Gyanmanjari Innovative University

Course Syllabus
Gyanmanjari College of Computer Application
Semester-7 (BCA)

Subject: Network Security and Ethical Hacking – BCACS10403

Type of course: Major Core

Prerequisite: Basic knowledge of computer systems, operating systems, and fundamental networking concepts such as IP addressing, internet usage, and network devices. Familiarity with basic command-line operations and elementary programming concepts will be advantageous.

Rationale:

This course provides foundational knowledge of network security concepts, threats, and defense mechanisms essential in today's digital environment. It equips students with practical skills in ethical hacking, scanning, and vulnerability assessment used in real-world cyber security practices. The inclusion of system hacking and exploitation techniques helps learners understand attacker methodologies for better defense strategies.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total Marks
				SEE		CCE			
CI	T	P	C	Theory	Practical	MSE	LWA	ALA	
3	0	2	4	75	25	30	20	50	200

Legends: *CI-Class Room Instructions; T – Tutorial; P - Practical; C – Credit; SEE - Semester End Evaluation; MSE- Mid Semester Examination; LWA - Lab Work Assessment; V – Viva voce; CCE-Continuous and Comprehensive Evaluation; ALA- Active Learning Activities.*

3 Credits * 25 Marks = 75 Marks (each credit carries 25 Marks) Theory
1 Credits * 25 Marks = 25 Marks (each credit carries 25 Marks) Practical
SEE 100 Marks will be converted in to 50 Marks
CCE 100 Marks will be converted in to 50 Marks
It is compulsory to pass in each individual component.

GYANMANJARI INNOVATIVE UNIVERSITY BHAVNAGAR

Course Content:

Sr. No	Course content	Hrs	% Weightage
1	**Introduction to Network Security and Network Fundamentals :** Importance of network security. TCP/IP Architecture, Topologies , Network Architectures : Network Types, Isolation, Remote Access, Security Technology: Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems.	7	20%
2	**Ethical Hacking :** Introduction to Ethical Hacking, Types of Ethical Hacking, Hacking Methodology: Foot printing and Scanning, Scanning, Enumeration, System Hacking and Trojans: System Hacking, Trojans and Black Box Vs White Box Techniques.	10	20%
3	**Reconnaissance, Scanning and Enumeration :** Introduction to Open Source Intelligence (OSINT),Passive OSINT, Introduction to Scanning and Enumeration, Scanning IP Address, Network and Its Services, Enumerating Tool -HTTP Smbclient. & Nmap, smtp-user-enum , Metasploit , net-cat,SNMP, Finding Vulnerabilities and Its Proof-of-Concept(POC).	10	20%
4	**System Hacking :** Basics of Shells - Reverse Shell, Bind Shell, Automated Exploitation – Metasploit, Manual Exploitation – Scripts, Password Attacks - Brute Force, Wordlist, Spraying, Malware Attacks - Trojans, Backdoors.	9	20%
5	**The Basic of Cryptography :** Introduction of Cryptography, Symmetric Key Cryptography – (AES - Advanced Encryption Standard, DES (Data Encryption Standard), 3DES),Asymmetric Key Cryptography – (RSA- Rivest–Shamir–Adleman, ECC - Elliptic Curve Cryptography, Diffie-Hellman, DSS) Hash Function, Encryption and Decryption	9	20%

Continuous Assessment:

Sr. No	Active Learning Activities	Marks

GYANMANJARI INNOVATIVE UNIVERSITY BHAVNAGAR

1	**Crack the Code: Wordlist Attack :** Students will create a sample password file and use a wordlist to perform a dictionary attack using tools like John the Ripper or Hydra. Students must capture screenshots of the process and record the cracked results And Upload on GMIU Web Portal.	10
2	**Footprinting Using Google Dorking :** Use advanced Google search operators (Google Dorks) to collect publicly available information about a target website, such as documents, emails, or directories.Make Document the search queries used, analyze the results, and explain how this information could be useful in the footprinting phase of ethical hacking Upload on GMIU Web Portal	10
3	**Password Strength & Cracking Analysis :** Students will test and compare weak and strong passwords to understand how password complexity affects security. Use appropriate tools to analyze the results, prepare a detailed report, and upload it to the GMIU Web Portal.	10
4	**Email Header Analysis Report :** Students will learn how to extract and analyze email headers to verify the authenticity of an email. Tracing originating IP addresses and scrutinizing technical metadata to detect sophisticated phishing or spoofing attempts. Students are required to document their forensic findings in a formal report for submission via the GMIU portal.	10
5	**Cyber Security Project :** Students will be required to develop a project based on the problem statement provided by the faculty. Students will design and a short report describing the project objectives, working process, components used, and data flow must be prepared and uploaded on the GMIU web portal.	10
Total		**50**

Suggested Specification table with Marks (Theory):75

Distribution of Theory Marks **(Revised Bloom's Taxonomy)**						
Level	Remembrance (R)	Understanding (U)	Application (A)	Analyze (N)	Evaluate (E)	Create (C)
Weightage	25%	25%	15%	15%	10%	10%

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcome:

GYANMANJARI INNOVATIVE UNIVERSITY BHAVNAGAR

After learning the course the students should be able to:	
CO1	Understand fundamental concepts of network security, TCP/IP architecture, network topologies, and security mechanisms such as firewalls, IDS, and IPS.
CO2	Implement ethical hacking concepts, types of hackers, and apply footprinting, scanning, and enumeration techniques for information gathering.
CO3	Apply reconnaissance and scanning tools (e.g., Nmap, Netcat, Metasploit) to identify vulnerabilities and analyze network services.
CO4	Analyze system hacking techniques including password attacks, malware, shells, and exploitation using automated and manual methods.
CO5	Describe and implement cryptographic techniques including symmetric and asymmetric encryption, hashing, and their significance in ensuring data security.

List of Practical

Sr. No	Descriptions	Unit No	Hrs
1.	**Study of following network emulators:** i) WHOIS Search ii) Whois CLI Command iii) Nslookup iv) Host v) Ping vi) Traceroute vii) Netstat viii) uptime	1	02
2.	**Create a malicious program that is (At least one program) :** i) Virus ii) Worm iii) Trojan	2	02
3.	Performing Password Cracking using Hydra Tool, Metasploit.	3	02
4.	How to Gather Info on Someone through OSINT	3	02
5.	Performing ARP Spoofing Attack using Ettercap Tool.	4	02
6.	Performing XSS Attack on Vulnerable Web Application.	4	02
7.	Performing Directory Traversal Attack on Web Application.	4	02
8.	Digital Steganography – Hiding sensitive information within Image, Audio, and Video files	4	02
9.	Examine keylogging attacks and how they compromise user privacy.(Hack System with Keylogger).	4	02
10.	Exploiting Improper Input Validation for Unauthorized File Access and Session Hijacking.	4	02

11.	Analyze and execute Evading IDS, Bypass Windows Firewalls, and Honeypots Module Evaluate it.	4	02
12.	To demonstrate the methodology of attacking / Hacking Web Server.	4	02
13.	Testing Web Application Security using Burp Suite	4	02
14.	Cracking Wi-Fi Password using Aircrack-ng (Wireless Security Attack)	4	02
15.	**Consider of Case Study on :** **1. Phishing Attack on Employees :** To analyze a real-world phishing attack scenario and understand its impact, causes, and preventive measures. **2. Symmetric Key Cryptography :** An organization needs to transfer confidential files between two departments over a network. To ensure data security, both sender and receiver use the same secret key to encrypt and decrypt the data.	5	02
Total			**30**

Instructional Method:

The course delivery method will depend upon the requirement of content and need of students. The teacher, in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc. From the content 10% topics are suggested for flipped mode instruction.

Students will use supplementary resources such as online videos, NPTEL/SWAYAM videos, e-courses, Virtual Laboratory.

The internal evaluation will be done on the basis of Active Learning Assignment.

Practical/Viva examination will be conducted at the end of semester for evaluation of performance of students in the laboratory.

Reference Books:

[1] Hands-On Ethical Hacking and Network Defense – by Michael T. Simpson, Nicholas D. Antill, and Robert S. Wilson , Cengage Learning , 2022/2023 (4th Edition).

[2] Cryptography and Network Security: Principles and Practice – by William Stallings , Pearson Education, 2023 (8th Edition).

GYANMANJARI INNOVATIVE UNIVERSITY BHAVNAGAR

[3] The Basics of Hacking & Pen Testing – by Patrick Engebretson.

[4] Metasploit: The Penetration Tester's Guide – by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni (Classic).

[5] The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws – by Dafydd Stuttard & Marcus Pinto , Wiley.