What I will Cover

1.Ethical HACKING 101
2.Installing kali Linux
3.Understanding Cyber Kill Chain
4.Intro to Reconnaissance
5.Google Dorking
6.WHOIS & DNS Recon
7.Social Media Recon
8.Identifying website tech
9.Subdomain Enumeration
10.Identify target WAF
11.Scanning with Nmap
12.Directory Brute Forcing
13.Vulnerability Scanning
14.Finding Exploits
15.Reverse Shells VS Bind Shells
16.Metasploit Basics
17.Exploitation with Metasploit
18.Brute Force Attacks
19.SQL Injection Attacks
20.XSS Attacks
21.Dumping hashes with Mimikatz
22.Passwords Cracking
23.Clearing Tracks
24.Become Anonymous while Hacking
25.Port forwarding 101
26.Social Engineering 101
27.Hacking Instagram
28.DDOS Attacks
29. OS login Phishing
30.Try Hackme vulnerability

Ethical Hacking 101

What Is Ethical Hacking?

Ethical hacking is the practice of legally and intentionally breaking into computer systems, networks, or applications to identify and fix vulnerabilities before malicious hackers can exploit them.

Ethical hackers and “White hat” hackers are professionals who use their skills for good.They make sure that an organization's security should be in place.

Different Types of hackers:

.White Hat Hacker
.Black hat hacker - malicious hackers (their intention is for monitoring illegally)
.grey hat hacker - (Their action may be illegally but their intention is good)
.script kiddies - (They are using other’s making tool for hacking but they have no proper knowledge about this)
.Hacktivists - (They are hacking illegally but their intention not bad as a example a hacker drop/down others illegal website)
.State-sponsored Hackers - (they are hacking for govt/nation .They are most skillful hackers.)

Testing approach in ethical hacking

.White box testing
.black box testing
.Grey box testing

White Box VS Blak Box VS Grey Box:

Testing Types	Knowledge Level	Focus Area	Common Use Cases
White Box Testing	Full Knowledge of code	Internal structure and knowledge	Unit and integration testing
Black Box Testing	No knowledge of code	Functionality and user experience	Systems and acceptance testing
Grey Box Testing	Partial knowledge	Both internal and external aspects	Integration and system testing

Red Team VS Blue Team VS Purple Team

Team Type	Focus Type	Key Activities	Goal
Red team	Offensive Security	Simulating attacks,penetration testing	Identify vulnerabilities
Blue Team	Defensive Security	Monitoring systems, incident response	Protect against attacks
Purple Team	Collaboration between red and blue	Joint exercises,knowledge sharing	Strengthen overall security posture