Name of the Programme: MCA
Course Code: CSA-529
Title of Course: Ethical Hacking
Number of Credits: 4 (4L-0T-0P)
Effective from AY: 2022-23

Prerequisites for the course	Internet Technologies, Operating System, Database Management, Programming Skills	
Objectives	To introduce the students to ethical hacking tools and practices used to protect systems from the wide-ranging impact of data breaches and cybersecurity incidents.	
Content	**Introduction:** The importance of security, The various phases involved in hacking, An overview of attacks and exploit categories, The legal implications.	2 hours
	Footprinting: Introduced to footprinting, Information gathering methodology, Tools used for the reconnaissance phase, countermeasures.	3 hours
	Scanning: Detecting 'live' systems on target network, Discovering services running/ listening on target systems, port scanning techniques, active and passive fingerprinting, Automated discovery tools.	3 hours
	Enumeration: Identifying valid user accounts or poorly protected resource shares, active connections to systems and directed queries, Null Session, NetBIOS Enumeration, SNMP enumeration, Applications and Banners.	3 hours
	System Hacking: Remote password guessing, Eavesdropping, Denial of Service, Buffer overflows, Privilege escalation, Password cracking, keystroke loggers, sniffers, Remote control and backdoors, Port redirection, Covering tracks, Hiding files	5 hours
	Trojans and Backdoors: Defining Trojans and Backdoors, Understanding the various backdoor genres, Trojan tools, Prevention methods and countermeasures, Anti-Trojan software.	2 hours
	Sniffers: Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing and Spoofing.	4 hours
	Denial of Service: DOS and Distributed DOS Attacks, Types of denial of service attacks, Tools for running DOS attacks, Tools for running DDOS attacks, Denial of Service Countermeasures	3 hours
	Social Engineering: Common Types of Attacks, Online Social Engineering, Reverse Social Engineering, Policies and Procedures, Employee awareness.	3 hours
	Session Hijacking: Spoofing Vs Hijacking, Types of session hijacking, TCP/IP concepts, Performing Sequence prediction, ACK Storms, Session Hijacking Tools.	4 hours
	Web Server Hacking: Web Servers and Common Vulnerabilities, Apache Web Server Security, IIS Server Security, Attacks against Web Servers, Countermeasures	3 hours
	Web Application Vulnerabilities: Common Web Application Security Vulnerabilities, Penetration Methodologies, Input Manipulation, Authentication And Session Management, Tools and Countermeasure.	5 hours
	Password cracking: HTTP Authentication Basic & Digest, NTLM Authentication, Certificate Based Authentication, Forms Based Authentication, Password Guessing, Password cracking Tools.	3 hours
	SQL injection: Exploiting the weakness of Server Side Scripting, Using SQL Injection techniques to gain access to a system, SQL Injection Scripts, Prevention and Countermeasures	3 hours

	Buffer Overflow: What is a Buffer Overflow, Exploitation, CPU / OS Dependency, Understanding Stacks, Stack Based Buffer Overflow, Defense against Buffer Overflows **Hacking wireless networks:** Introduction to 802.1, WEP, Cracking WEP Keys, WPA, WLAN Scanners, WLAN Sniffers, Securing Wireless Networks. **Viruses:** Types of viruses, virus signatures, Anti-virus software, few examples. **Evading Firewalls, IDS and Honeypots:** Intrusion Detection System, Integrity Verifiers, Intrusions Detection, Anomaly Detection, Signature Recognition, Protocol Stack Verification, Application Protocol Verification, Hacking Through Firewalls, Honey Pots.	4 hours 4 hours 2 hours 4 hours
Pedagogy		
References/ Readings	**Main Reading** 1. "Hacking Exposed", Osborne/ Mc Graw Hill. 2. "Hacking Exposed: Network Security Secrets and solutions", Osborne/ Mc Graw Hill. 3. "Hacking Exposed: Linux Security Secrets and Solutions", Mc Graw Hill. 4. "Hacking Exposed: Windows Security Secrets and Solutions", Mc Graw Hill. 5. "Hacking Exposed: Web Application Security Secrets and Solutions", Mc Graw Hill/Osborne.	
Course Outcomes	1. Discover the elements of a four-phase penetration test and how the four phases help successfully identify system vulnerability. 2. Learn about the different tools and techniques that hackers—including ethical hackers—employ.	

(Back to top)