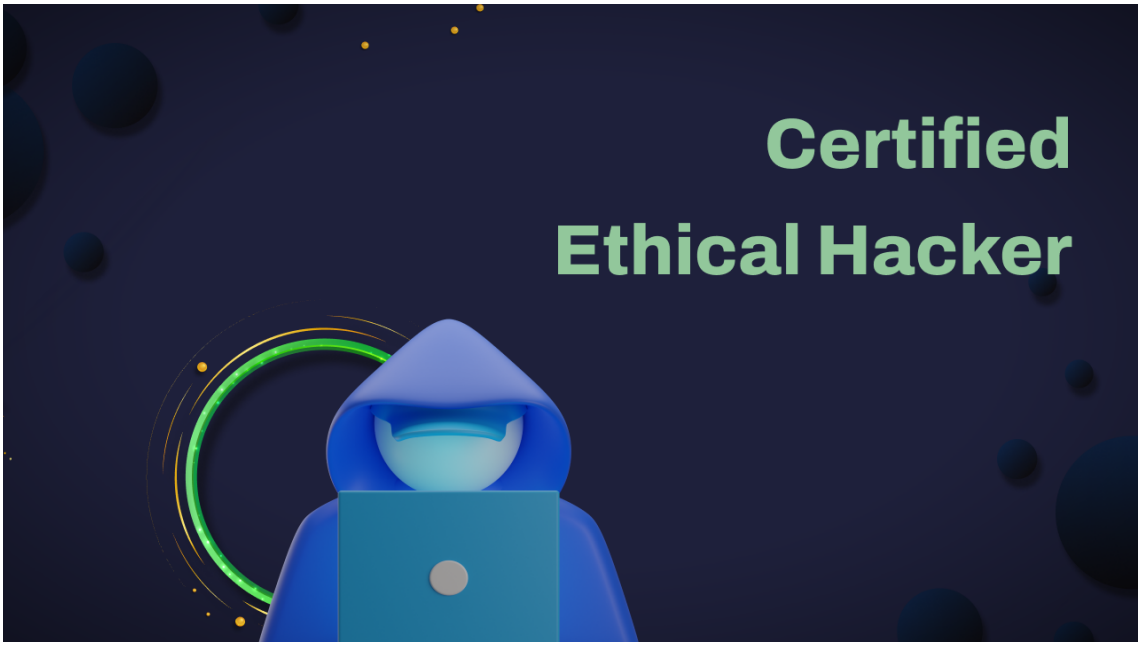
Welcome to ineuron.ai



Certified Ethical Hacker Bootcamp

Description:

Ethical hacking is a topic that has grown increasingly essential in today's world, and it can assist individuals and companies in adopting safe IT practices and usage. This ethical hacking course will teach you those skills as well as prepare you for associated certification examinations, allowing you to demonstrate your competence.

Start Date:

Doubt Clear Time:

Course Time:

Features:

Course material

Course resources

On demand recorded videos

Practical exercises

Quizzes

Assignments

Course completion certificate

What we learn:

Introduction to Ethical Hacking

Reconnaissance - Surveying the Attack Surface

Network Presence

Attacking

Web Hacking

Requirements:

System with Internet Connection

Interest to learn

Dedication

Instructor:

Name:

Joseph Delgadillo

Description:

The digital age is upon us. Would you like to build/protect the systems that shape our future? I am here on Teachable to produce valuable educational resources for students who wish to learn skills related to information technology, network security, programming languages and much more. Enroll in my course for a practical, down to earth approach to learning.

>Introduction to Ethical Hacking:

>>What is an ethical hacker

>>Terminology crash course pt1

>>Terminology crash course pt2

>>Terminology crash course pt3

>>CIA

>>Legal considerations

>Reconnaissance - Surveying the Attack Surface:

>>Surveying the attack surface

>>Recon types

>>Passive recon part 1

>>Passive recon part 2

>>Active recon

>>Recon walkthrough tools summary

>>Maltego demo

>>FOCA demo

>>Harvester demo

>>Reconng demo

>Scanning and Enumeration - Getting Down to Business:

>>Scanning enumeration

>>Identifying active hosts pt1

>>Identifying active hosts pt2

>>Identifying active services

>>OS and services fingerprinting

>>Network mapping

>>Final thoughts

>>Nmap syntax pt1

>>Nmap syntax pt2

>>Nmap hosts discovery

>>Nmap service discovery

>>Nmap scripts

>>masscan

>Network Presence:

>>Network insecurity

>>Sniffing and spoofing

>>Sniffing tools

>>Spoofing 2C crypto 2C and wifi

>>Tcpdump

>>Wireshark

>>Ettercap

>>SSL burp

>>Scapy

>Attacking:

>>Security overview windows architecture

>>Security overview credentials security

>>Security overview memory corruption and exploitation

>>Windows hacking basics

>>Local access and privilege escalation

>>Dumping hashes and cracking passwords

>>Linux attacking basics pt1

>>Linux attacking basics pt2

>>References

>>Windows msf exploit pt1

>>Windows msf exploit pt2

>>Post exploitation

>>Mimikatz

>>Mimikatz john the ripper

>>Hashcat

>>Konboot

>>Post cmd

>>Post powershell

>>Hydra ncrack pt1

>>Hydra ncrack pt2

>>Attacking Linux targets pt1

>>Attacking Linux targets pt2

>Web Hacking:

>>Introduction to web hacking

>>Web security architecture overview pt1

>>Web security architecture overview pt2

>>Attacking the web server pt1

>>Attacking the webserver pt2

>>Attacking the platform pt1

>>Attacking the platform pt2

>>Attacking the technology pt1

>>Attacking the technology pt2

>>OWASP top 10 pt1

>>OWASP top 10 pt2

>>Attacking the business logic pt1

>>Attacking the business logic pt2

>>Tools and methodology

>>References

>>OWASP

>>SQLI

>>SQL map intro

>>SQL map

>>Burpsuite

>>Burpsuite xsshunter

>>Mitmproxy

>>Skipfish pt1

>>Skipfish pt2

>Social Engineering - Hacking Humans:

>>Social engineering basics

>>Social engineering methods

>>Tools and techniques pt1

>>Tools and techniques pt2

>>Tools and techniques pt3

>>Physical security considerations

>>Final Thoughts

>>Intro demo

>>Toolkit prep

>>Credential harvesting

>>Website cloning

>>Automating an attack

>>Antivirus evasion pt1

>>Antivirus evasion pt2 UPDATED