Byte Care Academy
Empowering Minds, Securing Futures

Cyber Security Courses

‘Penetration Testing’

Course Outline

Class No	Modules Details	Duration
Module 01: Introduction to Advanced Vulnerability Exploitation		
01	➢ Overview of cybersecurity landscape ➢ Importance of understanding advanced attack techniques ➢ Key concepts and terminology	**1 Hours**
Module 02: Reconnaissance, Scanning and Enumeration Techniques		
02	➢ Passive and active reconnaissance ➢ Open Source Intelligence (OSINT) tools and techniques ➢ Identifying and mapping target vulnerabilities ➢ Hands-on Activity: Using OSINT tools to gather information about a target	**2 Hours**
Module 03: Vulnerability Assessment		
03	➢ Vulnerability Management in a Nutshell ➢ Vulnerability Discovery ➢ Vulnerability Classification ➢ Prioritisation and Risk Assessment	**2 Hours**

	➢ Vulnerability Assessment Documentation and Maintenance ➢ Remediation and Mitigation	
Module 04: Advanced Exploitation Techniques for Systems Vulnerabilities		
04	➢ Network Systems Penetration Testing ➢ Operating Systems Penetration Testing ➢ Services Penetration Testing ➢ Privilege Escalation ➢ Hands-on Activity: Exploiting a web application with known vulnerabilities	**3 Hours**
Module 05: Advanced Exploitation Techniques for Web Application Vulnerabilities		
05	➢ Advanced SQL injection techniques ➢ Buffer overflows ➢ Cross-site scripting (XSS) ➢ Command injection ➢ Remote Code Execution (RCE) ➢ Cross-Site Request Forgery (CSRF) ➢ Hands-on Activity: Performing an RCE attack on a vulnerable web application	**2 Hours**
Module 06: Advanced Exploitation Techniques for Network Vulnerabilities		
06	➢ Man-in-the-middle (MITM) attacks ➢ DNS poisoning ➢ ARP spoofing ➢ Hands-on Activity: Conducting a MITM attack in a controlled environment	**2 Hours**

Module 07: Defense Strategies and Mitigation Techniques		
07	➢ Secure coding practices ➢ Implementing security controls ➢ Incident response planning ➢ Real-time attack detection and prevention ➢ Hands-on Activity: Creating and implementing a defence strategy for a simulated attack	**2 Hours**
Module 08: Defense Strategies and Mitigation Techniques		
08	➢ Activity: A team-based CTF exercise where participants apply the techniques learned to identify and exploit vulnerabilities in a controlled environment. ➢ Workshop Wrap-up ➢ Duration: 1 hour ➢ Topics Covered: ➢ Summary of key takeaways ➢ Q&A session ➢ Feedback and evaluation	**2 Hours**
	✓ **Total Course Length**	**16 Hours**