University of Global Village

BSc in CSE Computer Science and Technology
7th Semester Skill Course
Cyber Security

Class Number	Topics	Class Hour	Practices Hour
Class-1	• Introduction of Cyber Security • What is hacking and who is a hacker • Types and Reasons of hacking • Effects of Computer hacking on an Organization • Network security challenges • Elements of information security • The security, functionality and usability triangle	2	6
New added boni	**virtualization and Lab Setup**		
Class-2	**Foot Printing** • Objectives of footprinting • Finding Company's details(Domain name, URL, Public and Restricted URL, Server details) • Finding the details of Domain registration, Range of IP address and DNS information • Finding the Location of Server and Services running on that Server • Tracking E-mail communications	2	10
Class-3	**Scanning** • Objectives of Network scanning • Finding the live Hosts in a Network • SNMP, SMTP and DNS Enumeration	2	10

	● Finding the Open ports and the services on a server ● OS fingerprinting		
Class-4	**Hacking Web Server and Application**		
	● What is Web Server ● Different web server applications in use ● Why Web server hacked and its Consequences ● Directory traversal attack ● Website defacement and password brute forcing	2	12
Class-5	**Session Hijacking**		
	● Objectives of session hijacking ● Session hijacking techniques and tools ● Defend against session hijacking ● Cross-site scripting attack	2	12
Class-6	**SQL Injection**		
	● What is SQL injection ● Effects and types of SQL injection attack ● SQL injection detection tools	2	8
Class-7	**Evading Firewalls, IDS and Honeypots**		
	● Objective and functions of Firewalls ● What is an IDS and how it works ● IDS tools ● Objectives and types of honeypot ● Honeypot detection tools	2	10
Class-8	**Buffer Overflow**		
	● What is buffer and usages of buffer in applications ● Buffer overflow and simple buffer overflow in C programming ● Defends against buffer overflow attacks	2	12
Class-9	**Denial of Service**		
	● What is DoS and DDoS attack ● DoS attack Techniques ● Defending DoS attack	2	8
Class-10	**Cryptography**		
	● Objectives and Types of Cryptography ● Ciper algorithm	2	10

	● Public Key Infrastructure ● What is Hash ● Cryptography attack		
Class-11	**System Hacking**		
	● Objectives and Goal of System Hacking ● Password cracking and complexity ● Password cracking methods ● Password guessing ● Brute force cracking ● Hybrid attack ● USB password stealers ● What and how to deploy a keylogger to a remote PC ● How to defend against a Keylogger	2	12
Class-12	**Sniffers**		
	● What is Sniffer and how Sniffer work ● Types of Sniffing ● How to defend against sniffer network ● ARP poison attack ● Threats of ARP poison attack ● How to put a PC promiscuous mode	2	12
Class-13	**Phishing**		
	● What is Phishing ● How to Phishing website in hosted ● How victims are tricked to access phishing websites ● How to defend against phishing attack	2	10
Class-14	**Malware**		
	● What is Malware and types of Malware ● What is virus program ● What are the properties of a virus program ● Types of virus ● What is Worm program and how worms are different from virus ● What is Trojan horse ● Types of Trojan ● Spyware ● Virus making Tools	2	10

Class-15	**Kali Linux**		
	● Objectives and uses of Kali Linux ● Tools for footprinting, scanning and sniffing ● What is Metasploit framework ● Using metasploit framework to attack windows machines	2	12
Class-16	**Wireless Hijacking**	2	10
	● Types of wireless network ● Finding a Wi-Fi network ● Types of Wi-Fi authentication ● Using centralized authentication server ● Using local authentication ● Weakness of WEP encryption ● How does WPA2 work ● Hardware and Software require to crack Wi-Fi networks ● How to crack WEP, WPA, WPA2 encryption ● How to defend against Wi-Fi cracking attack		
Class-17	**Penetration Testing**		
	● Objectives and types of Penetration testing ● Testing the network devices for mis-configuration ● Testing the server and hosting application for mis-configuration ● Testing the server and hosting application for vulnerability ● Testing wireless network ● Testing for Denial of service attack	2	15
Class-18	**CounterMeasure Techniques for (Network Level Attack)**		
	● Types of firewall ● Packet filtering firewall ● Security level gateway firewall ● Application level firewall ● Limitations of a firewall ● Different between IDS and IPS ● Placement and Configurations and IDS in the network ● Placement and Configurations and IPS in the network	2	12

Class-19	**Counter Measure Techniques for (Local System)**		
	● Identifying the vulnerability of a system ● Understanding the vulnerability of a system ● Patch Management ● Identify the patch for a Vulnerability ● Downloading the patch ● Deploying the patch to live network ● Finding the missing updates in an OS ● Microsoft Baseline Security analyzer ● Belarc Advisor	2	10
Class-20	**Counter Measure Techniques for (Malware Attacks)**		
	● Scanning system for malware infections ● Types of anti-malware ● Anti-virus ● Anti-worm ● Anti-Trojan ● **Anti-rootkit** ● **Internet security suites**	2	8

Osint :

Open Source Intelligence

— DNS Enumaration, ,Dig ,Nslookup & host

—- Meltago automotive information

—-- information with sodan

—--