Cybersecurity Course – Become a Pro…

- **Structured 12-Week Program** – Theory (60%) + Labs (40%)
- **Start from Scratch** – Cybersecurity Basics, Compliance, and GRC
- **Understand Attacks Deeply** – Cyber Kill Chain & MITRE ATT&CK Framework
- **Master Cybersecuriy Tools** – Splunk, Wireshark, Nmap, Burp Suite, Metasploit, SEToolkit & more
- **Exercise**– Real-world scenarios using Kali Linux
- **Target All Environments** – Servers, Web Apps, Mobile, Wi-Fi & IoT
- **Attack & Defend** – Recon to Exploitation, Privilege Escalation & Hardening
- **Risk & Incident Response** – Learn detection, containment & recovery
- **Final CTF Project** – Simulated attack-defence with documentation
- **Career Focused** – Interview prep, resume tips, and certification roadmap (CEH, OSCP, CISSP)

Cybersecurity Course Overview

Theory

- **Cybersecurity Fundamentals**
  - Threat landscape, security domains, compliance basics
- **CIA Triad & Cyber Kill Chain**
  - MITRE ATT&CK, TTPs, attacker lifecycle
- **Security Controls & Defense in Depth**
  - Firewalls, EDR, layered security
- **Passive Reconnaissance & Footprinting**
  - OSINT, Google Dorks, Shodan, DNS recon
- **Subdomain Enumeration**
  - Tools like Sublist3r, Amass, crt.sh
- **Wireless Security**
  - WPA2/3, Evil Twin, KRACK (concepts only)
- **Risk Management & BIA**
  - Threat modeling, risk treatment, impact analysis
- **Threats & Vulnerabilities**
  - XSS, SQLi, malware types, insider threats
- **Social Engineering**
  - Phishing, USB drops, SEToolkit tactics
- **Cryptography Basics**
  - Encryption, hashing, TLS/SSL
- **Incident Response & Blue Teaming**
  - IR lifecycle, SIEM intro, response strategies
- **Penetration Testing**
  - Scanning, exploitation, post-exploitation
- **Security Frameworks**
  - NIST, ISO 27001, CIS, GDPR
- **Career Prep**
  - CTF, certifications (CEH, OSCP), interview prep

Excercise

- Nmap scanning and live host discovery
- Passive recon using whois, theHarvester, Google Dorks
- Subdomain enumeration with Sublist3r and Amass
- SQL Injection & XSS attacks on DVWA or bWAPP
- Wireless scanning & simulated deauth attacks
- Social Engineering via SEToolkit phishing pages
- File encryption/decryption with GPG and OpenSSL
- Hash cracking using John the Ripper and Hashcat
- Exploitation via Metasploit on Metasploitable
- System hardening based on CIS Benchmarks
- Log analysis for incident response
- Final Capture the Flag challenge in lab environment

Structured Cybersecurity Course Roadmap

Module 1: Cybersecurity Foundations

Week	Theory Topics	Exercise
Week 1	Introduction to Cybersecurity Threat Landscape, Attack Types Domains: Network, AppSec, Cloud, IoT GRC: Governance, Risk Management (including AI GRC), Compliance (ISO 27001, NIST, GDPR)	Breach Analysis Case Study Cybersecurity Domains Brainstorm
Week 2	Cyber Kill Chain Model (Recon to Exploit) MITRE ATT&CK Framework Introduction TTPs: Real-World Mapping	Cyber Kill Chain Mapping Exercise ◇ MITRE ATT&CK Simulation Lab (Manual TTPs)

Module 2: Reconnaissance & Weaponization

Tools Focus: whois, nslookup, theHarvester, Google Dorks, dnsrecon, Sublist3r, Shodan, Maltego

Week	Theory Topics	Exercise
Week 3	Passive Recon: OSINT, Domain Footprinting, DNS Enumeration Subdomain Discovery, Shodan, Leaked Cameras	Recon Tools: theHarvester, dnsenum, Sublist3r , Subfinder ◇ Shodan, Google Dorking for Sensitive Info gathering
Week 4	Active Recon: Live Host Discovery, Banner Grabbing Fingerprinting (OS, Ports, Services)	nmap, netdiscover, fping, whatweb ◇ Banner grabbing with nc & nmap -sV

Module 3: Delivery, Exploitation & Installation

Tools Focus: SEToolkit, msfvenom, Metasploit, phishing, USB HID payloads

Week	**Theory Topics**	**Excercise**
Week 5	Social Engineering: Phishing, Pretexting, USB Drops SEToolkit & Payload Crafting	Email Phishing & Web Cloning with SET msfvenom for Payload Generation
Week 6	Malware Delivery: Executables, Macros, USB Drives Reverse Shells & RATs	Reverse Shell Delivery via Social Engineering ◇ Backdoor Injection & Listener Setup

Module 4: Post Exploitation & Privilege Escalation

Tools Focus: Metasploit, enum4linux, linpeas, netcat, mimikatz

Week	**Theory Topics**	**Exercise**
Week 7	Gaining Access & Maintaining Persistence Privilege Escalation Techniques	Metasploit Sessions & Token Stealing Local Privilege Escalation with linpeas
Week 8	Credential Dumping & Lateral Movement Covering Tracks	mimikatz, pwdump, hashdump Lateral Movement Simulation in Lab Setup

Module 5: Targeted Environments

Week	**Theory Topics**	**Exercise**
Week 9	Server-Side Pentesting (Linux/Windows) Service Exploits, SMB, RDP, SSH	Exploit Services (e.g., Samba, vsFTP) exploitdb, searchsploit, msfconsole

Week	Theory Topics	Exercise
Week 10	Web App Pentesting (OWASP Top 10) XSS, SQLi, LFI/RFI, Auth Bypass	DVWA/bWAPP: SQLi, XSS, Command Injection Burp Suite Manual Testing
Week 11	IOT pen testing concenpts	Capturing Handshake + Dictionary Attack
Week 12	Mobile Security & IoT (Intro only) Common Vulnerabilities (Rooting, exposed APIs, default creds)	Recon IoT on Local Network Android APK Analysis (Basic via MobSF if feasible offline)

Module 6: Hardening & Incident Response

Week	Theory Topics	Exercise
Week 13	Hardening Servers (Linux Best Practices)	Linux Hardening Checklist System Log Review for Attack Traces
Week 14	Incident Response Plan, Detection & Containment SIEM Concepts SPLUNK	Basic Manual IR Flow Recovery Simulation Lab

Any queries, write to us: info@staunchcuil.com