CYBER A1

CYBER SECURITY INTERNSHIP

Certification | Hands-on Exposure

Research Project | LiveTasks

60 + Hour Training
Currently Online

Who is this Training For?

- For individuals who wants to pursue their career in cybersecurity and gain professional hands on experience of the industry needs.

- This program is specially designed for beginner as well as intermediate cyber security enthusiast.

- This Training- is for individuals, who wants to learn and explore real world Ethical Hacking skills.

- This is not just a certification course, but also a Training-Internship program which will help you transfer skills to CEH, Security+, OSCP, and other hands-on certifications.

Description

CyberSecurity, one of the fastest-growing and highest-paying careers, with over 1 Million cybersecurity job openings available this year. This Ethical -Training is packed with real- world practical examples guided by Industry professionals. It also includes Live Practical, Research Project & Challenges.

which will be mentored by experts at CYBER A1 Security.
Working on Live Projects will help you sharpen your skills.
After the completion of this Ethical Hacking Training you will be capable enough to pursue a career in the field of Cyber Security.

Prerequisites

- Basic IT Skills

- Basic Linux, programming or hacking knowledge required.

- Computer with a minimum of 4GB ram/memory.
  - (i3 , 8 GB RAM , 120 SSD)

- Operating System: Windows / OS X / Linux.

What does this Internship-Training include?

Module 1:

- Introduction
- Check Your Skillset
  - ssh
  - http
  - https
  - ftp
  - Server Client
  - Server
  - LInux
  - Windows server
  - ADDS
  - Dns

Module 2:

- CTF
  - Vulnhub Box
  - HackThe Box
  - Try HackMe

Tools
Nmap,BurpSuite , Stegnography , Metasploit, Netcat,etc..
Reverse Shell (php)

Module 3:

- Scanning
- Theory Behind Scanning
- Nmap
  - Nmap Basics
  - nmap scan Techniques
  - Nmap Port Specification
  - Nmap Service and Version Detection
  - Nmap OS Detection
  - Nmap Scripting Engine
  - Nmap Output
  - etc..
-

What does this Ethical Hacking-Training include?

Module 4:

- Burpsuite

  - proxy
  - spider
  - Repeater
  - Decoder
  - Extention
  - Intruder

Module 5:

- Lab Setup
  - CTF , Vulnerable Machine , Live Target

Module 6:

- Recon
  - Automation (Bash) , Subdoamin Gather , Live , 200, 300, 403,404
  - Github Dork , Google Dork , Explot DB.

Module 7:

- A1:2017-Injection
- A2:2017-Broken Authentication
- A3:2017-Sensitive Data Exposure
- A4:2017-XML External Entities (XXE)
- A5:2017-Broken Access Control
- A6:2017-Security Misconfiguration
- A7:2017-Cross-Site Scripting (XSS)
- A8:2017-Insecure Deserialization
- A9:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging & Monitoring

Module 8:

- HTML injection
- File Inclusion
- Directory Traversal
- Mitigation

What does this Ethical Hacking-Training include?

Module 9:

- Host Header Attack
- Parameter Tampering
- Missing/insufficient SPF record
- Mitigation

Module 10:

- Authentication Bypass
- OTP Bypass
- Login Bypass Manipulate response
- Mitigation

Module 11:

- No Rate-Limit Attacks
- Bypass No Rate Limit
- Mitigation

Module 12:

- Subdomain takeover

Module 13:

- Broken link hijack (Social Media)

Module 14:

- Cross Site Scripting (XSS)

  - Stored XSS Attacks
  - Reflected XSS Attacks
  - DOM XSS

What does this Ethical Hacking-Training include?

Module 15 :

- Sql Injection
- CMS HACKING

Module 16:

- Cross Site Request Forgery (CSRF)
- Cross Origin Resource Sharing (CORS)

Module 17 :

- How to start with Bug Bounty Platforms
  - Hackerone
  - OpenBug Bounty
  - Bug Crowd
  - Yes We Hack
  - etc..

Module 18:

- CVE Hunting
  - 2020-5902
  - 2020-3452
  - 2020-3187 and etc

Module 19 :

- Report Writing
  - tools For Better POC Genaration
  - Visual Tools
  - Automation

Module 20:

BONUS Lecture

ALL TOPIC PRACTICAL BASE ON LIVE TARGET

What is the career path after Internship?

The top organizations like such as Infosys, Wipro, TCS, Tech Mahindra, IBM etc. are seeking good ethical hackers. The profiles that are on offer include Security Executive, Web Security Manager/Administrator, Network Security Administrator, Network Security Systems Manager and much more.

What is the next step after Internship?

So You Are ready to work as freelancer Hacker or Bug Bounty Hunter,
Or you can apply as VAPT Engineer or Web Penetration Tester to global company like TCS, Wipro, HCL ,Capgemini etc

Online Interactive Classroom with dedicated Faculty

The course fee is Rs.18,000/

LIMITED TIME OFFER

Secure The Digital