GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering
Subject Code: 3150714
Semester – V
Subject Name: Cyber Security

Type of course: Undergraduate (Open Elective)

Prerequisite: None

Rationale: In this digital age, the information and data are immense and need to be secured. The cyber crimes have increased as attackers see it as gaining big rewards. There is a need to examine the cyber attack patterns and provide security measures for them and also need to learn the cyber laws formed to effectively act upon cyber crimes.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE (E)	PA (M)	ESE (V)	PA (I)	
2	0	2	3	70	30	30	20	150

Content:

Sr. No.	Content	Total Hrs	Marks Weight age (%)
1	Systems Vulnerability Scanning Overview of vulnerability scanning, Open Port / Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit. Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance – Nmap, THC-Amap and System tools. Network Sniffers and Injection tools – Tcpdump and Windump, Wireshark, Ettercap, Hping Kismet	08	25
2	Network Defense tools Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs Firewall, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, Snort: Introduction Detection System	06	25
3	Web Application Tools Scanning for web vulnerabilities tools: Nikto, W3af, HTTP utilities - Curl, OpenSSL and Stunnel, Application Inspection tools – Zed Attack Proxy, Sqlmap. DVWA, Webgoat, Password Cracking and Brute-Force Tools – John the Ripper, L0htcrack, Pwdump, HTC-Hydra	06	25
4	Introduction to Cyber Crime and law Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics, Realms of the Cyber world, Recognizing and Defining Computer Crime, Contemporary Crimes, Contaminants and Destruction of Data, Indian IT ACT 2000.	03	10
5	Introduction to Cyber Crime Investigation Keyloggers and Spyware, Virus and Warms, Trojan and backdoors, Steganography, DOS and DDOS attack, SQL injection, Buffer	05	15

	Overflow, Attack on wireless Networks.		

Suggested Specification table with Marks (Theory): (For BE only)

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
20	**30**	**20**	**--**	**--**	**--**

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Course Outcomes: Students will be able to

Sr. No.	CO statement	Marks % weightage
CO-1	Describe system and web vulnerability.	40
CO-2	Evaluate network defence tools.	30
CO-3	Understand the cyber laws	10
CO-4	Investigate a cybercrime, prepare report and apply laws for the case	20

Reference Books:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley
2. Cyber Security and Cyber Laws Paperback – 2018 by Alfred Basta, Nadine Basta , Mary Brown , Ravinder Kumar, publication Cengage
3. 3. Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.
4. Cyber security and laws – An Introduction, Madhumita Chaterjee, Sangita Chaudhary, Gaurav Sharma, Staredu Solutions

List of Open Source Software/learning website:

www.wireshark.org

List of Practical:

1. Install Kali Linux. Examine the utilities and tools available in Kali Linux and find out which tool is the best for finding cyber attack/vulnerability.
2. Evaluate network defense tools for following
   (i) IP spoofing
   (ii) DOS attack
3. Explore the Nmap tool and list how it can be used for network defence.
4. Explore the NetCat tool.
5. Use Wireshark tool and explore the packet format and content at each OSI layer.
6. Examine SQL injection attack.

7. Perform SQL injection with SQLMap on vulnerable website found using google dorks.

8. Examine software keyloggers and hardware keyloggers.
9. Perform online attacks and offline attacks of password cracking.
10. Consider a case study of cyber crime, where the attacker has performed on line credit card fraud. Prepare a report and also list the laws that will be implemented on attacker..

Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE – SEMESTER- V EXAMINATION-SUMMER 2023

Subject Code: 3150714 **Date: 23/06/2023**

Subject Name: Cyber Security

Time: 02:30 PM TO 05:00 PM **Total Marks: 70**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

Marks

Q.1 **(a)** Define System and Web Vulnerability. **03**

(b) Explain Metasploit and OpenVAS. **04**

(c) Describe Nmap. Explain different functionality with its command in detail. **07**

Q.2 **(a)** Define Snort. **03**

(b) Differentiate between Stateful and Stateless firewalls. **04**

(c) Explain Network Sniffers with suitable example. **07**

OR

(c) Define NAT. Describe Port Forwarding with its types in detail. **07**

Q.3 **(a)** Explain Curl, OpenSSL and Stunnel. **03**

(b) Define Password cracking and Brute force tools. Explain any one in brief. **04**

(c) Describe DVWA. Explain SQL injection in DVWA with example in detail. **07**

OR

Q.3 **(a)** Explain Zed Attack Proxy. **03**

(b) Explain following terms: 1. Datapipe 2. Fpipe 3.WinRelay 4.Traffic Probe **04**

(c) Discuss the Web Vulnerability tools in detail. **07**

Q.4 **(a)** Define Digital Forensics. **03**

(b) Explain types of Cyber Crimes. **04**

(c) Explain IT Act, 2000. List out and discuss different sections under IT Act, 2000 in detail. **07**

OR

Q.4 **(a)** Define Incident Response. **03**

(b) Discuss about Contaminants and Destruction of Data. **04**

(c) Discuss Attack vector. List out different types of Attack vector. **07**

Q.5 **(a)** Explain SQL Injection. **03**

(b) Discuss Keyloggers and Spyware. **04**

(c) Explain Virus, Worms, Trojan Horses and Backdoors in detail with example. **07**

OR

Q.5 **(a)** Explain Steganography with example. **03**

(b) Explain Buffer Overflow attack in detail. **04**

(c) Describe DOS and DDOS attack with suitable example. **07**

Enrolment No./Seat No_____________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–V (NEW) EXAMINATION – SUMMER 2024

Subject Code:3150714 Date:16-05-2024

Subject Name:Cyber Security

Time:02:30 PM TO 05:00 PM Total Marks:70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	Write sort note on Indian IT ACT 2000.	**03**
	(b)	What is the difference between Threat, Vulnerability, and Risk and Computer Virus?	**04**
	(c)	What is the need of Demilitarized Zone (DMZ)? Explain with example.	**07**
Q.2	**(a)**	Define the term in briefly: (i) Open Port Identification (ii) Banner Check	**03**
	(b)	What is Probe. Explain its different types.	**04**
	(c)	List and explain types of Network Sniffer. List Network Sniffers and Injection tools.	**07**
		OR	
	(c)	Explain Ettercap and Hping Kismet.	**07**
Q.3	**(a)**	What do you mean by Cyber Crime? How do you relate it with Hacking?	**03**
	(b)	Explain Traditional Problems Associated with Computer Crime.	**04**
	(c)	What is firewall? Explain three main type of firewall.	**07**
		OR	
Q.3	**(a)**	How ZAP proxy works? Explain with suitable example.	**03**
	(b)	What do you mean of contaminants and destruction of data? Explain it.	**04**
	(c)	Explain Digital Forensics life cycle in detail.	**07**
Q.4	**(a)**	Explain Curl, OpenSSL and Stunnel.	**03**
	(b)	Explain Wireshark and how do we use Wireshark to find a password in network?	**04**
	(c)	What is Netcat? Explain steps for File Transfer process by using Netcat in detail.	**07**
		OR	
Q.4	**(a)**	What is Metasploit? Explain payload types in short.	**03**
	(b)	How Buffer overflow attack works?	**04**
	(c)	What is Nmap? Explain different functionality with its command in detail.	**07**
Q.5	**(a)**	What is Brute-Force Attack? How it can be prevented?	**03**
	(b)	Justify the attack vector. List out different types of attack vector.	**04**
	(c)	Explain how SQL Injection attacks can be prevented.	**07**
		OR	
Q.5	**(a)**	What is Keyloggers? Explain different types of Keyloggers.	**03**
	(b)	Explain L0htcrack, HTC-Hydra, Pwdump.	**04**
	(c)	Explain DVWA and Web goat.	**07**

****

Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–V (NEW) EXAMINATION – WINTER 2021

Subject Code:3150714 **Date:15/12/2021**

Subject Name:Cyber Security

Time:02:30 PM TO 05:00 PM **Total Marks: 70**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	Explain Vulnerability Scanning.	**03**
	(b)	Define the term in briefly: (i) Open Port Identification (ii) Banner Check	**04**
	(c)	Describe Network Sniffers and Injection Tool. Explain any two injection tools in brief.	**07**
Q.2	**(a)**	Define Network Address Translation.	**03**
	(b)	What is Probe. Explain its different types.	**04**
	(c)	Differentiate between Packet Filter and Firewall.	**07**
		OR	
	(c)	Differentiate between Stateless and Stateful Firewalls.	**07**
Q.3	**(a)**	Define Snort.	**03**
	(b)	What are the different usages of Network Sniffers? List out it.	**04**
	(c)	List out various Application Inspection tools. Explain any two.	**07**
		OR	
Q.3	**(a)**	How do you protect Wireless Network?	**03**
	(b)	What do you mean by Password cracking and brute force tools? Explain any one in brief.	**04**
	(c)	What are the different kinds of Web Vulnerabilities Tools available? Explain any two in brief.	**07**
Q.4	**(a)**	Define Denial-of-Service.	**03**
	(b)	Justify the attack vector. List out different types of attack vector.	**04**
	(c)	What is Firewall and illustrate its different types.	**07**
		OR	
Q.4	**(a)**	Illustrate the aim and objective of Indian IT ACT 2000.	**03**
	(b)	List out different types of Traditional Problems Associated with Computer Crime.	**04**
	(c)	What is Incident Response. Explain it process flow with appropriate diagram.	**07**
Q.5	**(a)**	Define the term: (i)Trojan Horse (ii)Spyware	**03**
	(b)	What is Destruction of Data. List out the different reason for it.	**04**
	(c)	What are the Cyber-Crime Scenarios and explain its applicability for Legal Sections?	**07**
		OR	
Q.5	**(a)**	What is Keyloggers? Explain different types of Keyloggers.	**03**
	(b)	Differentiate between Computer Viruses and Worms.	**04**
	(c)	Define the Cyber Crime in your own word. Explain the different type of classification of Cyber Crime.	**07**

****

Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–V (NEW) EXAMINATION – WINTER 2022

Subject Code:3150714 Date:04-01-2023

Subject Name:Cyber Security

Time:10:30 AM TO 01:00 PM Total Marks:70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			Marks
Q.1	**(a)**	Describe Reconnaissance and Probe	**03**
	(b)	Explain Phishing and 3 ways it is done.	**04**
	(c)	Explain Metasploit and Nmap	**07**
Q.2	**(a)**	Describe NAT with example	**03**
	(b)	Differentiate between Stateful and Stateless firewalls.	**04**
	(c)	Explain Injection tools like Tcpdump, Windump and Wireshark	**07**
		OR	
	(c)	Explain Ettercap and Hping Kismet	**07**
Q.3	**(a)**	Explain Zed Attack Proxy.	**03**
	(b)	Differentiate between John Ripper and HTC-Hydra.	**04**
	(c)	Explain the web vulnerability tools like Nikto and W3af.	**07**
		OR	
Q.3	**(a)**	Explain Curl, OpenSSL and Stunnel.	**03**
	(b)	Differentiate between packet filter and firewall.	**04**
	(c)	Explain the network monitoring tool Snort.	**07**
Q.4	**(a)**	Describe attack vector, cyberspace and IT act 2000.	**03**
	(b)	Explain hacking and its types.	**04**
	(c)	Explain Incident response and digital forensics.	**07**
		OR	
Q.4	**(a)**	List three contemporary crimes?	**03**
	(b)	Explain the types of cybercrimes.	**04**
	(c)	Explain DVWA and Web goat	**07**
Q.5	**(a)**	Features of Trojan virus.	**03**
	(b)	List four functions a backdoor can do to help the attacker.	**04**
	(c)	Explain how SQL Injection attacks can be prevented.	**07**
		OR	
Q.5	**(a)**	What is Stegnography and list two examples.	**03**
	(b)	Differentiate between 1. DOS and DDOS attack 2. Keyloggers and Spyware	**04**
	(c)	Explain the tools for attacking wireless Networks.	**07**

****

Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–V (NEW) EXAMINATION – WINTER 2023

Subject Code:3150714 Date:05-12-2023

Subject Name: Cyber Security

Time:10:30 AM TO 01:00 PM Total Marks:70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	Describe Network Sniffers with suitable example.	**03**
	(b)	What is Cyber Crime? Explain different types of Cyber Crimes in brief.	**04**
	(c)	What do you mean by Password cracking and brute force tools? Explain any one in detail.	**07**
Q.2	**(a)**	Differentiate between Computer Viruses and Worms.	**03**
	(b)	What are the Cyber Crime Scenarios and explain its applicability for Legal Sections?	**04**
	(c)	Explain attacks on wireless network. How do you protect Wireless Network?	**07**
		OR	
	(c)	Define Denial-of-Service (DOS). How can we prevent DDOS attack?	**07**
Q.3	**(a)**	What is Keyloggers? Explain different types of Keyloggers.	**03**
	(b)	Explain Wireshark and how do we use Wireshark to find a password in network?	**04**
	(c)	What is Hacking? Explain types of Hackers.	**07**
		OR	
Q.3	**(a)**	Difference between Stateless Vs Stateful Firewalls.	**03**
	(b)	Define Snort? What is the difference between IPS and IDS?	**04**
	(c)	Explain in details: Network Address Translation (NAT) with suitable diagram.	**07**
Q.4	**(a)**	What is SQL injection?	**03**
	(b)	List out different types of Traditional Problems Associated with Computer Crime.	**04**
	(c)	Describe all HTTP utilities in details.	**07**
		OR	
Q.4	**(a)**	What is contemporary approach in criminology in the world of computer science?	**03**
	(b)	Explain in details: Buffer Overflow.	**04**
	(c)	Explain in details: Hacking, Attack vectors, Cyberspace and Criminal Behavior.	**07**
Q.5	**(a)**	Explain Vulnerability Scanning.	**03**
	(b)	What is OpenVas? Write advantage and disadvantage of OpenVas.	**04**
	(c)	Describe credit card fraud that can be done through mobile or other wireless devices.	**07**
		OR	
Q.5	**(a)**	Explain passive attacks and active attacks with respect to cyber criminals?	**03**
	(b)	What is Packet Filter Vs Firewall?	**04**
	(c)	What is Incident Response. Explain it process flow with appropriate diagram.	**07**

****