CEH v.13 (Certified Ethical Hacker)

- **Introduction to Ethical Hacking**
- **Foot printing and Reconnaissance**
- **Scanning Network**
- **Enumeration**
- **Vulnerability Analysis**
- **System Hacking**
- **Malware threats**
- **Sniffing**
- **Social Engineering**
- **Denial-of-Service**
- **Session Hijacking**
- **Evading IDS, Firewalls and Honeypots**
- **Hacking Web Servers**
- **Hacking Web Applications**
- **SQL Injections**
- **Hacking Wireless Networks**
- **Hacking Mobile Platforms**
- **IoT and OT Hacking**
- **Cloud Computing**
- **Cryptography**

PWK (Penetration Testing with Kali)

- **Penetration Testing: What You Should Know**
- **Getting Comfortable with Kali Linux**
- **The Essential Tools**
- **Passive Information Gathering**
- **Active Information Gathering**
- **Vulnerability Scanning**
- **Buffer Overflows**
- **Working with Exploits**
- **File Transfers**
- **Privilege Escalation**
- **Client-Side Attacks**
- **Web Application Attacks**
- **Password Attacks**
- **Port Redirection and Tunneling**
- **The Metasploit Framework**

Sec 580 (Metasploit Kungfu for Enterprise Pen Testing)

- **Metasploit Introduction**
- **Metasploit Console Commands**
- **Metasploit Exploitation**
- **Meterpreter, Script, Post Modules**
- **Metasploit Reconnaissance, Scanning**
- **Client-Side Exploitation**
- **Metasploit Malwares**
- **Metasploit Integrations**
- **SET Toolkit**

Sec 560 (Network Penetration Testing and Ethical Hacking)

- **Pen Test Planning**
- **Recon**
- **Scanning**
- **Exploitation**
- **Post- Exploitation**
- **Password Attacks and Merciless Pivoting**
- **Web App Attacks**

Sec 542 (Web Application Penetration Testing and Ethical Hacking)

Introduction and Information Gathering

01-Why the Web

02-Understanding the Web

03-Web App. Pen Tester's Toolkit

04-Interception Proxies

05-WHOIS and DNS

06-Open Source Information

07-The HTTP Protocol

08-HTTP Methods

09-HTTP Status Codes

010-WebSocket

011-HTTPS

Configuration, Identity, and Authentication Testing

01-Nmap

02-Testing Software Configuration

03-Spidering Web Applications

04-Analyzing Spidering Results

05-Fuzzing

06-Authentication

07-Username Harvesting

Injection

01-Session Tracking

02-Session Fixation

03-Bypass Flaws

04-Vulnerable Web Apps

05-Command Injection

06-File Inclusion-Directory Traversal

07-SQL Injection Primer

08-Discovering SQLi

09-Exploiting SQLi

010-SQL Tools

XXE and XSS

01-Cross Site Scripting

02-XSS Fuzzing

03-XSS Exploitation

04-BeEF

05-XXE

CSRF, Logic Flaws

01-Cross Site Request Forgery

02-Logic Attacks

03-WPScan and Other Tools

04-Pen Testing Methods

05-Reporting