What you'll learn

- Start from 0 up to a high-intermediate level.
- Learn ethical hacking, its fields & the different types of hackers.
- Install a hacking lab & needed software (on Windows, OS X and Linux).
- Hack & secure both WiFi & wired networks.
- Understand how websites work, how to discover & exploit web application vulnerabilities to hack websites.
- Use 30+ hacking tools such as Metasploit, Aircrack-ng, SQLmap.....etc.
- Discover vulnerabilities & exploit them to hack into servers.
- Hack secure systems using client-side & social engineering.
- Secure systems from all the attacks shown.
- Install & use Kali Linux - a penetration testing operating system.
- Learn linux basics.
- Learn linux commands & how to interact with the terminal.
- Learn Network Hacking / Penetration Testing.
- Network basics & how devices interact inside a network.
- Run attacks on networks without knowing its key.
- Control Wi-Fi connections without knowing the password.
- Create a fake Wi-Fi network with internet connection & spy on clients.
- Gather detailed information about networks & connected clients like their OS, ports ...etc.
- Crack WEP/WPA/WPA2 encryptions using a number of methods.
- ARP Spoofing / ARP Poisoning.
- Launch various Man In The Middle attacks.
- Access any account accessed by any client on the network.
- Sniff network traffic & analyse it to extract important info such as: passwords, cookies, urls, videos, images ..etc.
- Intercept network traffic & modify it on the fly.
- Discover devices connected to the same network.
- Inject Javascript in pages loaded by clients connected to the same network.
- Redirect DNS requests to any destination (DNS spoofing).
- Secure networks from the discussed attacks.
- Edit router settings for maximum security.
- Discover suspicious activities in networks.
- Encrypt traffic to prevent MITM attacks.
- Discover open ports, installed services and vulnerabilities on computer systems.
- Hack servers using server side attacks.
- Exploit buffer over flows & code execution vulnerabilities to gain control over systems.
- Hack systems using client side attacks.

- Hack systems using fake updates.
- Hack systems by backdooring downloads on the fly.
- Create undetectable backdoors.
- Backdoor normal programs.
- Backdoor any file type such as pictures, pdf's ...etc.
- Gather information about people, such as emails, social media accounts, emails and friends.
- Hack secure systems using social engineering.
- Send emails from ANY email account without knowing the password for that account.
- Analyse malware.
- Manually detect undetectable malware.
- Read, write download, upload and execute files on compromised systems.
- Capture keystrokes on a compromised system.
- Use a compromised computer as a pivot to hack other systems.
- Understand how websites & web applications work.
- Understand how browsers communicate with websites.
- Gather sensitive information about websites.
- Discover servers, technologies & services used on target website.
- Discover emails & sensitive data associated with a specific website.
- Discover subdomains associated with a website.
- Discover unpublished directories & files associated with a target website.
- Discover websites hosted on the same server as the target website.
- Exploit file upload vulnerabilities to gain control over target website.
- Discover, exploit and fix code execution vulnerabilities.
- Discover, exploit & fix local file inclusion vulnerabilities.
- Discover, exploit & fix SQL injection vulnerabilities.
- Bypass login forms and login as admin using SQL injections.
- Exploit SQL injections to find databases, tables & sensitive data such as usernames, passwords...etc
- Read / Write files to the server using SQL injections.
- Learn the right way to write SQL queries to prevent SQL injections.
- Discover reflected XSS vulnerabilities.
- Discover Stored XSS vulnerabilities.
- Hook victims to BeEF using XSS vulnerabilities.
- Fix XSS vulnerabilities & protect yourself from them as a user.