# iSecur1ty Ethical Hacking Basics Course V2.0 syllabus

IS|EHB v2.0

# Course overview

- Intro to the course & Labs Configuration.
- penetration testing methodologies.
- Information Gathering.
- Port Scanning techniques.
- Vulnerability Analysis.
- Exploitation.
- Buffer Overflow(Win32 + Linux).
- Post Exploitation.

# Module 1
# Intro to the course & Labs Configuration.

- Introduction to the course.
- Labs Configuration.
- Materials and forums support.

# Module 2
# penetration testing methodologies.

- Introduction to Penetration Testing.
- Penetration Testing Vs Vulnerability Analysis.
- PTES Methodology.
- OWASP Methodology for web pentesting.

# Module 2
# penetration testing methodologies.

- Penetration Testing types.

  Penetration Testing categories.

# Module 3
# Information Gathering

- Introduction to Information Gathering.
- Passive Information Gathering.
  * Whois.
  * Google.
  * Google Hacking Database.
  * Social Media
  * The Harvester.
  * NetCraft

# Module 3
# Information Gathering

- Active Information Gathering.
  * host.
  * ping.
  * netcat.
  * dig.
  * manual enumeration.
  * special techniques.

# Module 3
# Information Gathering

- Port Scanning techniques.
  * How TCP works ?.
  * ping sweep techniques.
  * Banner Grabbing.
  * Introduction to Nmap.
  * Nmap Syn Scan.
  * Nmap TCP Scan.

# Module 3
# Information Gathering

- Port Scanning techniques.
  * UDP Scan.
  * Xmas / Fin / Null Scans.
  * Nmap Script Engine.
  * Netcat - The Swiss Army Knife.

# Module 4
# Vulnerability Analysis

- Introduction to Vulnerability Analysis.

- Vulnerability Analysis Tools.
  * Nessus.
  * OpenVas.

- Install , active and use Nessus.

# Module 5
# Exploitation

- Definition of Exploitation.
- Put all data together.
- Introduction to Metasploit.
- Remote system exploitation (Linux / Windows clients).

# Module 5
# Exploitation

- Password Attacks.

  * Services Brute force attacks.
  * Password Cracking.
  * John - john the ripper.

# Module 5
# Exploitation

- Client Side Attacks - CSA.
  * File Format Attacks.
    * mp3 file format attack case study.
    * PDF file format attack case study.
  * Browser Attacks.
    * Metasploit Browser autopwn.
    * IE multiple attack scenario.

# Module 5
# Exploitation

- Social Engineering Attacks.
  * SET - Social Engineering Toolkit.
  * Phishing Attacks.
  * Using SET with web application attacks.

- Bypassing Antivirus.

# Module 5
# Exploitation

- Web Application Attacks.
  * Introduction to Web Application Attacks.
  * Reviewing OWASP Methodology.
  * Introduction to HTTP protocol.
  * Web Spidering.
  * Introduction to Burp Suite.

# Module 5
# Exploitation

- cross site scripting Attacks (XSS).
  * Reflected XSS.
  * Stored XSS.
  * Blind XSS.
- Unrestricted File Upload Attacks.
- Remote Command Exection Attacks (RCE).

# Module 5
# Exploitation

- SQL injection Attacks (SQLi).
  * Types of SQLi.
  * Exploiting SQLi Manually.
  * Using SQLmap.
  * From SQLi to RCE.
  * Read Files using SQLi.
- Review the Labs.

# Module 6
# Buffer Overflow vulnerabilities

- Introduction to Buffer Overflow Attacks.
- Introduction to python.
- Introduction to Fuzzing.
- Fuzzing techniques.
  * Remote Fuzzing.
  * Local Fuzzing.
- Introduction to DEP / ASLR.

# Module 6
# Buffer Overflow vulnerabilities

- Win32 Buffer overflow.
  * Generate the Crash.
  * Controlling EIP techniques.
  * Playing around the Return Address.
  * Checking for  Bad Characters.
  * Generate The Shellcode Using Metasploit.
  * Solve the puzzle :D

# Module 6
# Buffer Overflow vulnerabilities

- Linux Buffer overflow.
  * Lab Configuration.
  * Introduction to GDB.
  * Generate the Crash.
  * Controlling the EIP.
  * Generate the Shellcode.
- Return to Libc technique.

# Module 7
# Post Exploitation

- Introduction to Post Exploitation.
- Privilege Escalation Attacks.
- The art of Persistent Using Metasploit.
- Meterpreter modules.