



# Introduction to Offensive Security Certified Professional **Bootcamp**

---

Host,

**VISHNU VIJAYAN VS** Founder, Nixie\_Bytes Security Team 🙌 Co-founder, Cyfosis Cyber Solutions

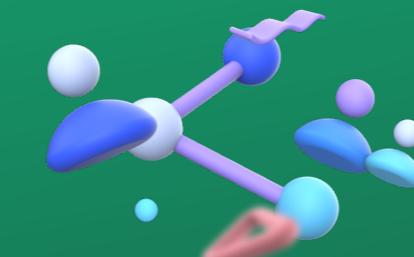




# Hi there!

---

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

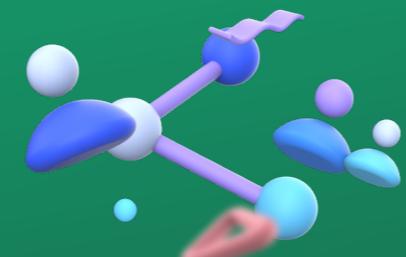




# Offensive Security Certified Professional

---

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 Kroptrix . Kroptrix 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

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

25 hours



# Introduction to Cyber Security

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

## Contents

- 01 | **Cyber security a walk-through**  
Intro to Cyber world & Cyber Security
- 02 | **Different careers in cyber security**  
How to build cyber security career & it's streams
- 03 | **Key terminology in cyber security**  
Importance of cyber security & how to differ from other fields
- 04 | **Elements of information security**  
Discussing about 5 Key elements and critical elements of an information Security



# Fundamentals of Cyber Security

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

## Contents

- 01 **Types of threat actors**  
Common Threats & defense Mechanism
- 02 **Passive attacks in cyber security**  
Discuss the passive attacking vector
- 03 **Active attacks in cyber security**  
Explore active attacking vector



# Setting up a lab

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

## Contents

- 01 **Download and install VMware**  
Download and Setup Virtual Machine in Windows
- 02 **Download and install BlackUbuntu & Ralph OS**  
Download and Setup Blackubantu and Ralph OS in VMWare
- 03 **Download and Setup Kiptrix1 in VM**  
Simply install and configure Kiptrix in VMWare



# Linux Basics (os)

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

## Contents

- 01 | **Difference between windows and linux**  
looking the main difference between Windows & Linux : User Experiences
- 02 | **Linux file system**  
Understanding & explore Linux File systems
- 03 | **Basic commands**  
Explore Linux 20 basic commands for working in Linux
- 04 | **Creating and viewing commands**  
Explore the file creating and viewing commands
- 05 | **Users and privileges**  
figure out and use the users privileges in linux OS
- 06 | **Apt & configuration**  
Simply configuring linux by apt



# 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

- 01 **Team Networking**  
Explore the trem networking
- 02 **Different types of network**  
Explore the types of networks around the world.
- 03 **Network topology**  
Disuss about main topologies in networking
- 04 **IP address**  
The term IP Address and it's working
- 05 **MAC address**  
The term MAC Address and it's working
- 06 **Subnetting**  
The term Subnetting and it's working



# 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

- 07 | **OSI model** — Walk into the OSI Model and Explain how it works
- 08 | **TCP & UDP** — Discuss main TCP & UDP Protocols and it's working
- 09 | **Network commands** — Explore more network Commads
- 10 | **Starting & stopping services** — Explore main commands for starting & stoping a service



# 5 Stages of Hacking

## Information Gathering

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

## Scanning & Enumeration

02 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 subdomain under main domain

### 03 Identify web technology

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



# 5 Stages of Hacking

## 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

## 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

### 01 | Scanning with Nmap

Scanning the host with nmap & collect all the info about the host.

### 02 | Nmap commands

Discuss about 15 Nmap commands

### 03 | Scanning with Brup

Setting up Burp and scan the host

### 04 | Scanning with Nikto

Scanning the host with nikto tool and find major Vulanarabilities

### 05 | Introduction to Metasploit

Starting with metasploit and scanning the host

### 06 | Enumeration SMB

Find the version and other details of SMB port

### 07 | Enumeration SSH

Find the version and other details of SSH port



# Exploitation Basics

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

## Contents

- 01 | **Re-potential vulnerabilities** 

---

find the easiest vulnerability using art of googling
- 02 | **Reverse shell vs bind shell** 

---

Discuss about main difference and use of bind shell & reverse shell
- 03 | **Understanding shells working** 

---

simple practical session for understanding the shells working principle
- 04 | **Staged vs non-staged payload** 

---

Discuss about main difference between staged & Non Staged payloads
- 05 | **Gaining root access with metasploit** 

---

In this session we got root access of Kroptrix using metasploit
- 06 | **Manual exploitation [openfuzz]** 

---

here we are using a simple C Script to exploit the kroptrix
- 06 | **Brute force tool - Hydra** 

---

finally we enter in the bruteforcing for getting root access using Hydra tool
- 06 | **Brute force tool - Metasploit** 

---

Here we are trying to gain root access using metasploit



# System Requirements

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

## Prerequisites

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



# Thank You!

---

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

