Byte Care Academy
Empowering Minds, Securing Futures

Cyber Security Courses

'Cyber Drill / Capture The Flag (CTF)'

Course Outline

Class No	Modules Details	Duration
Module 01: Introduction		
01	➢ Overview of CTF (Capture-the-flag) ➢ Introduction to Pentesting ➢ Penetration Testing Methodologies ➢ Lab Environment Setup for CTF ➢ Introduction with Linux ➢ Useful commands ➢ Hands-on problem solving of basic/general CTF challenges	**4 Hours**
Module 02: Network		
02	➢ Overview of network ➢ OSI layers & TCP/IP ➢ HTTP status code ➢ IP Header ➢ Introduction to network pentesting ➢ Network protocols enumeration & pentesting ➢ FTP ➢ DNS ➢ ARP ➢ NFS	**4 Hours**

	➢ SSH ➢ SMB & more. ➢ Network packet sniffing ➢ Packet Analysis ➢ Tools (Wireshark, Network Miner) ➢ Solving related CTF challenges	
Module 03: Footprinting & Reconnaissance		
03	➢ Overview of footprinting and reconnaissance ➢ Passive vs Active Reconnaissance ➢ Introduction with reconnaissance tools ➢ Different protocols enumeration ➢ Google dorking ➢ Overview of recon-ng ➢ Usage of Nmap for reconnaissance ➢ Identifying open ports, services, and protocols ➢ Firewall Detection and Bypass ➢ Recon website technologies and frameworks ➢ Searchsploit/Exploit-db ➢ Metasploit Framework	**4 Hours**
Module 04: Steganography		
04	➢ Introduction to steganography ➢ Image Steganography ➢ Video Steganography ➢ Audio Steganography ➢ Text Steganography ➢ Metadata Steganography ➢ Binary Steganography ➢ File password cracking ➢ Zip password cracking	**4 Hours**

	➢ Hydra ➢ John the Ripper ➢ Hashcat ➢ Ophcrack ➢ Steganography tools ➢ Advanced steganography techniques ➢ Solving related CTF challenges	
Module 05: Forensics		
05	➢ Introduction to forensics ➢ PCAP File Analysis ➢ File Signature Analysis ➢ Metadata Extraction ➢ Image forensic ➢ USB forensics ➢ Wireless forensics ➢ Browser History ➢ Memory forensics ➢ Email Header Analysis ➢ Registry Analysis ➢ Virtual Machine Forensics ➢ OS Forensic ➢ Basic Malware Analysis ➢ Log Analysis	**4 Hours**
Module 06: OSINT (Open Source Intelligence)		
06	➢ Introduction to OSINT ➢ OSINT Profiling ➢ Search Engine Queries ➢ Public Records and Databases ➢ Image OSINT ➢ Video OSINT ➢ Social Media OSINT ➢ People OSINT	**4 Hours**

	➢ Domain OSINT ➢ Email OSINT ➢ Dark Web OSINT ➢ Geolocation OSINT ➢ Business OSINT ➢ Solving related CTF challenges	
Module 07: Cryptography		
07	➢ Introduction to cryptography ➢ Encoding and Decoding ➢ Base Encoding/Decoding ➢ Encryption and Decryption ➢ Symmetric and asymmetric ➢ Hashing ➢ Plain text vs ciphertext ➢ Ciphers Identification ➢ Cipher to plaintext ➢ Substitution Cipher ➢ Transposition Cipher ➢ Steganography Cryptography ➢ Hash Cracking ➢ Solving related CTF challenges	**4 Hours**
Module 08: Reverse Engineering		
08	➢ Introduction of Reverse Engineering ➢ Overview of assembly language ➢ Familiarization with RE tools ➢ Static Analysis ➢ Dynamic Analysis ➢ Binary Analysis ➢ String Analysis ➢ Solving related CTF challenges	**4 Hours**

Module 09: Web application		
09	➢ Overview of web application architecture ➢ Understanding HTML, CSS, JavaScript, etc. ➢ Web application assessment ➢ SQL Injection ➢ Cross-Site Scripting ➢ Remote Code Execution ➢ Local File Inclusion (LFI) ➢ Remote File Inclusion (RFI) ➢ Command Injection ➢ Directory Traversal ➢ Insecure Direct Object Reference (IDOR) ➢ Session Hijacking ➢ XML External Entity (XXE) Injection ➢ File Upload exploitation ➢ Hidden file finding ➢ Subdomain finding ➢ Brute force attack ➢ Authentication Bypass ➢ Fuzzing ➢ Web exploitation Tools ➢ Browser extension for exploitation ➢ Solving related CTF challenges	**4 Hours**
Module 10: Web application		
10	➢ Assessment ➢ Participate in Real Life CTF Program	**4 Hours**
Module 10: Others		
11	➢ OS Enumeration ➢ Password Cracking ➢ OS Vulnerability scanning	**4 Hours**

	➢ Exploiting weak configurations ➢ Buffer overflow attacks ➢ Privilege escalation ➢ Key logger installation in OS ➢ Data exfiltration ➢ Clearing logs	
Review & Practice Class		
12	➢ Review ➢ Lab Practice	**4 Hours**
	Total Course Length	**48 Hours**