

**ETHICAL HACKING**

**AND**

**BUG BOUNTY**

## Why Ethical Hacking ?

According to INFOSEC Institute, the average salary for a Certified Ethical Hacker is \$71,331 per annum. If you learn Ethical Hacking, your chances of securing a career in Cyber Security will increase, an industry which will be recruiting 3.5 million unfilled cybersecurity jobs globally by 2022. On top of it, the demand for Cyber Security professionals is more than the supply.

## Career Options In Ethical Hacking

- Government/Private Firms
- Network Security Engineers
- Security Consultant.
- Information Security Analyst.
- Security Analyst.
- Penetration Tester.

## Introduction

- What Is Hacking Types of hacker
- Why hackers hack? Preventions from hacker
- Why Ethical Hacking?

## Getting Started

- Note Keeping
- Prerequisites
- Software & Tools Needed

## Basic & Fundamental

- Web Technology
- Web Development
- Web Hosting

## Networking Refresher

- IP Address
- MAC Addresses
- TCP, UDP and the Three-Way Handshake
- Common Ports & Protocols
- The OSI Model

## Steps Of Ethical Hacking

- Reconnaissance
- Scanning & Enumeration
- Gaining Access (Exploitation)
- Maintaining Access
- Covering Tracks

## Information Gathering And Scanning

- Why Information gathering?
- Whois lookup
- Reverse IP mapping
- Information Gathering Using Search Engine
- Google Hacking

## Email Hacks

- How Email Works?
- Email service protocols
- Email spoofing
- PHP Mail sending script
- Email Spamming
- Phishing
- Prevention from phishing
- Email Tracing
- Keystroke loggers
- Securing Your Email account

## Attacks On Web Servers And Security

- Introduction to Web Servers
- The Basic Process: How Web servers work
- Attacks on Web servers
- Web Ripping
- Protecting Your Files from Google

- Directory Traversal Attack
- SQL injection
- PHP Injection: Placing PHP backdoors
- How Attackers Hide Them While Attacking
- Types of Proxy Servers
- Hacking Wordpress, Drupal & Joomla

## Bug Bounty (\$\$ Earning From Hacking \$\$)

- How to earn from Hacking?
- What is Bug Bounty
- Bug Bounty Platforms
- How much can we earn from Bug Bounty.
- How to participate on Bug Bounty Programs

## Setting Up Our LAB

- Installing VMWare / VirtualBox
- Installing OS / Images
- Installing Kali Linux

## Introduction To Linux

- Exploring Kali Linux
- Sudo Overview
- Navigating The File System
- Users & Privileges
- Common Network Commands
- Network Commands Update
- Installing and Updating Tools
- Installing gedit
- Viewing, Creating and Editing Files
- Scripting with Bash

## Setting Up Tools For Hunting

- Introduction
- Installing Go
- Finding Subdomains with Assetfinder
- Finding Subdomains with Amass
- Finding Alive Domains with Httprobe
- Screenshotting websites with GoWitness
- Installing other necessary tools
- Automating the Enumeration Proces

## OWASP Top 10 Vulnerabilities Overview

- Injections
- Broken Authentication and Session management
- Cross Site Scripting
- Type of Cross Site Scripting
- Insecure Direct Object Reference
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Using Components with Known Vulnerabilities
- Invalidated Redirects and Forwards

## Testing The Top 10 Web Application Vulnerabilities

- Introduction
- The OWASP Top 10 and OWASP Testing Checklist
- Installing OWASP Juice Shop
- Installing Foxy Proxy
- Exploring Burp Suite

- Introducing the Score Board
- SQL Injection Attacks Overview
- SQL Injection Walkthrough
- SQL Injection Defenses
- Broken Authentication Overview and Defenses
- Testing for Broken Authentication
- Sensitive Data Exposure Overview and Defenses
- Testing for Sensitive Data Exposure
- XML External Entities Overview
- XXE Attack and Defense
- Broken Access Control Overview
- Broken Access Control Walkthrough
- Security Mis-configuration Attacks and Defenses
- Cross Site Scripting Overview
- Reflected XSS Walkthrough
- Stored XSS Walkthrough
- Preventing XSS
- Insecure De-serialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

## Legal Documents And Report Writing

- Common Legal Documents
- Pentest Report Writing
- Reviewing a Real Pentest Report

## Career Advice

- Finding Job
- Getting Opportunities
- Selecting A Job