Introduction to Offensive Security Certified Professional

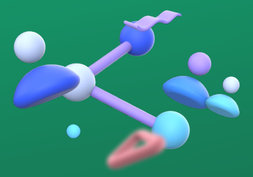
Bootcamp

Host,

VISHNU VIJAYAN V S Founder, Nixie_Bytes Security Team 🤘 Co-founder, Cyfosis Cyber Solutions

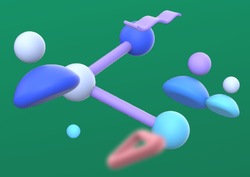
Hi there!

Psst.. Glad you scrolled through!
Let’s have a look into what this introduction to offensive security certified professional bootcamp consists of, shall we?



Offensive Security Certified Professional

The OSCP is a well-respected ethical hacking certification offered by Offensive Security, a company that specializes in penetration testing training and certifications. Offensive Security offers several certifications but the OSCP is probably one of the most well-known.



Bootcamp

Pentesting is a hard thing, It’s even harder to figure out how to get started on this journey. This Boot-camp is aimed at absolute beginners and to give them an easy to understand learning path.

In this Boot camp we are focus on to crack OSCP like box Kioptrix . Kioptrix boot-to-root VM is well known as a good starter vulnerable machine for hacking challenges. This is especially true for persons looking to pursue the OSCP certification, as it is considered to be beginner friendly.

Time Taken to Complete the Bootcamp — 25 hours

5 days of hands-on workshop with 5 hours per day

01 /06

Introduction to Cyber Security

In this Session we discuss about the basics of cyber seurity and key elements of cyber security.

Contents

NEXT PAGE >

02 /06

Fundamentals of Cyber Security

In this Session we discussed about the fundamentals of Cyber Security & types of acttacking vectors

Contents

03 /06

Setting up a lab

In this Session we discuss about how to set up virtual labs for hacking & testing our skills

Contents

NEXT PAGE >

04 /06

Linux Basics (OS)

In this Session we Explore about the amazing linux operating system, How it work?, main commanads, main Functions etc.

Contents

05 /06

Introduction to Network

To get a big-picture understanding of networking as a field and how the concept of layering makes the operation of large-scale networks possible.

Contents

05 /06

Introduction to Network

To get a big-picture understanding of networking as a field and how the concept of layering makes the operation of large-scale networks possible.

Contents

NEXT PAGE ›

05 /06

5 Stages of Hacking

01

Information Gathering

Information Gathering means gathering different kinds of information about the target. It is basically, the first step or the beginning stage of Ethical Hacking

02

Scanning & Enumeration

This module covers phase two of an attack. Scanning and enumeration is the phase where the attacker begins to “touch” the systems.

Contents

Information Gathering

01 **Email harvesting**

Find the all mails under main domain

02 **Subdomain gathering**

find all the sundomain under main domain

03 **Identify web technology**

this session we find out which are the technologies used behind the web applications

NEXT PAGE >

05 /06

5 Stages of Hacking

01

Information Gathering

Information Gathering means gathering different kinds of information about the target. It is basically, the first step or the beginning stage of Ethical Hacking

02

Scanning & Enumeration

This module covers phase two of an attack. Scanning and enumeration is the phase where the attacker begins to “touch” the systems.

Contents

Scanning & Enumeration

NEXT PAGE >

04 /06

Exploitation Basics

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce vitae arcu id leo ultrices tristique.

Contents

NEXT PAGE >

System Requirements

Make sure you are meeting the minimum requirements so you can attend this Bootcamp.

Prerequirements

Windows **Linux** — Minimum System Requirements

Operating System	Windows 64-bit (VM Blackubantu & Ralph)
Ram	4 GB ~ 8 GB
Disk Space	40 GB ~ 50 GB
Support for Virtualization enabled via BIOS	

WRAP UP >

Thank You!

THAT'S A WRAP. SEE YOU ALL AT THE BOOTCAMP!