
O N- AO
Presentations are communication tools
that can be used as demonstrations
CYBERHACKZ
ETHICAL HACKING COURSE

O N- AO

COURSES

01.

PRE HACKER

It is a beginner level course of 30 days.

02.

CYBERHACKZ CERTIFIED ETHICAL HACKER

It is advance level course including pre hacker.It will take 4 months.

03.

COMPUTER HACKING FORENSIC INVESTIGATION

it is advance level course . it will take 6 months..

04.

OSINT-CERTIFIED CYBER CRIME INVESTIGATION OFFICER

It is expert level course for police and investigation.

O N- AO

01

PRE HACKER

It is a beginner level course of 30 days.

O N- AO

Pre Hacker

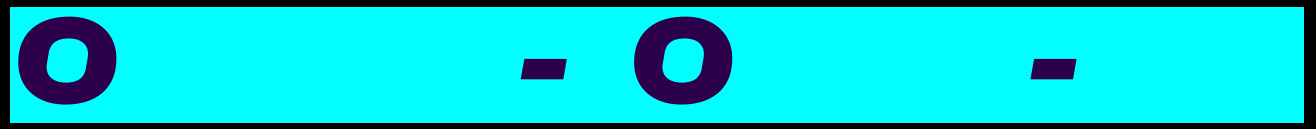
Description

Whether you're a beginner or looking to solidify your cybersecurity basics, this course is your gateway to understanding the world of ethical hacking. Join Cyberhackz and build the knowledge needed to navigate the realms of cybersecurity confidently.n this you will learn about basics of hacking. It is course of 30 days .

O - O -

MODULE 1

1: Who is a Hacker?
2: Who are Cyber Security Experts?
3: About Ethical Hackers & the Importance of Ethical Hacking
4: 12 Steps to Become an Ethical Hacker / Cyber Security Expert
5: What is Hacking & Who are Hackers?
6: Hacking Law & Punishment
7: Types of Hackers
8: What is Cyber Crime? & Types of Cyber Crime
9: Types of Operating Systems & Interfaces of OS
10: IP Address & MAC Address
11: How to View IP Address & MAC Address in a Computer Through CMD - Practical
12: How to Get System Information Through CMD - Practical
13: How to Check Communication Between Two Nodes Through CMD - Practical
14: What is WebRTC - Practical
15: What is Footprinting?
16: How to do Footprinting on a Victim
17: What is Phishing?
18: How to Create a Phishing Website for 30+ Social Media Platforms
19: What is Spoofing?
20: How to do MAC Spoofing
21: How to do Email Spoofing
22: How to do IP Spoofing



23: What is VPN?
24: What is the Darkweb?
25: How to Surf the Darkweb with Anonymity
26: What is Virtualization?
27: How to Create an ONN Hacking Lab Setup
28: What are Cookies?
29: How to Access Someone's Social Media Account Without User ID and Password
30: What is Android Hacking?
31: How to Create Your Own Spyware
32: How to Bind Spyware in an Image
33: What is Bypassing?
34: How to Bypass Windows Password
35: How to Bypass Kali Linux Password
36: Windows Run Command Every Hacker Must Know
37: What is Cyber Forensics?
38: Tools Used for Cyber Forensics
40: How to Extract Location from an Image
41: What is Cryptography?
42: How to Use Cryptography
43: What is Steganography?
44: How to Hide Text in an Image
45: How to Check if Your Password is Vulnerable

O N- AO

02

CYBERHACKZ CERTIFIED ETHICAL HACKER

O N- AO

Presentations are communication tools that can be used as demonstrations

CYBERHACKZ CERTIFIED ETHICAL HACKER

Description

It is a advance level course for being a certified hacker in 4 months.

Elevate your cybersecurity skills with Cyberhackz's Certified Ethical Hacking Course. Led by industry-certified experts, this program provides a comprehensive exploration of ethical hacking methodologies. Gain hands-on experience in penetration testing, vulnerability assessment, and threat mitigation. Equip yourself with the coveted Certified Ethical Hacker (CEH) certification, ensuring you're well-prepared to safeguard networks and emerge as a trusted ethical hacking professional. Enroll now to stay ahead in the dynamic world of cybersecurity.

- - A

O N- AO

O - O -

MODULE 1

1. What is Computer Networking?
2. How does Networking Work?
3. Types of Networks
4. What is IP Address?
5. IPv4 vs IPv6
6. Types of IP Address
7. Introduction to MAC Address?
8. Role of Ports in Networking
9. Introduction to Router and its elements
10. What is OSI Model and How does It Work?
11. What is TCP/IP Model and How does It Work?
12. OSI vs TCP/IP Model
13. What are Network Protocols?
14. Types of Protocols
15. How does TCP Work?
16. TCP vs UDP
17. What is Domain Name?
18. What is DNS?
19. DNS Records and Their Uses
20. What is Zone File?
21. What is HTML Request?
22. What is HTML Response?
23. Types of Request Methods
24. Capturing and Analyzing Network Packets (Wireshark)

MODULE 2

1. What is Ethical Hacking?
2. Types of Hackers
3. Types of Attacks on a System
4. Cybersecurity Laws
5. What is Linux?
6. Cool Features of Linux
7. Basic File System of Linux
8. Basic Linux Commands (Practical)
9. Advance Linux Commands (Practical)

O N- AO

O - O -

MODULE 3

1. Installing Kali Linux in Virtual Box
2. Configuring Kali Linux
3. Downloading a Good Wordlist
4. Installing Burp Suite Pro
5. Installing Acunetix Pro
6. And different tools with there Modules..

MODULE 4

1. What are Footprinting and Reconnaissance?
2. Types of Footprinting & Reconnaissance
3. Use of Footprinting & Reconnaissance
4. Footprinting Through Search Engines
5. Footprinting using Advanced Google Hacking Techniques
6. Footprinting Through Social Networking Sites
7. Website Footprinting (Netcraft, Wappalyzer)
8. Email Footprinting (Email tracker pro)
9. DNS Footprinting (DNSenum, DNS Lookup, MX Lookup, NS Lookup)
10. WHOIS Footprinting
11. Footprinting Through OSINT Framework

O N- AO

O - O -

MODULE 5

1. What is Network Scanning?
2. Network Scanning Methodology
3. Types of Network Scans
4. Checking for Live Systems and Buffer Size
5. Checking for Open Ports
6. Checking for Services On Ports
7. Checking for Software with versions
8. OS Fingerprinting & Banner Grabbing
9. Countermeasures
10. Saving xml report for Metasploit & Conversion

MODULE 6

1. What is Enumeration?
2. Types of Enumeration
3. Default Ports
4. How to Enumerate NetBIOS?
5. How to Enumerate SNMP?
6. How to Enumerate SMTP?
7. How to Enumerate NFS?
8. How to Enumerate DNS?
9. How to Enumerate all Services?
10. Countermeasures

O N- AO

O - O -

MODULE 7

1. Understanding layers of Internet (Deep, Dark, Surface & Hidden Web)
2. Changing User Agent (Random User Agent Switcher)
3. Changing MAC Address (Macchanger)
4. Auto Run Shell Script (MAC Changer)
5. Changing Wi-Fi MAC Address
6. Configuring Proxy (Mannual and tor proxy)
7. Configuring VPN (Free VPN)
8. Who is best for IP Anonymous?
9. Anonymous Configuration in Linux
10. Accessing Dark Web (Tor Browser)
11. Creating Dark Web Website (tor Server)

MODULE 8

1. What is Vulnerability Assessment?
2. Classification of Vulnerability
3. Vulnerability Assessment Lifecycle
4. Vulnerability Assessment Solutions
5. Vulnerability Scoring Systems
6. Scanning for Vulnerability in Nmap scans result (MSF, Exploit DB, Armitage)
7. Vulnerability Scanning - ZAP (OWASP)

O N- AO

O - O -

MODULE 9

1. What is System Hacking?
2. System Hacking Methodology
3. Cracking Windows Password (Pwdump, ophcrack, lophcrack)
4. Creating a Good Password list
5. Escalate Privileges in Linux
6. Escalate Privileges in Windows OS
7. System Hacking using URL(Camera, Location, Passwords and more)
8. URL Masking
9. System Hacking using Open Ports (nmap, NetCat, MSF, Armitage, Exploit DB)
10. What is Steganography?
11. Types of Steganography
12. Steganography Practical

MODULE 10

1. What is Malware?
2. Example of Malware
3. What is Trojan?
4. What are Viruses and Worms?
5. Types of Malware Analysis
6. Static Malware Analysis
7. Dynamic Malware Analysis
8. How to Create RAT Trojan? (HTTP, RAT)
9. Creating Payloads (MSF)
10. Creating Undetectable Payloads

O N- AO

O - O -

MODULE 11

1. What is Sniffing?
2. How an Attacker Hacks the Network Using Sniffers?
3. Active Scanning Techniques
4. Types of Sniffing
5. Protocols Vulnerable to Sniffing
6. MAC Spoofing
7. MAC Flooding
8. DHCP Flooding
9. Setup DHCP Rouge (MITM Attack)
10. MITM Attack
11. Sniffing with Wireshark

MODULE 12

1. What is Social Engineering?
2. Types of Social Engineering
3. Human-based Social Engineering
4. Computer-based Social Engineering
5. Mobile-based Social Engineering
6. Social Engineering Using SET

O N- AO

O - O -

MODULE 13

1. What is Social Engineering?
2. Types of Social Engineering
3. Human-based Social Engineering
4. Computer-based Social Engineering
5. Mobile-based Social Engineering
6. Social Engineering Using SET

MODULE 14

1. What is DoS Attack?
2. What is DDoS Attack?
3. Basic Categories of DoS/DDoS Attack Vectors
4. DoS in Networking (hping3, MSF, yersiniya)
5. DoS in Websites
6. DoS using Programs and Commands (CPU and Memory Utilisations)

O N- AO

O - O -

MODULE 15

1. What is DoS Attack?
2. What is DDoS Attack?
3. Basic Categories of DoS/DDoS Attack Vectors
4. DoS in Networking (hping3, MSF, yersiniya)
5. DoS in Websites
6. DoS using Programs and Commands (CPU and Memory Utilisations)

MODULE 16

1. What is Session Hijacking?
2. Why is Session Hijacking Successful?
3. Session Hijacking Process
4. Types of session Hijacking
5. Performing Session Hijacking(Burp Suite Professional, Ettercap)

O N- AO

03

COMPUTER HACKING FORENSIC INVESTIGATION

. Prepare to become a skilled cyber forensic analyst and contribute to the relentless pursuit of justice in the digital realm. Enroll now to master the art of cyber forensics with Cyberhackz.It is advance level course for cyber forensics of about 6 months.

O N- AO

O - O -

Module 01: Computer Forensics in Today's World
Module 02: Computer Forensics Investigation Process
Module 03: Understanding Hard Disks and File Systems
Module 04: Data Acquisition and Duplication
Module 05: Defeating Anti-Forensics Techniques
Module 06: Windows Forensics
Module 07: Linux and Mac Forensics
Module 08: Network Forensics
Module 09: Investigating Web Attacks
Module 10: Dark Web Forensics
Module 11: Database Forensics
Module 12: Cloud Forensics
Module 13: Investigating Email Crimes
Module 14: Malware Forensics
Module 15: Mobile Forensics
Module 16: IoT Forensics

O N- AO

04

OSINT-CERTIFIED CYBER CRIME INVESTIGATION OFFICER

Cyber investigator skilled in OSINT techniques, adept at tracing and analyzing digital footprints to uncover and mitigate hacking activities.

O N- AO

OSINT- CERTIFIED CRIME INVESTIGATION OFFICER

Short description

OSINT cyber hacking investigator adept at leveraging open-source intelligence for tracking and analyzing digital threats. Proficient in uncovering malicious activities, identifying threat actors, and providing critical insights to strengthen cybersecurity defenses.

O N- AO

O - O -

1. Course Intro and WhoAmI.
2. What is OSINT and How to Help Investigate Any Cyber Crime.
3. What Is a Sock Puppet In (OSINT).
4. Sock Puppet Practical (OSINT).
5. OSINT Practical & What Resources Are Used In Cyber Crime Investigation.
6. (Theory) Website Whois, DNS Subdomain Enumeration, etc.
7. How To Investigate Any Domain Or Website & Other Related Things (OSINT).
8. How Google Dorks Help In Cyber Crime Investigation Or OSINT Investigation.
9. Find Someone's Social Media & Online Account Using Username, PersonName & Generate Report (OSINT).
10. How To Find All Information About Any People In A Single Click. Investigate Any Cyber Crime Also.
11. How To Find Anyone Or Social Media Profile, Email, Domain OR Online Presence Using Username.
12. How To Find Anyone Social Media Account & Other Information Using Images Or Pictures OSINT.
13. How To Find Someone's Real User ID And Username Of Any Facebook Account.
14. How To Get Any Facebook Profile, Page, Group, Account Facebook ID Fb-Id (FACEBOOK OSINT).
15. How To Investigate Anyone Person And Collect All Information e.g., Social media Device Info Metadata.

O N- AO

O - O -

16. How To Know About Any Email Where Registered, Identifying & Active Account-Existing.
17. How To Know And Discover Hostnames Of Any Target IP Addresses.
18. How To Know Someone's Instagram Account Private Connected Email Or Phone Number (OSINT).
19. How To Know Who Visited & Seen. My, Or Stalk My Facebook Profile (FACEBOOK – OSINT).
20. Browser Extension Helps In OSINT And Cyber Crime Investigations.
21. DarkWeb Investigation (OSINT).
22. Email Information Gathering - Get details, Phone number, Email Harvesting.
23. Email2Phonenumber that allows you to obtain a target's phone number just by having his email address.
24. Finding a location From Any Image And Get Exact Geolocation GEO-OSINT.
25. Gmail Or Google Account Investigation To Trace Location & Activities Or Know Active Google services (OSINT).
26. How Censys Helps in OSINT And Cyber Crime Investigations.
27. How Intelligence Framework Helps In OSINT And Cyber Crime Investigation.
28. How Shodan Helps In OSINT Or Cyber Crime Investigations.
29. How Spiderfoot Framework Is Used For Cyber Crime Investigation Or Threat Intelligence OSINT.
30. How To Decrypt Hash and Encrypt Any Word Into Hash Easily (OSINT).

O N- AO

O - O -

31. How To Detect Phishing Domain And Link, URL Or Investigate Phishing Domain, URL Threat Intelligence.
32. How To Extract Text Into Any Image In OSINT Investigations.
33. How To Get Location Or Device Model Information in Any Image Photo Using Metadata Extraction.
34. How To Track Exact GPS Location Of Anyone (OSINT).
35. How To Use Maltego Tools And How They Help In OSINT And Cyber Crime Investigations.
36. Instagram Account Investigation (OSINT) & Also See Or Investigate Private profile Photo, Story.
37. Mobile Phone Cell Tower Tracking In Any Area Without GPS Location Or Device (OSINT).
38. OSINT-FrameWork Helps In OSINT And Cyber Crime Investigation To Find Information On Anything.
39. Proton-Mail Email Or Proton-Vpn Investigation (OSINT).
40. Recover Deleted WebPages, Websites, And Old Websites, And PostWebsite Time Machine.
41. Snapchat (OSINT) Surveillance Or Track Snapchat Users.
42. Track Any WiFi And Mac Address BSSID & SSID GPS Location (OSINT).
43. Track Tor IP Investigation Or Tor Exit Node Checker (OSINT).
44. VoIP Or Internet Calling Number Investigation OSINT Find Real Owner Details And Many More Details.
45. Remotely Click Camera Pic Without Touch Android , Computer.


THANKS