SecureHack
Making Internet Safe

Year Diploma in Ethical Hacking and Cybersecurity

Introduction:

Starting from the basics, this cybersecurity course provides a solid foundation for students from any stream at any level entering the field. No prior knowledge or experience is required, making it accessible to beginners who are eager to learn. The course begins by emphasizing the significance of cybersecurity in today's interconnected world. The course has been designed with a practical approach so that students will gain a clear understanding of the threats and attack vectors that jeopardize our digital systems and personal information. These topics cover the foundational aspects of cybersecurity and provide a solid understanding of key concepts, technologies, and practices. This Ethical Hacking Course is provided by the professionals of EHI. It is framed by the expert professionals of EHI who have hands-on experience in Cyber Security.

Course outcome: The course outcomes of these topics aim to equip students with the knowledge and skills necessary to understand, mitigate, and respond to cybersecurity threats effectively. Upon completing the training program, students should be able to implement security measures, assess risks, protect data, and contribute to a secure computing environment.

- Full-fledged course designed by EHI covering all domains of hacking.
- Framed ina manner such that it covers all aspects of Ethical Hacking.
- Complete Ethical Hacking toolkit will be provided.
- Along with the toolkit complete study material and guidance will be provided.
- Live Hacking demonstrations will be provided.
- Complete Industry exposure with hands-on experience on penetration testing projects.
- Tests will be scheduled at regular intervals.

Mode: Online/Offline

Duration: 1 Year

SecureHack
Making Internet Safe

System Requirements:

Operating System:
Windows 10, macOS, or Linux (based on the training program and tools being used)
Processor:
Intel Core i5 or equivalent (or higher)
RAM:
Minimum of 8 GB RAM (16 GB or higher recommended for better performance)
Storage:
At least 256 GB of available storage space
Network Connectivity:
Ethernet or Wi-Fi capability for internet access and networking tasks
Virtualization:
If virtualization software like VMware or VirtualBox is used, the system should support hardware virtualization technology (e.g., Intel VT-x or AMD-V)

Tools :

1. **Virtualization Software:**
   VMware Workstation
   VirtualBox
2. **Network Security Tools:**
   Wireshark
   Nmap
   tcpdump
3. **Penetration Testing Tools:**
   Metasploit Framework
   Kali Linux (including its various tools)
4. **Intrusion Detection and Prevention Systems (IDS/IPS)**
   Snort
5. **Forensics and Incident Response Tools:**
   EnCase
   Autopsy

Course Content:

1. **Basics**
   - Introduction to Cyber Security
   - Introduction to Cryptography and Hashes
   - Ethical Hacking Introduction

- Introduction
- Introduction to all Underground Ethical Hacking Community

2. Basics of Linux

- Linux architecture
- Linux File directory architecture
- Installation of Linux
- Basic commands of Linux and their usage
- Description of files like password shadow sudoers etc
- Virtual Machine Installation
- Installation of Linux
- Introduction to Kali Linux and its Tools
- Introduction to Backtrack/Kali Operating System
- Penetration Testing using Backtrack/Kali
- The Bash Environment
- Simple Bash Scripting
- Finding your way around Backtrack
- Backtrack Services

3. Basic networks

- Important Protocols and their headers In Depth)
- TCP
- UDP
- IP
- ICMP
- Ports and their basic
- Basics of Linux Services
- IPV6 &IPV4

4. Basics of Networking

- Information Gathering and Footprinting
- Network Vulnerability Assessment
- WiFi Hacking and Security 2 Hours
- Router Penetration Testing 2 Hours
- Metasploit Framework
- Network Exploitation Frameworks

- Brute Force attack
- Secure Socket Layer SSL) Torn Apart
- Determining whether yourconnection is secure or not
- SSL: How it works
- Cryptography Firewalls and Error Messages
- Penetration Testing
- Introduction to Penetration Testing
- How to do Penetration Testing
- Preparing the Report
- Wi-Fi Ethical Hacking &Security
- Ethical Hacking on Wi-Fi Passwords on Wi-Fi router with WEP|WPA|WPA2 encryption
- Securing Wi-Fi Routerfrom being hacked
- Sniffing the Network to E-Hack passwords
- DHCP
- Static IP Assignment
- SSHD
- Apache
- FTP
- TFTPD
- VNC Server
- Net cat the Almighty
- Connecting to a TCP/UDP port with Net cat
- Listening on a TCP/UDP port with Net cat

- Transferring files with Net cat
- Remote Administration with Net cat
- Using Wire shark
- Peeking at a Sniffer
- Capture and Display filters
- Following TCP Streams
- Information Gathering Techniques
- Open Services Information Gathering
- DNS Reconnaissance
- Interacting witha DNS server
- Automating lookups
- Forward lookup brute force
- Reverse lookup brute force
- DNS Zone Transfers
- SNMP reconnaissance
- Enumerating Windows Users
- Enumerating Running Services
- Enumerating open TCP ports
- Enumerating installed software
- SMTP reconnaissance
- Microsoft NetBIOS Information Gathering
- Null sessions
- Scanning for the NetBIOS Service
- Enumerating Usernames/ Password policies
- Port Scanning
- TCP Port Scanning Basics

- UDP Port Scanning Basics
- Port Scanning Pitfalls
- Nmap4
- Important Protocols and their headers In Depth)
- Network Traffic Analysis
- Network Threats and Attack Methodology
- Reconnaissance Basic and Advance)
- Information gathering tools
- Hashing Cryptographic functions)
- Port scanning via NMAP
- Pentesting Methodology
- Metasploit Framework
- Manual Port Scanning
- Scapy MODIFY IP PACKET HEADER PARAMETERS be fool the server)
- Hping Automatic packet generation tool)
- Server pentesting
- Hacking networks
- VAPT
- Secure network design
- IDS &IPS
- Rules of IDS &IPS
- RFI& LFI
- Denial of service (DOS) and distributed Denial of service (DDOS) attacks over thenetwork
- Countermeasures of DoS and DDoS
- Practical Aspects of Networking
- Knowing the Basics of IP Address
- Knowing Remote System IP Address
- Hiding Your IP address Proxy Server)
- Be Anonymous in Cyber World VPN and Proxy Servers
- VPN Virtual Private Network)
- Tracing an IP Address
- Attack Scanning &Virtual Lab Preparation
- Network Reconnaissance
- Port Scanning Daemon Banner Grabbing
- OS Detection & Firewall Enumeration

- Sniffing
- Making Virtual Lab using VMware or Oracle Virtual Box
- Active and Passive Information Gathering
- Configuring and Testing Your Network
- Live Firewall Implementation

- Network Sweeping
- OS fingerprinting

- Banner Grabbing / Service Enumeration
- Nmap Scripting Engine
- ARP Spoofing
- Ettercap
- Working With Exploits
- Looking foranexploit on Backtrack
- Looking forexploits onthe web
- Transferring Files
- The non interactive shell
- Uploading Files
- Using TFTP
- Using FTP
- Inline Transfers
- Exploit frameworks
- Meta Spoilt
- Interesting Payloads
- Meterpreter Payload

- Binary Payloads
- FTP Brute force
- POP3 Brute force
- SNMP Brute force

5. Web Application security

- Basics of Web Security
- HTTP Methods
- HTTP status codes
- Burp Suite tool
- Sql injection
- Xss Attack
- Defence mechanism of Sql Injection and xss attack
- Security misconfiguration
- Session hijacking
- Malicious file inclusion
- Broken authentication and session hijacking
- Insecure direct object reference
- Information leakage and improper error handling
- Failure to restrict URL access
- Cross site request forgery attack and countermeasures
- Remote code executionvulnerability study
- RFI& LFI remote file inclusion &local file inclusion) vulnerability
- Denial of service DOS) and distributed denial of service DDOS) attacks
- Countermeasures of DoS and DDoS

SecureHack
Making Internet Safe

- Web platform security issues and countermeasures
- Website code review and secure coding principles
- Projects based onlive websites
- Basics of Web technology
- Web Architecture and PHP

- Demonstration of leaking of confidential information on vulnerable website
- Securing a website from Google Ethical Hacking
- Website Ethical Hacking Attacks &Security Important Module)
- CMS Ethical Hacking Introduction
- 0+ Website Ethical Hacking Techniques First Time Ever In World) &Countermeasures
- SQL Injection Basic &Advance)
- Website Security
- Input Validation Attack
- Session Hijacking
- Protocols Vulnerabilities and Exploiting through Sniffers
- Server routing and Countermeasures Website Ethical Hacking)
- Website Ethical Hacking &Security
- Open Web Information Gathering
- Google Hacking
- Miscellaneous Web Resources
- Other search engines
- SSLEncapsulation – Stunnel
- HTTP CONNECT Tunneling
- Proxy TunnelSSHTunneling

- SQL Injection in ASP / MSSQL
- Identifying SQL Injection Vulnerabilities
- Enumerating Table Names
- Enumerating the columntypes
- Fiddling withthe Database
- Microsoft SQLStored Procedures
- Code execution

6. OS and Database security

- LINUX And Windows Based server hardening
- Controls and authorization Configuration Privileges to Users)
- Database Access Configuration
- Database/Platform Interaction Configuration
- Secure Communication configuration
- Secure Services Configuration
- Logs and Event Management
- Security Auditing

7. Database security

- Hijacking os withusing RAT and trojan
- Operating System Hacking and Security\
- CMS Exploitationand Database Pentesting
- System Hardening |Windows |Linux |Mac

8. FORENSICS

- Chain of custody &6 A's of forensics
- Legal study of evidence acquisition
- Disk based forensics
- Network Forensics
- Data packet analysis
- Browser forensics
- USB forensics
- Memory analysis
- windows forensics
- Tools based onforensic study
- Deleted data recovery
- Image Forensics
- Case investigation
- Evidence recovery
- Protocol standards
- Firewalls
- WLAN Security
- Dead vs Live forensics
- Computer Investigation process
- Investigating attacks
- Cyber Forensics and Investigations
- Digital Forensics Science

- Recoverdata from the USB Pendrives Hard Disk Drive – Police Forensic way

9. COMPLIANCE

- Basic principles of assessment &auditing
- Types of Auditing
- IT LAWS and ACTS
- ISO 2 00 :200 :20 3 basics
- PCI DSS
- Risk Assessment
- BCM
- Network Security Auditing
- Physical Security and Complaince

10. Miscellaneous

- Email Attacks and Security
- Smartphone Attacks and Security
- Google Hacking Database
- Introduction to Buffer Overflows
- Buffer Overflows
- Wireless Sniffing
- Email Ethical Hacking
- What is Email Ethical Hacking
- Tracing Email

- Other Input Validation Attack
- Important Theft Techniques
- Spamming Attacks
- USB Ethical Hacking Technique
- Implementing security against Important Theft Techniques
- Social Engineering Attack
- Ethical Hacking Anyone without evenusing a single tool
- Physical Security Threats
- Steganography Hide data into images)
- Banking Ethical Hacking &Security
- Concept of how ATM Hacking happens &Security
- How Credit Card &Debit Card Hack Attacks &Security
- Advance Ethical Hacking Technique
- Ethical Hacking **I** S Server
- Advance Email Ethical Hacking Techniques
- Shell Ethical Hacking Website Ethical Hacking)
- Live Ethical Hacking Demonstration on Dedicated Server in US orat other Country
- Credit Card Ethical Hacking &Security
- Malt Ego
- Network Infrastructure
- Social Infrastructure
- PBNJ
- Unicorn Scan
- Buffer Overflow Exploitation
- Looking for Bugs
- Fuzzing

- Exploiting Windows Buffer Overflows
- Replicating the Crash
- Controlling EIP
- Locating Space forour Shell code
- Redirecting the executionflow
- Finding a return address
- Basic shell code creation
- Getting ourshell
- Exploiting Linux Buffer Overflows
- Setting things up
- Controlling EIP
- Landing the Shell
- Avoiding ASLR
- Other Framework v3 x features
- Core Impact
- Client Side Attacks
- Client side attacks
- CVE-2009-092
- MS0 -0 – From POC to Shell
- MS06-00
- Client side exploits inaction
- Port Fun
- Port Redirection

- J ohn the Ripper
- Rainbow Tables
- Password Attacks

11. Certified Malware Analysis

- Malware Fundamentals : Reverse engineering
- Malicious Code &Pattern analysis
- Complete Malware analysis
- Static Malware Analysis
- Dynamic malware Analysis
- In-depth study of Self-Defending Malware
- Maneuvering Techniques
- Persistence Techniques
- Self destruction
- Self Avoidance
- Security degradation
- Malicious Documents
- Memory Forensics
- Registry Settings
- System Settings
- Malware Illustration
- Basics of Reverse Engineering
- Reverse Engineering Part - Windows Memory Management

- Reverse Engineering Part 3
- Demonstration of E-Hacker Virus
- Keylogger Spyware Software
- Trojan and Backdoors Attack
- Virus Worm &Trojan
- Binders and Cryptors
- Root kits
- Aphex Root kit
- HXDEF Root kit
- Registry Backdoors
- Trojan Horses
- Binary Trojan Horses