- |   |  |
|---|--|
|  BIOS Security     |  User Management                      |
|  Security Policy   |  Database Architecture                |
|  Event Log         |  Basics of SQL'                       |
|  Windows hardening |  Hardening the SQL service.           |
|  Linux hardening   |  Recovery from an Incident: Forensics |

**KEY TAKEAWAYS**

- Learn how to secure your Linux server and services.
- Learn how to secure your Windows server and services.
- Learn how to secure the OS boot process.
- Learn how to secure a database server.
- At the end of the course, the student will understand the different ways the application can be compromised and how to secure these services.







## TOPICS

- Web Application Architecture
- OWASP 10
- Injection Attack
- Broken authentication and authorization
- XSS Attack
- Burp
- secure coding practices.
- Insecure Direct Object Reference








## KEY TAKEAWAYS

- Learn the architecture of the Web application.
- Perform injection attacks such as command injection, SQL injection, and LDAP injection.
- Perform a broken authentication and authorization attack.
- Learn to use Burp Suite to perform various attacks.
- Learn the mitigation techniques to harden the application against the attack.
- At the end of the module, the student will be fluent in using the Burp Suite proxy tool and well versed in compromising application security.

**TOPICS**

-  Android Architecture  ADB
-  Mobile [OWASP 10]
-  Bypass SSL pinning
-  SAST
-  DAST

**KEY TAKEAWAYS**

-  Learn the architecture of the Android.
-  Learn about the OWASP mobile vulnerabilities.
-  Learn how to exploit these mobile OWASP vulnerabilities.
-  Learn how to bypass SSL pinning.
-  Learn about SAST and DAST testing.
-  Learn to use tools such as Drozer, ADB, and MobSF.
-  At the end of the module, the student will be aware of the Android architecture and Be well versed in compromising the mobile app using different hacking techniques.

# Admission Process

## Programme Eligibility

Applicants should be a graduate or a final semester student in any of the IT streams and must have an exposure to Linux, Shell scripting and Python.

The number of seats for this program is 10 and the participants will be evaluated on a first come first serve basis. The admission process is closed once the requisite number of candidates have been enrolled into the program.

## Selection Process



### APPLY

Apply by filling a simple online application form



### SCREENING PROCESS

Attend an application screening call



### JOIN PROGRAMME

An offer letter will be rolled out to selected candidates

## Programme Fee

Online application form

<https://buff.ly/3HXA9oZ>

# INR 1,50,000 + GST

Please get in touch with a Program Advisor for details on installment options.

**Registration Closes on 5th March**

March 2023 – Jun 2023 – Training

July 2023 – Dec 2023 – Internship with a stipend of Rs.25,000 per month.

Jan 2024 – Assured placement with StrongBox IT, at market standards ( minimum of Rs. 40,000 per month)