DHANALAKSHMI SRINIVASAN ENGINEERING COLLEGE
(AUTONOMOUS)
(Approved by AICTE & Affiliated to Anna University, Chennai)
Re-Accredited with 'A' Grade by NAAC, Accredited by TCS
Accredited by NBA – BME, ECE & EEE
PERAMBALUR - 621 212. Tamil Nadu.
website : www.dsengg.ac.in

COURSEPLAN

Course Code/Name	U23AIV31-CYBER SECURITY			
Year/Section/Department	III/B/AI&DS			
Credits Details	**L:3**	**T:0**	**P:0**	**C:3**
Total Contact Hours Required	45			

Syllabus:

UNIT I INTRODUCTION	**No. of Periods:9**
Cyber Security – History of Internet – Impact of Internet – CIA Triad; Reason for Cyber Crime – Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes – A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.	
UNIT II ATTACKS AND COUNTERMEASURES	**No. of Periods9**
OSWAP; Malicious Attack Threats and Vulnerabilities: Scope of Cyber-Attacks – Security Breach – Types of Malicious Attacks – Malicious Software – Common Attack Vectors – Social engineering Attack – Wireless Network Attack – Web Application Attack – Attack Tools – Countermeasures	
UNIT III RECONNAISSANCE	**No. of Periods9**
Harvester – Whois – Netcraft – Host – Extracting Information from DNS – Extracting Information from E-mail Servers – Social Engineering Reconnaissance; Scanning – Port Scanning – Network Scanning and Vulnerability Scanning – Scanning Methodology – Ping Sweer Techniques – Nmap Command Switches – SYN – Stealth – XMAS – NULL – IDLE – FIN Scans – Banner Grabbing and OS Finger printing Techniques	
UNIT IV INTRUSION DETECTION	**No. of Periods9**
Host -Based Intrusion Detection – Network -Based Intrusion Detection – Distributed or Hybrid Intrusion Detection – Intrusion Detection Exchange Format – Honeypots – Example System Snort.	
UNIT V INTRUSION PREVENTION	**No. of Periods9**
Firewalls and Intrusion Prevention Systems: Need for Firewalls – Firewall Characteristics and Access Policy – Types of Firewalls – Firewall Basing – Firewall Location and Configurations – Intrusion Prevention Systems – Example Unified Threat Management Products.	

Objective:

The main learning objective of this course is to prepare the students:

To learn cybercrime and cyberlaw.

To understand the cyber-attacks and tools for mitigating them.

To understand information gathering.

To learn how to detect a cyber-attack.

To learn how to prevent a cyber-attack.

Text Book:

T1: Anand Shinde, "Introduction to Cyber Security Guide to the World of Cyber Security", Notion Press, 2021 (Unit 1)

T2: Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publishers, 2011 (Unit 1)

Reference Book:

R1: David Kim, Michael G. Solomon, "Fundamentals of Information Systems Security", Jones & Bartlett Learning Publishers, 2013 (Unit 2)

R2: Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made easy", Elsevier, 2011 (Unit 3)

R3: Kimberly Graves, "CEH Official Certified Ethical hacker Review Guide", Wiley Publishers, 2007 (Unit 3)

R4: William Stallings, Lawrie Brown, "Computer Security Principles and Practice", Third Edition, Pearson Education, 2015 (Units 4 and 5)

R5: Georgia Weidman, "Penetration Testing: A Hands-On Introduction to Hacking", No Starch

Website:

W1: HYPERLINK "https://www.nist.gov/cybersecurity-and-privacy" \t "https://www.google.com/_blank" https://www.nist.gov/cybersecurity-and-privacy

W2: https://www.dsci.in/

W3: HYPERLINK "https://safety.google/intl/en_in/safety/" \t "https://www.google.com/_blank" https://safety.google/intl/en_in/safety/ HYPERLINK

Online Mode of Study:

NPTEL details can be listed.

HYPERLINK "https://www.google.com/url?sa=i&source=web&rct=j&url=https://onlinecourses.nptel.ac.in/noc24_cs121/announcements&ved=2ahUKEwiqstq5-JmRAxVQamwGHXGWK9IQy_kOegQIAxAC&opi=89978449&cd&psig=AOvVaw0YKnUVW3Y-UFfsre3WIR1x&ust=1764594377685000" \t "https://www.google.com/_blank" https://onlinecourses.nptel.ac.in/noc24_cs121/announcements

HYPERLINK "https://onlinecourses.nptel.ac.in/noc25_cs117/preview" \t

Course Plan:

Topic Number	Topic	Reference Detail	Page Number	Mode of teaching	Number of Periods Required	Cumulative Period
UNIT I–INTRODUCTION						**9**
1	Introduction to Cyber Security	T1	2	BB	1	1
2	History of Internet & Cyber Security	T1	3-5	BB	1	2
3	Impact of Internet – CIA Triad	T1	5-8	BB	1	3
4	Reason for Cyber Crime & Need for Cyber Security	T1	8-12	PPT	1	4
5	History of Cyber Crime and Cybercriminals	T1	12-14	BB	1	5
6	Classification of Cybercrimes	T1	14-20	BB	1	6
7	Global Perspective on Cybercrimes	T1	20-23	PPT	1	7
8	Cyber Laws Overview	T1	23-24	BB	1	8
9	Indian IT Act – Cybercrime & Laws – Punishments	T1	24-26	BB	1	9
Outcome of Unit I: **CO1**:Explain the basics of cyber security, cyber crime and cyber law						
UNIT II-ATTACKS AND COUNTERMEASURES						**9**
10	Overview of OSWAP – Attack Threats & Vulnerabilities	R1	28-29	BB	1	10
11	Cyber Attacks: Scope & Security Breaches	R1	29-33	BB	1	11
12	Types of Malicious Attacks	R1	34-40	PPT	1	12
13	Malicious Software – Malware Samples	R1	41-52	BB	1	13
14	Common Attack Vectors	R1	53	BB	1	14

15	Social Engineering Attacks	R1	53	BB	1	15
16	Wireless Network Attacks	R1	53-54	BB	1	16
17	Web Application Attacks	R1	54-57	BB	1	17
18	Attack Tools & Countermeasures	R1	57-66	BB	1	18

Outcome of Unit II:

CO2: Classify various types of attacks and learn the tools to launch the attacks

	UNIT III–RECONNAISSANCE					**9**
19	Harvester, Whois, Netcraft Tools	R2	80-82	BB	1	19
20	Host Information Gathering	R2	83-86	BB	1	20
21	DNS Enumeration Techniques	R2	87-90	PPT	1	21
22	Email Server Info Extraction	R2	90-94	BB	1	22
23	SocialEngineering Reconnaissance	R2	95-98	BB	1	23
24	Scanning Techniques	R2	98-100	BB	1	24
25	Vulnerability Scanning – Methodology	R2	100-103	BB	1	25
26	Nmap Basics – Scanning Types	R2	104-105	BB	1	26
27	OS Fingerprinting, Banner Grabbing	R2	105-106	BB	1	27

Outcome of Unit III:

CO3: Apply various tools to perform information gathering

	UNIT IV–INTRUSION DETECTION					**9**
28	Host-Based Intrusion Detection	R4	509	BB	1	28
29	Network-Based Intrusion Detection	R4	509-511	BB	1	29
30	Distributed & Hybrid IDS	R4	444-449	PPT	1	30

31	Intrusion Detection Tools Overview	R4	519-523	BB	1	31	
32	Intrusion Detection Exchange Format	R4	523-526	BB	1	32	
33	Signature & Anomaly-Based Detection	R4	526-529	BB	1	33	
34	Real-time Detection Approaches	R4	530-532	BB	1	34	
35	Honeypots – Purpose & Deployment	R4	533-535	BB	1	35	
36	Example IDS: Snort – Architecture	R4	536-538	BB	1	36	
Outcome of Unit IV:							
UNIT V–INTRUSION PREVENTION						**9**	
37	Need for Firewalls & Prevention Systems	R4	526-528	BB	1	37	
38	Firewall Characteristics	R4	288-289	BB	1	38	
39	Access Policies – Rules	R4	305-310	BB	1	39	
40	Types of Firewalls	R4	289-304	BB	1	40	
41	Firewall Basing	R4	237-239	BB	1	41	
42	Firewall Configurations	R4	401-440	BB	1	42	
43	Intrusion Prevention Systems	R4	440-444	BB	1	43	
44	Unified Threat Management (UTM)	R4	444 -446	BB	1	44	
45	Case Studies & Example Products	R4	446-448	BB	1	45	
Outcome of Unit V: **CO 5:** Apply intrusion prevention techniques to prevent intrusion **CO 6:** Develop and Evaluation of Intrusion Prevention Systems							
CO4: Apply intrusion techniques to detect intrusion							

Course Outcome:

At the end of course: Students should be able to do:

CO 1: Explain the basics of cyber security, cyber crime and cyber law
CO 2: Classify various types of attacks and learn the tools to launch the attacks
CO 3: Apply various tools to perform information gathering
CO 4: Apply intrusion techniques to detect intrusion
CO 5: Apply intrusion prevention techniques to prevent intrusion
CO 6: Develop and Evaluation of Intrusion Prevention Systems

Course Outcome Vs Program Outcome Mapping:

	Program Outcomes												**PSO**		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO-1	3	3	0	0	0	2	1	1	0	2	0	0	3	2	2
CO-2	3	3	2	2	0	0	0	0	0	2	1	1	3	3	2
CO-3	3	3	3	3	3	0	0	0	1	3	1	1	3	3	3
CO-4	2	3	3	3	2	0	0	0	0	2	0	1	3	3	2
CO-5	2	3	3	3	3	1	0	0	0	3	1	1	3	3	3
AVG	2.6	2.8	2.75	2.75	2.67	1.50	1	1	1	2.40	1	1	3	2.8	2.4

Content beyond Syllabus:

Ai-driven threat detection.
Blockchain for cybersecurity.
Security in IoT devices.
Dark web monitoring tools.

Internal Evaluation Components:

Web portal	**Assignment**	**Components**	**Topic Number with Topic/Unit Details**	**Relevance to CO**
Web portal 1	**--**	**Assessment–I(60)**	**Unit I andII**	**CO 1 & CO2**
	1	**Assignment – Hand written(20)**	1. History of Cyber Crime and Cybercriminals 2. Reason for Cyber Crime & Need for Cyber Security 3. Social Engineering Attacks	**CO1&CO 2**

	2	**Assignment – Presentation(20)**	1. Classification of Cybercrimes 2. Types of Malicious Attacks 3. Wireless Network Attacks	**CO1&CO 2**
Web portal 2	**--**	**Assessment–II (60)**	Unit III and IV	**CO3 & CO4**
	3	**Seminar(20)**	1. Network-Based Intrusion Detection 2. DNS Enumeration Techniques 3. Vulnerability Scanning – Methodology	**CO3& CO4**
	4	**Case Study Report (20)**	1.Host-Based Intrusion Detection 2.Nmap Basics – Scanning Types 3.Signature & Anomaly-Based Detection	**CO3& CO4**
Web portal 3	**--**	**Model Exam(75)**	**Unit I to V**	**CO1to CO6**
	5	**MCQ(15)**	Unit I to V	**CO1 to CO6**
	-	**Course Attendance (10)**	**Attendance Percentage** >=75% =2 Mark >=80% =4 Mark >=85% =6 Mark >=90% =8 Mark >=95% =10 Mark	**--**

Submission Details:

Phase1 (Before AT 1)		**Phase 2 (Before AT 2)**		**Phase 3(Model)**
Assignment 1	**Assignment 2**	**Assignment 3**	**Assignment 4**	**Assignment 5**

PLAN OF ASSESSMENT TEST–DISTRIBUTION OF MARKS:

DSEC/AI&DS/U23CSV63/ III/ VI

TEST	CO-MARK WISE DISTRIBUTION						BLOOM'S LEVEL MARK WISE DISTRIBUTION					
AT-1	CO1	CO2	CO3	CO4	CO5	CO6	BTL1	BTL2	BTL3	BTL4	BTL5	BTL6
AT-2	CO1	CO2	CO3	CO4	CO5	CO6	BTL1	BTL2	BTL3	BTL4	BTL5	BTL6
MODEL	CO1	CO2	CO3	CO4	CO5	CO6	BTL1	BTL2	BTL3	BTL4	BTL5	BTL6

Prepared by **Verified By**

Approved By
PRINCIPAL