



ERODE SENGUNTHAR ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University, Chennai &
Accredited by National Board of Accreditation (NBA), New Delhi,
National Accreditation Assessment Council (NAAC), Bangalore with A Grade
PERUNDURAI-638 057, TAMILNADU, INDIA



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

Innovative Teaching Practice

Name of the Subject with Code : 21CSX04 – CYBER SECURITY AND ETHICAL HACKING
Course Coordinator : Mr A Rajesh, Associate Professor/M.Tech CSE
Academic Year : 2023-2024 Even Semester
Year/Semester : III Year / VI Semester
Branch : M.Tech Computer Science and Engineering

Index

S.No	Content
1	Lesson plan with innovative practices and content beyond syllabus highlighted
2	Innovative teaching process evidence
3	Log book copies
4	Content beyond syllabus
5	Innovative assignment questions and sample papers



Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.



ERODE SENGUNTHAR ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai, Accredited by National Board of Accreditation (NBA), New Delhi & National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade
PERUNDURAI -638 057, TAMILNADU, INDIA.



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

LESSON PLAN

Name of the Subject with Code : 21CSX04 CYBER SECURITY AND ETHICAL HACKING.
Course Coordinator : Mr. A.RAJESH , ASSOCIATE PROFESSOR
Academic Year : 2023-2024
Year/ Semester : III / VI
Branch : M.Tech. COMPUTER SCIENCE AND ENGINEERING

COURSE OBJECTIVES:

The purpose of learning this course is:

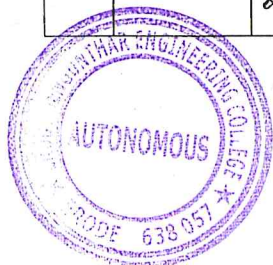
- To learn cybercrime and cyber law.
- To understand the cyber attacks and tools for mitigating them.
- To understand information gathering.
- To understand the basics of computer based vulnerabilities.
- To explore different foot printing, reconnaissance and scanning methods.

COURSE OUTCOMES:

At the end of the course, the students will be able to:

- CO1: Explain the basics of cyber security, cyber crime and cyber law.
CO2: Classify various types of attacks and learn the tools to launch the attacks.
CO3: Apply various tools to perform information gathering
CO4: To express knowledge on basics of computer based vulnerabilities.
CO5: To gain understanding on different foot printing, reconnaissance and scanning methods.
CO6: Understand about the Advancement in Cyber Security and Ethical Hacking

S. No.	Planned date	Actually conducted date	Topic to be covered	Key terms	Objective	Methodology adopted	ICT Tools used	No of periods required
UNIT – I INTRODUCTION								
1.	22.01.24	22/1/24	Course Orientation PPT	Web Resources, Working scope	To know the syllabus of Cyber Security and Ethical Hacking and unit description	Lecturing	Power point presentation software	1
2.	24.01.24	24/1/24	<ul style="list-style-type: none"> Cyber Security History of Internet Impact of Internet 	<ul style="list-style-type: none"> Encryption DoS Botnet Phishing 	To understand the basic Concept of Cyber Security	Lecturing	Power point presentation software	1
3.	29.01.24	29/1/24	<ul style="list-style-type: none"> CIA Triad Reason for Cyber Crime 	<ul style="list-style-type: none"> Client List Insiders 	To understand the Reason for Cyber Crime	Lecturing	Black Board	1



Dr. V.VENKATACHARI, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.

				• Outsiders				
4.	31.01.24	31/1/24	• Need for Cyber Security • History of Cyber Crime	• 1971 Bob Thomas • Creeper	To know the Importance of Cyber Security	Lecturing	Black Board	1
5.	01.02.24	1/2/24	• Cyber Criminals	• Hackers • Threat Actors • Malicious	To understand the Need of Cyber Criminals	Lecturing	Black Board	1
6.	02.02.24	2/2/24	• Classification of Cybercrimes	• DDoS Attacks • Botnets • Cyber stalking	To know the motivation of Cyber Criminals	Lecturing	Power point presentation software	1
7.	05.02.24	5/2/24	• A Global Perspective on Cyber Crimes	• Cyber Security • Cyber Criminals	To understand the Global Perspective of Cyber Crime	Lecturing	Power point presentation software	1
8.	07.02.24	7/2/24	• Cyber Laws • The Indian IT Act	• Data Privacy • Hacking • Identity Theft	To Know about the Cyber Laws in India	Role Play	-	1
9.	08.02.24	8/2/24	• Cybercrime and Punishment.	• Deterrence • Punishment • Protection	To understand the Cyber Crime and its punishment	Seminar	-	1
10.	09.02.24	9/2/24	Content Beyond the Syllabus: SiteLock	• Vulnerability • Web Application Security	To know about the software of Cyber Security	Lecturing	Power point presentation software	1

UNIT -II ATTACKS AND COUNTERMEASURES

11.	12.02.24	14/2/24	• OSWAP	• Security • Application • Technologies	To understand the basic concept of OSWAP	Lecturing	Black Board	1
12.	14.02.24	15/2/24	• Malicious Attack threats • Vulnerabilities	• Objective • Delivery • Concealment	To understand the Process of Malicious Attack threats	Lecturing	Power point presentation software	
13.	15.02.24	16/2/24	• Scope of Cyber Attacks • Security Breach	• Network Security • Application Security • Information Security	To understand the Features of Scope of Cyber Attacks	Lecturing	Black Board	1
14.	16.02.24	19/2/24	• Types Malicious Attacks	• Viruses • Worms • Ransomware • Rootkits	To understand the Malicious Attacks	Lecturing	Smart Board	1
15.	19.02.24	21/2/24	• Malicious Software	• SpyWare • Adware • Trojan Horse	To understand the basics of Malicious Software	Lecturing	Black Board	1
16.	21.02.24	22/2/24	• Common Attack Vectors	• Credential theft • Vulnerability exploits	To know the importance of Attack Vectors	Lecturing	Power point presentation software	1
17.	22.02.24	22/2/24	• Social Engineering Attack • Wireless Network Attack	• Baiting • Scareware • Pretexting • Jamming/ Interference	Learn about the Social Engineering Attack	Lecturing	Black Board	1
18.	23.02.24	23/2/24	• Web	• XSS	To know about the	Group	-	1



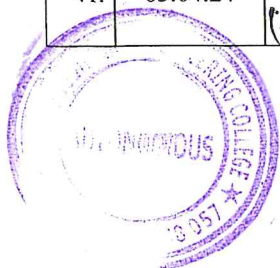
Dr. V. VENKATARAMAN, M.S., M.Tech.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode - 638 057.

			Application attack	<ul style="list-style-type: none"> • CSRF • XXE 	Web Application attack	Discussion		
19.	26.02.24	29/2/24	<ul style="list-style-type: none"> • Attack Tools • Countermeasures 	<ul style="list-style-type: none"> • Physical and Operational Security Countermeasures 	To understand the attack tools	Seminar	-	1
20.	28.02.24	12/2/24	Content Beyond the Syllabus: Countermeasures in IoT Environment	<ul style="list-style-type: none"> • Industrial IoT • Commercial IoT • Healthcare IoT 	To understand the Countermeasures of IoT	Lecturing	Black Board	1
UNIT -III RECONNAISSANCE								
21.	29.02.24	6/3/24	<ul style="list-style-type: none"> • Harvester and Whois • Netcraft • Host 	<ul style="list-style-type: none"> • OSINT • Reconnaissance • Foot Printing 	To understand the basic concept of Harvester and NetCraft	Lecturing	Power point presentation software	1
22.	01.03.24	7/3/24	<ul style="list-style-type: none"> • Extracting Information from DNS • Extracting Information from E-mail Servers 	<ul style="list-style-type: none"> • Zone transfers • Host • NSLookup • Email Servers 	To apply Knowledge of DNS and Email Servers	Lecturing	Power point presentation software	1
23.	04.03.24	8/3/24	<ul style="list-style-type: none"> • Social Engineering Reconnaissance 	<ul style="list-style-type: none"> • Phishing • Spear phishing • Vishing 	To understand about Social Engineering Reconnaissance	Lecturing	Power point presentation software	1
24.	06.03.24	11/3/24	<ul style="list-style-type: none"> • Scanning • Port Scanning 	<ul style="list-style-type: none"> • IDS • OS • Firewall 	To know about Scanning	Lecturing	Smart Board	1
25.	07.03.24	12/3/24	<ul style="list-style-type: none"> • Network Scanning and Vulnerability Scanning 	<ul style="list-style-type: none"> • Data Breaches • Host-based scanning • Network-based scanning 	To know about Network and Vulnerability Scanning	Lecturing	Power point presentation software	1
26.	08.03.24	14/3/24	<ul style="list-style-type: none"> • Scanning Methodology • Sweer Techniques 	<ul style="list-style-type: none"> • Half-open scan • FIN scan • Null Scan 	To know about Challenges of Sweer Techniques	Lecturing	Power point presentation software	1
27.	11.03.24	15/3/24	<ul style="list-style-type: none"> • Nmap Command Switches • SYN • Stealth 	<ul style="list-style-type: none"> • TCP Connect Scans • UDP Scans • Nmap Scripting Engine 	To know the function of Nmap Command Switches	Seminar	-	1
28.	13.03.24	18/3/24	<ul style="list-style-type: none"> • XMAS • NULL • IDLE • FIN Scans 	<ul style="list-style-type: none"> • Null scan • Fin scan • Xmas scan 	To know about XMAS, NULL, IDLE	Peer Learning	-	1
29.	14.03.24	22/3/24	<ul style="list-style-type: none"> • Banner Grabbing • OS Finger printing Techniques 	<ul style="list-style-type: none"> • Active Banner Grabbing • Passive Banner Capture 	To know about Banner Grabbing and OS Finger Print Techniques	Lecturing	Power point presentation software	1
30.	15.03.24	21/3/24	Content Beyond the	<ul style="list-style-type: none"> • Implanted the payload 	To study the working of Cobalt	Lecturing	Power point	1



Dr. V.VENKATACHARI, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode - 638 057.

			Syllabus: Cobalt Strike		Strike		presentation software	
UNIT -IV INTRODUCTION								
31.	18.03.24	22/3/24	• Ethical Hacking Overview	• Website Hacking • Network Hacking • Email Hacking	To understand the Ethical Hacking	Lecturing	Power point presentation software	1
32.	20.03.24	27/3/24	• Role of Security and Penetration Testers	• Opaque box • Semi-opaque box • Transparent box	To understand the Security and Penetration Testers	Lecturing	Smart Board	1
33.	21.03.24	28/3/24	• Penetration • Testing Methodologies	• Operational focus • Channel testing • Trust analysis	To understand the Testing Methodologies	Lecturing	Power point presentation software	1
34.	22.03.24	31/4/24	• Laws of the Land	• Civil law • Criminal law	To understand the Laws of the Land	Lecturing	Power point presentation software	1
35.	25.03.24	4/4/24	• Overview of TCP/IP • The Application Layer	• Shijack • Hunt • Quick Tip	To understand the Overview of TCP/IP	Lecturing	Power point presentation software	1
36.	27.03.24	5/4/24	• The Transport Layer • The Internet Layer	• UDP • UDP Segment • MAC Address	Learn the significance of Transport and Internet Layer	Lecturing	Power point presentation software	1
37.	28.03.24	8/4/24	• IP Addressing • Network and Computer Attacks • Malware	• Malware • Virus • Worm • Botnet	To understand the Network and Computer Attacks	Lecturing	Power point presentation software	1
38.	01.04.24	10/4/24	• Protecting Against Malware Attacks. • Intruder Attacks	• Anti-virus • Anti-spyware software • Keep software updated	Apply the Knowledge of Protecting Against Malware	Seminar	-	1
39.	03.04.24	12/4/24	• Addressing Physical Security	• Deterrence • Physical Barriers • Detection	Implementation of Addressing Physical Security	Video Demonstration	Browser With Video Player	1
40.	04.04.24	15/4/24	Content beyond the syllabus: Invicti	• Scanner • Open source	To know the significance of Invicti Tool	Lecturing	Power point presentation software	1
UNIT - V FOOT PRINTING, RECONNAISSANCE AND SCANNING NETWORKS								
41.	05.04.24	17/4/24	• Foot printing Concepts	• Social Media • Job websites • Google	To know the Concept of Foot printing	Lecturing	PowerPoint presentation software	1

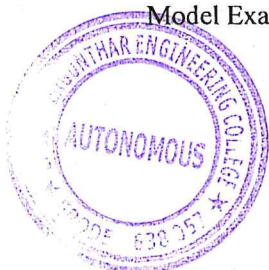


Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.

42.	08.04.24	18/4/24	<ul style="list-style-type: none"> Foot printing through Search Engines 	<ul style="list-style-type: none"> Overview Resources required Initial Setup Task 	Learn the importance of Foot printing through Search Engines	Lecturing	Power point presentation software	1
43.	10.04.24	22/4/24	<ul style="list-style-type: none"> Web Services Social Networking Sites 	<ul style="list-style-type: none"> Active Digital Footprint Passive Digital Footprint 	To know the Social Networking Sites	Lecturing	Power point presentation software	1
44.	12.04.24	24/4/24	<ul style="list-style-type: none"> Website Email Competitive Intelligence 	<ul style="list-style-type: none"> Predictive Intelligence Behavioral 	To understand the Email Competitive Intelligence	Seminar	-	1
45.	15.04.24	25/4/24	<ul style="list-style-type: none"> Foot printing through Social Engineering 	<ul style="list-style-type: none"> Eavesdropping Shoulder Surfing Dumpster Diving 	To know the importance of Foot printing	Lecturing	Power point presentation software	1
46.	17.04.24	26/4/24	<ul style="list-style-type: none"> Foot printing Tools 	<ul style="list-style-type: none"> TheHarvester Maltego SpiderFoot 	To understand the Foot printing Tools	Lecturing	Power point presentation software	1
47.	18.04.24	21/5/24	<ul style="list-style-type: none"> Network Scanning Concepts Port-Scanning Tools 	<ul style="list-style-type: none"> Nmap UnicornsCan Angry IP Scan 	To know the basics of Foot printing Tools	Lecturing	Power point presentation software	1
48.	19.04.24	31/5/24	<ul style="list-style-type: none"> Scanning Techniques 	<ul style="list-style-type: none"> ICMP Scanning Ping Sweep ICMP Echo Scanning 	To aware of the Scanning Techniques	Lecturing	Power point presentation software	1
49.	22.04.24	7/5/24	<ul style="list-style-type: none"> Scanning Beyond IDS and Firewall 	<ul style="list-style-type: none"> Packet Fragmentation: Source Routing IP Address Decoy 	To understand the importance of IDS and Firewall	Lecturing	Power point presentation software	1
50.	24.04.24	7/5/24	<ul style="list-style-type: none"> Content beyond the Syllabus: VPN Foot printing 	<ul style="list-style-type: none"> VPN VoIP IP 	To analyze the VPN Foot printing	Lecturing	Power point presentation software	1
Total no. of Hours								50
Total hours prescribed in the syllabus								45

TENTATIVE DATES OF EVENTS:

Reopening Date	: 22.01.2024
Last Working Day	: 22.05.2024
Continuous Assessment Test I	: 21.02.2024 to 29.02.2024
Continuous Assessment Test II	: 20.03.2024 to 28.03.2024
Continuous Assessment Test III	: 17.04.2024 to 25.04.2024
Model Examination	: 06.05.2024 to 14.05.2024



Dr. V.VENKATACHANDAN, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode - 638 052.

TEXT BOOKS:

1. Anand Shinde, "Introduction to Cyber Security Guide to the World of Cyber Security", Notion Press, 2021.
2. Michael T. Simpson, Kent Backman, and James E. Corley, Hands-On Ethical Hacking and Network Defense, Course Technology, Delmar Cengage Learning, 2010.


REFERENCES:

1. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publishers, 2011
2. The Basics of Hacking and Penetration Testing - Patrick Engebretson, SYNGRESS, Elsevier, 2013.

WEB LEARNING RESOURCES:

1. <https://www.youtube.com/watch?v=ULGILG-ZhO0>
2. <https://www.youtube.com/watch?v=DLiP7y51OAQ>
3. <https://nitttrc.edu.in/nptel/courses/video/106106178/L13>
4. <https://www.youtube.com/watch?v=t8nwQ6At0CU>
5. <https://www.youtube.com/watch?v=jRyexbPCnNo>


COURSE COORDINATOR


HOD/M.Tech. CSE


PRINCIPAL




Dr. V. VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode - 638 057.

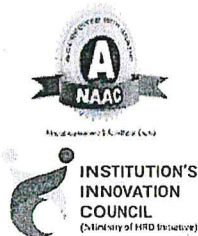


ERODE SENGUNTHAR

ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai,
Accredited by National Board of Accreditation (NBA), New Delhi &
National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade
PERUNDURAI -638 057, TAMILNADU, INDIA.



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

Innovative Teaching Process

2023-2024 EVEN SEMESTER

1. Name of subjects with course code : 21CSX04 Cyber Security and Ethical Hacking
2. Class/Year/Branch : M.Tech CSE (5 Years Integrated) / III
3. Name of course Co-ordinator : Mr. A.Rajesh
4. Date & Hour : 07.02.2024 & 5th hour
5. Title of Innovative teaching learning process : Role Play
6. Topic of the Class : Cyber Crime and Punishment
7. Objective : The main objective of this session is
To learn about Cyber Crime and
punishment
8. Students name list-Batch wise:

S.No.	Register Number	Name of the Student
1	730421553002	ABINESH M
2	730421553003	ARUNPRASATH B
3	730421553004	ASWIN V
4	730421553005	BHARANIDHARAN C
5	730421553007	DHILIP KUMAR S
6	730421553008	DOHITH VIGNESHWAR SP
7	730421553009	GOKUL KRISHNAN B
8	730421553010	GUGHAN S
9	730421553012	IMMANUEL S
10	730421553013	JAMES CHRUSTOBAR P
11	730421553014	JEEVA P
12	730421553015	JEEVITHAA S



Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.



ERODE SENGUNTHAR

ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai,
Accredited by National Board of Accreditation (NBA), New Delhi &
National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade
PERUNDURAI -638 057, TAMILNADU, INDIA.



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

Innovative Teaching Process

2023-2024 EVEN SEMESTER

16	730421553019	KANNAN G
17	730421553020	KIRANPRASATH P
18	730421553021	KRISHNAN G
19	730421553022	LEVIN EFRON N
20	730421553023	LOGESHWARAN B
21	730421553024	MOHANA PRIYA S
22	730421553025	NAHARAJAN M
23	730421553026	NIVETHA M
24	730421553027	PARAMESHWARAN M
25	730421553028	PRASANNA S
26	730421553029	PRAVEEN RAJ GV
27	730421553030	RISHIKESH V
28	730421553031	ROHEETH B
29	730421553032	SANJAY K
30	730421553033	SIVAKUMAR.R
31	730421553034	SRIMARIAPPAN S
32	730421553035	SUBAGANESH S
33	730421553036	SUJITHKUMAR K
34	730421553037	SURIYA KUMAR D
35	730421553038	SURIYAPRASATH B
36	730421553039	SWAPNA S
37	730421553040	VENISHRAM M
38	730421553041	VIGNESWARAN S
39	730421553042	VIKRAM P
40	730421553043	VINITHA K
41	730421553044	YOGESH K
42	730421553045	YUVAPRABHA V



Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.



ERODE SENGUNTHAR ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai,
Accredited by National Board of Accreditation (NBA), New Delhi &
National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade
PERUNDURAI -638 057, TAMILNADU, INDIA.




DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

Innovative Teaching Process

9.Geo-tagged Photos:





Course Coordinator


HoD


Principal




Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.



ERODE SENGUNTHAR

ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai,
Accredited by National Board of Accreditation (NBA), New Delhi &
National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade
PERUNDURAI -638 057, TAMILNADU, INDIA.



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

Innovative Teaching Process

2023-2024 EVEN SEMESTER

1. Name of subjects with course code : 21CSX04 Cyber Security and Ethical Hacking
2. Class/Year/Branch : M.Tech CSE (5 Years Integrated) / III
3. Name of course Co-ordinator : Mr. A.Rajesh
4. Date & Hour : 23.02.2024 & 5th hour
(Map with concern subject logbook)
5. Title of Innovative teaching learning process : Group Discussion
6. Topic of the Class : Web Application Attack
7. Objective : The main objective of this session is to learn about Web Application Attack
8. Students name list-Batch wise:

S.No.	Register Number	Name of the Student
1	730421553002	ABINESH M
2	730421553003	ARUNPRASATH B
3	730421553004	ASWIN V
4	730421553005	BHARANIDHARAN C
5	730421553007	DHILIP KUMAR S
6	730421553008	DOHITH VIGNESHWAR SP
7	730421553009	GOKUL KRISHNAN B
8	730421553010	GUGHAN S
9	730421553012	IMMANUEL S
10	730421553013	JAMES CHRUSTOBAR P
11	730421553014	JEEVA P
12	730421553015	JEEVITHAA S
13	730421553016	JOHNINBARAJ M
14	730421553017	KALPANA G



Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College
(Autonomous)



ERODE SENGUNTHAR

ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai,
Accredited by National Board of Accreditation (NBA), New Delhi &
National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade
PERUNDURAI -638 057, TAMILNADU, INDIA.



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

Innovative Teaching Process

2023-2024 EVEN SEMESTER

15	730421553018	KANCHANA SV
16	730421553019	KANNAN G
17	730421553020	KIRANPRASATH P
18	730421553021	KRISHNAN G
19	730421553022	LEVIN EFRON N
20	730421553023	LOGESHWARAN B
21	730421553024	MOHANA PRIYA S
22	730421553025	NAHARAJAN M
23	730421553026	NIVETHA M
24	730421553027	PARAMESHWARAN M
25	730421553028	PRASANNA S
26	730421553029	PRAVEEN RAJ GV
27	730421553030	RISHIKESH V
28	730421553031	ROHEETH B
29	730421553032	SANJAY K
30	730421553033	SIVAKUMAR.R
31	730421553034	SRIMARIAPPAN S
32	730421553035	SUBAGANESH S
33	730421553036	SUJITHKUMAR K
34	730421553037	SURIYA KUMAR D
35	730421553038	SURIYAPRASATH B
36	730421553039	SWAPNA S
37	730421553040	VENISHRAM M
38	730421553041	VIGNESWARAN S
39	730421553042	VIKRAM P
40	730421553043	VINITHA K
41	730421553044	YOGESH K
42	730421553045	YUVAPRABHA V



Dr. V.VENKATACHANDRAN, M.Sc., M.Tech., Ph.D.,
Professor,
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.



ERODE SENGUNTHAR ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai,
Accredited by National Board of Accreditation (NBA), New Delhi &
National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade
PERUNDURAI -638 057, TAMILNADU, INDIA.

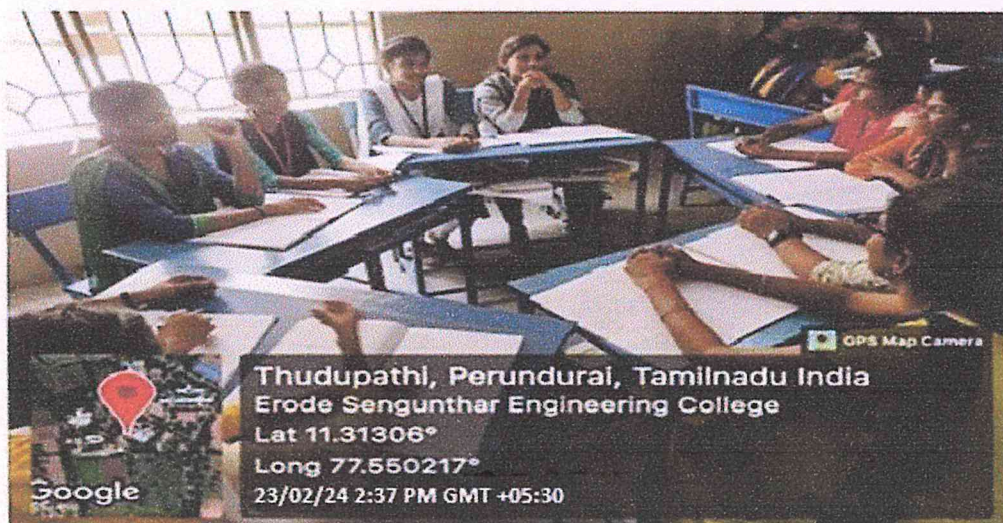
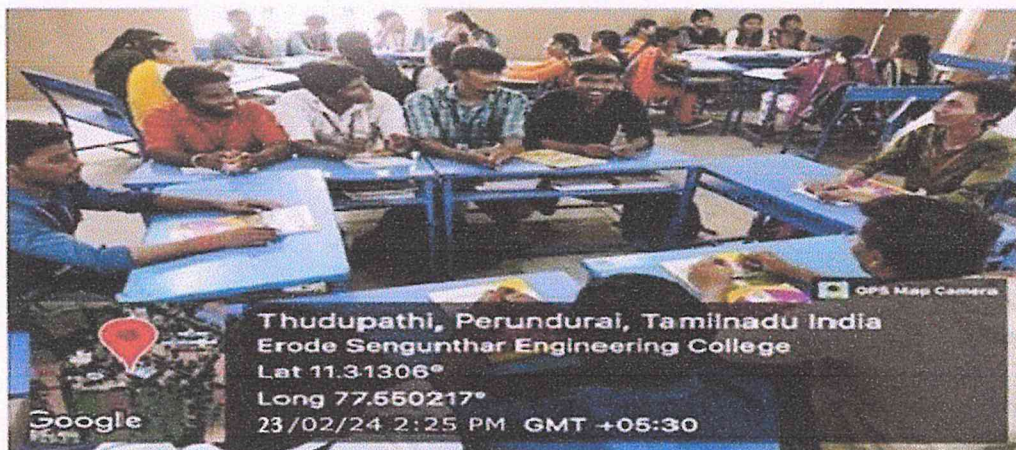


DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

Innovative Teaching Process

2023-2024 EVEN SEMESTER

9. Geo-tagged Photo:



Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College.
(Autonomous)
Thudupathi, Perundurai



ERODE SENGUNTHAR

ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai,
Accredited by National Board of Accreditation (NBA), New Delhi &
National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade

PERUNDURAI -638 057, TAMILNADU, INDIA.

DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

(5 YEARS INTEGRATED)

Innovative Teaching Process

2023-2024 EVEN SEMESTER



1. Name of subjects with course code :21CSX04 Cyber Security and Ethical Hacking
2. Class/Year/Branch : M.Tech CSE (5 Years Integrated) / III
3. Name of course Co-ordinator :Mr. A.Rajesh
4. Date & Hour : 18.03.2024 & 1st hour
(Map with concern subject logbook)
5. Title of Innovative teaching learning process : Peer Learning
6. Topic of the Class : XMAS,NULL,IDLE and FIN Scans
7. Objective :The main objective of this session is to learn about XMAS, NULL, IDLE and FIN Scans by Peer Learning

8. Students name list-Batch wise:

S.No.	Register Number	Name of the Student
1	730421553002	ABINESH M
2	730421553003	ARUNPRASATH B
3	730421553004	ASWIN V
4	730421553005	BHARANIDHARAN C
5	730421553007	DHILIP KUMAR S
6	730421553008	DOHITH VIGNESHWAR SP
7	730421553009	GOKUL KRISHNAN B
8	730421553010	GUGHAN S
9	730421553012	IMMANUEL S
10	730421553013	JAMES CHRUSTOBAR P
11	730421553014	JEEVA P
12	730421553015	JEEVITHAA S



Dr. V.VENKATACHALAM, M.S., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College
(Autonomous)
Thudupathi, Perundurai, Tamil Nadu - 638 057



ERODE SENGUNTHAR

ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai,
Accredited by National Board of Accreditation (NBA), New Delhi &
National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade

PERUNDURAI -638 057, TAMILNADU, INDIA.

DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

(5 YEARS INTEGRATED)

Innovative Teaching Process

2023-2024 EVEN SEMESTER



13	730421553016	JOHNINBARAJ M
14	730421553017	KALPANA G
15	730421553018	KANCHANA SV
16	730421553019	KANNAN G
17	730421553020	KIRANPRASATH P
18	730421553021	KRISHNAN G
19	730421553022	LEVIN EFRON N
20	730421553023	LOGESHWARAN B
21	730421553024	MOHANA PRIYA S
22	730421553025	NAHARAJAN M
23	730421553026	NIVETHA M
24	730421553027	PARAMESHWARAN M
25	730421553028	PRASANNA S
26	730421553029	PRAVEEN RAJ GV
27	730421553030	RISHIKESH V
28	730421553031	ROHEETH B
29	730421553032	SANJAY K
30	730421553033	SIVAKUMAR.R
31	730421553034	SRIMARIAPPAN S
32	730421553035	SUBAGANESH S
33	730421553036	SUJITHKUMAR K
34	730421553037	SURIYA KUMAR D
35	730421553038	SURIYAPRASATH B
36	730421553039	SWAPNA S
37	730421553040	VENISHRAM M
38	730421553041	VIGNESWARAN S
39	730421553042	VIKRAM P
40	730421553043	VINITHA K
41	730421553044	YOGESH K
42	730421553045	YUVAPRABHA V



Dr. V. VENKATARAMAN, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode - 638 057.



ERODE SENGUNTHAR ENGINEERING COLLEGE

(An Autonomous Institution)

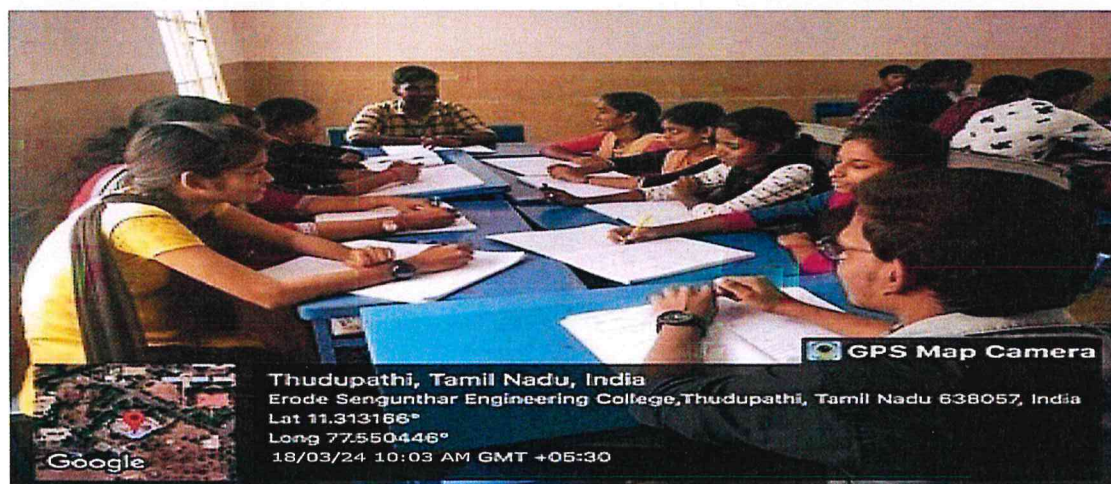
Approved by AICTE, New Delhi, Permanently Affiliated to Anna University- Chennai,
Accredited by National Board of Accreditation (NBA), New Delhi &
National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade
PERUNDURAI -638 057, TAMILNADU, INDIA.



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

Innovative Teaching Process

9. Geo-tagged Photos:




Course Coordinator


HoD


Principal




Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.

PARTICULARS OF PORTIONS COVERED

Semester : VI Branch/Class : M.Tech Course : CSE

Date	Time	Topic	Sign.	Remarks
		UNIT I		
		INTRODUCTION		
22/1/24	1	course orientation	h	
		PPT		
24/1/24	5	cyber Security	h	
		History of Internet and		
		Impact of Internet		
27/1/24	1	CIA Triad, Reason	h	g
		for cyber crime		
31/1/24	5	Need for cyber	h	
		Security		
1/2/24	1	cyber criminals	h	
2/2/24	2	classification of	h	
		cyber crimes		
5/2/24	1	A global Perspective	h	
		on cyber crimes		
7/2/24	5	cyber Laws and	h	
		Indian IT Act		
8/2/24	5	cyber crime and	h	
		Punishment		
9/2/24	6	Content beyond	h	
		the syllabus:		
		site Lock		
		UNIT II		
		ATTACKS AND COUNTER MEASURES		
14/2/24	5	Introduction of OSWAP	h	
15/2/24	5	malicious attacks	h	
		threats, vulnerabilities		



Dr. V. VENKATESH, M.A.M., M.S., M.Tech
 PRINCIPAL
 Erode Sengunthar Engineering Co
 (Autonomous)
 Thudupathi, Perundurai, Erode - 63

PARTICULARS OF PORTIONS COVERED

Semester : VI

Branch/Class : M.Tech Course : CSE

Date	Time	Topic	Sign.	Remarks
16/2/24	6	Scope of cyber attacks	h	
		Security breach		
17/2/24	1	Types of malicious attacks	h	
21/2/24	5	Malicious Software	h	
22/2/24	5	Social Engineering of wireless network	h	
23/2/24	6	web application attacks	h	
28/2/24	5	Attack tools of cybercriminals	h	
29/2/24	5	Content Regulation System	h	
		Issue in IoT		
12/2/24	1	Common vector attacks	h	
		UNIT III		
		RECONNAISSANCE		
11/3/24	1	CAT I	h	
11/3/24	2	CAT II	h	
6/3/24	5	Harvester, who is, Notoratt	h	
7/3/24	5	Extracting information from DNS and Email server	h	
8/3/24	6	Social Engineering Reconnaissance	h	
11/3/24	1	Scanning, Port Scanning	h	
13/3/24	5	Network and vulnerability Scanning	h	
14/3/24	5	Scanning Methodology	h	
		and sweet to snippets		
15/3/24	6	Xmap Command Scanning	h	
		SYN, Stealth		
18/3/24	1	XMAS, NULL, IDLE	h	
		FIN Scans		



Dr. V. VENIKATA SURESH, M.S., M.Tech., Ph.D.,
 Associate Professor
 Erode Sengunther Engineering College,
 Thudupathi, Perundurai, Erode - 638 057.

PARTICULARS OF PORTIONS COVERED

Semester: VI Branch/Class: M.Tech Course: CSE

Date	Time	Topic	Sign.	Remarks
20/3/24	5	Banner Grabbing and as Fingerprinting Techniques	h	
21/3/24	5	Content Regulate symbols cobalt strike	h	
		UNIT IV		
		INTRODUCTION		
22/3/24	6	Ethical Hacking Overview		
27/3/24	5	Role of Security and Penetration Testers		
28/3/24	5	Penetration and Testing methodologies		g
01/4/24	1	CAT II	h	
01/4/24	2	CAT II	h	
03/4/24	5	Law of the Land	h	
04/4/24	5	Overview of TCP/IP and The Application Layer	h	
05/4/24	6	Transport and Internet Layer	h	
08/4/24	1	IP Addressing, Network and Complex Attacks, Malware	h	
10/4/24	5	Protecting Against Malware Attacks, Intruders Attacks	h	
12/4/24	6	Addressing Physical Security	h	




Dr. V. VENKATACHANDRAN, M.Tech, M.Sc.
 Associate Professor
 Erode Sengunthar Engineering College
 (Autonomous)
 Thudupathi, Perundurai, Tamil Nadu - 638053.

PARTICULARS OF PORTIONS COVERED

Semester : VI

Branch/Class : M.Tech Course : QSE

Date	Time	Topic	Sign.	Remarks
15/4/24	1	Content Based to Syllabus: Trimester UNIT IV	h	
F00T		PRINCIPLES, RECOGNITION AND SCANNING NETWORKS		
17/4/24	5	Foot Printing Groups	h	
18/4/24	5	Foot printing through social English	h	
22/4/24	1	web services & Networking	h	
24/4/24	5	website & Email Computer network	h	
25/4/24	5	Foot printing through social English	h	
26/4/24	6	Foot Printing Tools	h	2
21/5/24	5	Network Scanning concepts Foot scanning concept	h	
3/5/24	6	Scanning Techniques	h	
6/5/24	1	CAT III	h	
6/5/24	2	CAT IV	h	2
HISTU	1	Scanning Beyond IDS at Network	h	
HISTU	2	Content Based to Syllabus - vpon Foot Printing	h	
HISTU	CT4	Model Exam	h	
		System Graph		
				
		19/5/24		



Dr. V. VENKATACHARI, M.S., M. Tech. Ph.D.
 PRINCIPAL
 Erode Senguntha Engineering College,
 (Autonomous)
 Thudupathi, Perundurai, Tamil Nadu - 625 002



ERODE SENGUNTHAR ENGINEERING COLLEGE (AUTONOMOUS)

Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai &
Accredited by National Board of Accreditation (NBA), New Delhi
THUDUPATHI, ERODE – 638 057.



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING (5 YEARS INTEGRATED) CONTENT BEYOND THE SYLLABUS

UNIT 1 SITELOCK

What is SiteLock?

SiteLock is a cloud-based security tool that scans your website for malware and vulnerabilities. SiteLock not only detects threats, but can also fix problems or security risks it encounters on your web space. **SiteLock** is a well-known company in the field of cybersecurity that provides a range of security services for websites. It specializes in protecting websites from online threats such as malware, hacking, and various types of cyberattacks. SiteLock's tools are designed to detect, prevent, and resolve security issues, and they often cater to small businesses, enterprises, and web hosting providers.

Here's a breakdown of SiteLock's key features and services:

1. Website Malware Removal

SiteLock offers malware detection and removal services to eliminate harmful software from your website. This includes scanning for viruses, spyware, and other malicious code that can infect a website, often leading to data theft, website downtime, or loss of credibility.

2. Website Vulnerability Scanning

SiteLock runs regular vulnerability scans to identify weaknesses in a website's code, plugins, or server configuration. These scans help website owners address issues before attackers can exploit them.

3. Website Firewall (WAF)

SiteLock provides a Web Application Firewall (WAF) that monitors and filters incoming traffic to the website, blocking malicious requests such as SQL injection, cross-site scripting (XSS), and other common attack vectors. The WAF acts as a shield against cyberattacks, ensuring that only legitimate traffic reaches your site.



Dr. V. VENKATACHANDRAN, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode - 638 057.

4. DDoS Protection

SiteLock offers Distributed Denial of Service (DDoS) attack protection. DDoS attacks overwhelm a website with traffic, making it unavailable to users. SiteLock's DDoS mitigation helps ensure that your site remains operational even under attack.

5. SSL Certificates

SSL (Secure Sockets Layer) certificates are used to encrypt communication between users' browsers and websites, ensuring secure data transmission. SiteLock provides SSL certificates to improve website security and help websites earn users' trust.

6. Automated Backups

Regular backups are crucial for maintaining the integrity of a website. SiteLock offers automated backup solutions to ensure that your website's data can be restored quickly in case of a security breach or technical failure.

7. Website Monitoring and Alerts

SiteLock continuously monitors websites for signs of malicious activity or downtime. Website owners are notified immediately if any issues are detected, allowing for swift action to prevent or mitigate potential damage.

8. PCI Compliance

SiteLock helps businesses comply with the Payment Card Industry Data Security Standard (PCI DSS) by offering tools and services that ensure sensitive customer payment information is securely handled on their websites.

9. SEO Spam Monitoring and Removal

Hackers sometimes inject spammy content into websites, leading to blacklisting by search engines. SiteLock monitors websites for such issues and removes SEO spam to protect the website's search engine rankings and online reputation.

10. Daily Security Scans and Reports

SiteLock offers daily scans to identify vulnerabilities or malware on a website, ensuring it remains secure. Users receive detailed reports outlining any issues found and steps to resolve them.

11. Security Badge

SiteLock provides a security badge that website owners can display to show visitors their site is secure and protected from threats. This badge helps increase trust and confidence among users.

12. SiteLock SMART SiteLock's SMART service combines all of its key security features in one package, including malware removal, vulnerability scanning, and a web application firewall, offering comprehensive protection for websites.



**Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.**

Benefits of Using SiteLock:

- **Proactive Security:** Continuous monitoring and protection against emerging threats.
- **Ease of Use:** Automated tools and easy integration with websites.
- **Reputation Protection:** Helps maintain user trust and prevent website blacklisting.
- **Compliance:** Helps meet security and privacy standards, including PCI DSS.
- **Comprehensive Protection:** Includes malware removal, vulnerability scanning, backup, and more.

Who Should Use SiteLock?

- **Small to Medium-Sized Businesses:** SiteLock provides affordable and scalable security solutions that are easy to use for businesses without dedicated IT security teams.
- **Web Hosting Providers:** Many hosting companies partner with SiteLock to offer integrated website security solutions to their customers.
- **E-commerce Sites:** Websites that handle sensitive customer data or financial transactions benefit greatly from SiteLock's compliance, DDoS protection, and malware removal features.

SiteLock's Role in Web Application Security Standards

Compliance and Legal Frameworks:

- SiteLock plays an integral role in helping websites comply with industry standards such as PCI DSS (Payment Card Industry Data Security Standard), GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and other frameworks by offering tools and services that ensure a website adheres to data privacy and security requirements.
- SiteLock's tools ensure that sensitive data, such as credit card information, is encrypted and that security logs are available for auditing purposes.

Integration with DevOps (DevSecOps):

- **SiteLock for DevSecOps:** Modern development cycles follow the DevSecOps model, where security is integrated into every phase of the development lifecycle. SiteLock integrates with Continuous Integration/Continuous Deployment (CI/CD) pipelines, providing real-time security scans as code is pushed or deployed, helping developers identify vulnerabilities early in the development process.
- Automated security scans and testing help DevOps teams identify and fix vulnerabilities before they become a threat.



Dr. [Name], M.Sc., M.Tech., Ph.D.,
Erode Engineering College,
Thudupathi, Perundurai, Erode - 638 057.



ERODE SENGUNTHAR ENGINEERING COLLEGE (AUTONOMOUS)

Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai &
Accredited by National Board of Accreditation (NBA), New Delhi
THUDUPATHI, ERODE – 638 057.



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING (5 YEARS INTEGRATED)

CONTENT BEYOND THE SYLLABUS

UNIT 2

COUNTER MEASUREMENTS IN IOT ENVIRONMENT

IoT (Internet of Things) environments present unique challenges due to the sheer number of connected devices, their varied capabilities, and often weak security mechanisms. IoT devices are becoming integral to industries such as healthcare, manufacturing, smart homes, and transportation. However, they also introduce significant attack vectors for cybercriminals. Given these risks, **countermeasures** in the IoT environment are essential for mitigating vulnerabilities and securing IoT ecosystems.

1. Device Authentication and Authorization

Countermeasure: Strong Authentication Mechanisms

- **Secure Authentication:** Devices should be authenticated using secure methods (e.g., mutual TLS (Transport Layer Security) or public key infrastructure (PKI)) to ensure that only authorized devices are connected to the network.
- **Multi-Factor Authentication (MFA):** For sensitive IoT systems (e.g., healthcare, industrial), implement multi-factor authentication to strengthen access controls for both users and devices.
- **Device Identity Management:** Each IoT device should have a unique, non-reusable identity (using digital certificates or hardware security modules (HSMs)) to ensure that unauthorized devices cannot join the network.



Dr. V. VENKATACHALAM, M.S., M.Tech., Ph.D.,
Erode Sengunthar Engineering College
Thudupathi

2. Encryption and Data Protection

Countermeasure: Encryption of Data at Rest and in Transit

- End-to-End Encryption: All communication between IoT devices, servers, and cloud platforms should be encrypted using strong protocols (e.g., AES (Advanced Encryption Standard) for data at rest and TLS/SSL for data in transit).
- Key Management: Securely manage encryption keys to prevent unauthorized access. Use hardware security modules (HSMs) or cloud key management services to protect keys.
- Data Minimization: Avoid collecting unnecessary personal or sensitive data. If storing personal data, ensure it is anonymized or pseudonymized where possible.

3. Secure Network Architecture

Countermeasure: Segmentation and Isolation of Networks

- Network Segmentation: Use network segmentation to isolate IoT devices from other critical systems, especially in cases where the devices are vulnerable or untrusted. For example, IoT devices should be placed in a dedicated IoT VLAN (Virtual Local Area Network) or a separate network from other enterprise assets.
- Zero Trust Architecture: Implement a Zero Trust security model, which assumes that no device or user should be trusted by default, whether inside or outside the network. This approach requires continuous verification and least-privilege access controls.
- Firewalls and Intrusion Detection Systems (IDS): Deploy firewalls to monitor and restrict traffic to/from IoT devices. Additionally, Intrusion Detection Systems (IDS) can detect abnormal network traffic patterns that may indicate an attack.

4. Firmware and Software Updates

Countermeasure: Regular Patching and Firmware Updates

- Automatic Updates: IoT devices should support automatic or over-the-air (OTA) updates for both device firmware and software. This ensures that devices are protected from known vulnerabilities and that security patches are applied quickly.
- Patch Management: Establish a patch management process that includes verifying the authenticity and integrity of firmware updates to prevent attackers from installing malicious firmware.



Dr. V.VENKATACHALAM, M.S., M.Tech.,
PRINCIPAL
Erode Sengunthar Engineering College
(Autonomous)
Thudupathi, Perundurai, Erode - 638 001

5. Device and Network Monitoring

Countermeasure: Continuous Monitoring and Anomaly Detection

- Behavioral Monitoring: Use anomaly detection systems to monitor device behavior and identify irregular activity, such as unexpected data transmission or unauthorized access attempts. These systems often use machine learning (ML) and artificial intelligence (AI) to identify threats in real-time.
- Centralized Security Information: Implement a centralized Security Information and Event Management (SIEM) system to aggregate logs from IoT devices and network infrastructure, enabling effective monitoring and incident response.
- Real-Time Alerts: Set up automated alerts for suspicious activity (e.g., large data transfers, access from unknown devices, or abnormal device interactions).

6. Physical Security

Countermeasure: Securing Devices from Physical Tampering

- Tamper-Proof Devices: Ensure that IoT devices have tamper-proof or tamper-evident designs, such as sealed enclosures or secure boot mechanisms, which prevent attackers from physically altering the device or its software.
- Device Location and Access Control: For IoT devices in critical infrastructure or industrial settings, limit physical access to authorized personnel only. Implement strict access control policies to avoid unauthorized tampering.

7. Access Control and Least Privilege

Countermeasure: Role-Based Access Control (RBAC) and Least Privilege

- Role-Based Access Control (RBAC): Implement RBAC to define specific roles and permissions for devices, users, and administrators. This minimizes unnecessary access and limits potential damage from compromised accounts.
- Least Privilege Principle: Apply the principle of least privilege to IoT devices and users by ensuring they have only the permissions required to perform their tasks and no more. This helps prevent lateral movement in case of a breach.



Dr. V.VENKATACHANDAN, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College
(Autonomous)
Thudupathi, Perundurai, Dt. Je. 625 012



ERODE SENGUNTHAR ENGINEERING COLLEGE (AUTONOMOUS)



Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai &
Accredited by National Board of Accreditation (NBA), New Delhi
THUDUPATHI, ERODE - 638 057.



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING (5 YEARS INTEGRATED)

CONTENT BEYOND THE SYLLABUS

UNIT 3

COBALT STRIKE

Cobalt Strike is a well-known and sophisticated penetration testing and post-exploitation tool widely used in the cybersecurity field. While it was originally designed for legitimate use by security professionals to simulate real-world cyberattacks and test the resilience of networks, it has also become notorious for its adoption by cybercriminals and advanced persistent threat (APT) groups for malicious purposes.

Here's a comprehensive breakdown of **Cobalt Strike**, its legitimate uses, malicious uses, key features, and how organizations can defend against its exploitation:

Overview of Cobalt Strike

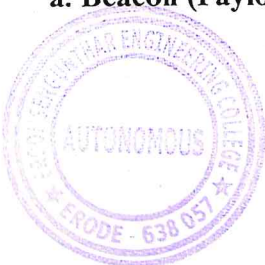
Cobalt Strike was developed by Raphael Mudge and initially marketed as a legitimate tool for red team exercises (simulated cyberattacks to assess the security posture of an organization). It allows security professionals to emulate real-world adversaries by mimicking the tactics, techniques, and procedures (TTPs) commonly used by cybercriminals, state-sponsored hackers, and APT groups.

However, its extensive features also make it a prime tool for cybercriminals and threat actors looking to carry out cyberattacks. The tool's ability to compromise networks, establish persistent access, and escalate privileges makes it highly effective for malicious actors looking to infiltrate systems, steal sensitive information, or disrupt operations.

Key Features of Cobalt Strike

Cobalt Strike is packed with various features that enhance its versatility in penetration testing and cyberattacks. Some of its core capabilities include:

a. Beacon (Payload)



Dr. V. VENKATACHALAN, M.S., M.Tech., Ph.D.
PRINCIPAL
Erode Sengunthar Engineering College
(Autonomous)
Thudupathi, Perambalur, Erode - 638 057

- Beacon is the core payload of Cobalt Strike, used to maintain access to compromised systems. It communicates with a remote server (called a C2 (Command and Control) server) to receive instructions.
- Beacon can use a variety of communication channels, including HTTP, HTTPS, DNS, and SMB, to evade detection and make it difficult for defenders to block the communication.
- It is highly configurable, allowing attackers to adjust the frequency and type of communication (e.g., timing of beacons, data exfiltration, and remote shell access).

b. Post-Exploitation Capabilities

- **Privilege Escalation:** Cobalt Strike supports privilege escalation techniques that allow attackers to gain higher levels of access on compromised systems.
- **Credential Dumping:** It can extract credentials from memory, such as those stored in LSASS (Local Security Authority Subsystem Service) and other sensitive locations, allowing attackers to move laterally in the network.
- **Persistence:** Attackers can maintain a persistent foothold by establishing scheduled tasks, backdoors, or modifying system configurations to ensure access is maintained even after reboots.

c. Lateral Movement

- **SMB/WinRM Exploitation:** Cobalt Strike supports lateral movement via SMB and Windows Remote Management (WinRM), allowing attackers to propagate across internal networks.
- **Credential Dumping and Pass-the-Hash:** The tool can dump user credentials and use Pass-the-Hash (PtH) or Pass-the-Ticket (PtT) attacks to move laterally across networked systems without needing plaintext passwords.

d. Social Engineering and Phishing

- **Phishing:** Cobalt Strike allows red teams to simulate phishing attacks by crafting malicious emails, links, and attachments that can exploit vulnerabilities in human behavior to deliver payloads.
- **Web Shells:** It enables the creation of web shells on compromised web servers, which can be used to gain control over web applications or backend systems.



Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.
PRINCIPAL
Erode Sengunthar Engineering College
(Autonomous)
Thudupathi, Perundurai, Erode - 638 057

e. Command and Control (C2)

- **Cobalt Strike's C2 infrastructure** allows for remote control of compromised systems. This can be done using a variety of protocols and communication methods, making it harder for defenders to identify malicious traffic.
- **Malleable C2:** One of Cobalt Strike's unique features is its Malleable C2 profiles. This allows the attacker to customize the communication patterns between the beacon and the C2 server, making it easier to evade detection by bypassing security controls like firewalls, IDS/IPS, and endpoint security systems.

f. Evading Detection

- **Anti-Detection Techniques:** Cobalt Strike supports several techniques for evading detection, including:
 - Obfuscating payloads to evade signature-based detection systems.
 - Bypassing endpoint security using techniques like living off the land, where attackers leverage native system tools to perform actions (e.g., using PowerShell or Windows Management Instrumentation (WMI)).
 - Injecting malicious code into legitimate processes, making it harder for antivirus software to flag malicious activity.

3. Legitimate Use of Cobalt Strike

When used for legitimate purposes, Cobalt Strike is a powerful tool for:

- **Red Teaming:** Security professionals can use Cobalt Strike to simulate real-world attacks, test defenses, and improve incident response capabilities.
- **Penetration Testing:** Organizations hire ethical hackers to conduct controlled penetration tests. Cobalt Strike helps identify vulnerabilities, test defense mechanisms, and improve overall security posture.
- **Security Training:** Many cybersecurity professionals use Cobalt Strike in simulated attack environments to understand adversarial tactics and improve defensive skills.

4. Malicious Use of Cobalt Strike

Despite its legitimate use in cybersecurity, Cobalt Strike has become a popular tool for cybercriminals, hackers, and APT groups due to its powerful post-exploitation capabilities. Some examples of its malicious use include:



Dr. V. VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode - 638 037.

- **Ransomware Attacks:** Cybercriminals use Cobalt Strike to infiltrate networks, escalate privileges, move laterally, and deploy ransomware, leading to widespread data encryption and demanding ransoms.
- **Data Theft:** Cobalt Strike is used to extract sensitive data, including financial records, intellectual property, and customer information, which is then exfiltrated to the attacker's remote servers.
- **Advanced Persistent Threats (APT):** Nation-state actors and advanced cybercriminal organizations often use Cobalt Strike as part of long-term campaigns to maintain undetected access to target networks. This allows them to exfiltrate data, monitor communications, or disrupt critical infrastructure.
- **Botnet Creation:** Cybercriminals also use Cobalt Strike to infect multiple systems, creating large botnets that can be used for further attacks like Distributed Denial-of-Service (DDoS) attacks.

5. Detecting and Defending Against Cobalt Strike

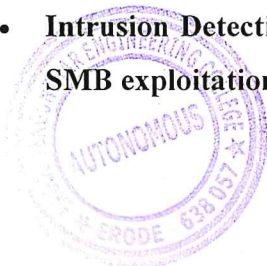
Given its dual-use nature, Cobalt Strike is a significant threat when used maliciously. To defend against it, organizations can implement the following countermeasures:

a. Endpoint Detection and Response (EDR)

- **Monitor for Indicators of Compromise (IOCs):** Implement EDR systems to detect the presence of Cobalt Strike beacons by looking for known IOCs (e.g., Cobalt Strike-related file names, registry entries, and network traffic patterns).
- **Behavioral Analytics:** Use machine learning or anomaly-based detection systems that can identify unusual patterns of activity typically associated with Cobalt Strike's exploitation, such as abnormal network communication, privilege escalation, or lateral movement.

b. Network Detection and Prevention

- **Monitor C2 Traffic:** Set up network monitoring tools to detect unusual C2 traffic. Given that Cobalt Strike uses malleable C2 profiles, network traffic can appear normal, so it's essential to look for patterns such as unusual beaconing activity or unexpected protocols.
- **Intrusion Detection Systems (IDS):** Use IDS/IPS to detect common attack vectors like SMB exploitation, DNS tunneling, and HTTP-based C2 communications.



Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perambalur, Tamil Nadu - 638 057.

c. Segmentation and Least Privilege

- **Network Segmentation:** Implement strict **network segmentation** to isolate critical systems and sensitive data from IoT devices, endpoints, and less secure areas of the network. This limits lateral movement once a breach occurs.
- **Least Privilege Access:** Ensure that users and systems operate with the least amount of privilege necessary. This limits the scope of damage in case of an attack, preventing attackers from escalating privileges.

d. Dealing with Phishing and Social Engineering

- **User Training:** Educate employees about phishing, social engineering, and safe web practices to prevent initial compromise from happening via Cobalt Strike's phishing capabilities.
- **Email Filtering:** Implement robust email filtering solutions to block phishing emails and malicious attachments before they reach end-users.

e. Application Whitelisting

- **Application Whitelisting:** Use **application whitelisting** to allow only authorized software to run on endpoints, preventing the execution of malicious payloads like Cobalt Strike on compromised systems.

f. Regular Patching and Updates

- **Patch Management:** Keep systems and applications up to date with the latest security patches to prevent exploitation of known vulnerabilities that could be leveraged by tools like Cobalt Strike.

6. Legal and Ethical Considerations

The use of Cobalt Strike for malicious purposes is illegal and constitutes a criminal act in many jurisdictions. Organizations are encouraged to use Cobalt Strike only for legitimate, ethical activities such as penetration testing and red teaming (with the proper authorization). Any unauthorized use of Cobalt Strike for cyberattacks, data theft, or other malicious activities is punishable under laws related to hacking, data theft, and cybersecurity crimes.



Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perandurai, Erode - 633 021



ERODESENGUNTHAR ENGINEERINGCOLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna

University-

Chennai, Accredited by National Board of Accreditation (NBA), New Delhi &

National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade

**PERUNDURAI-638057, TAMILNADU,
INDIA.**



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING (5 YEARS INTEGRATED)

21CSX04-CYBER SECURITY AND ETHICAL HACKING

Innovative Assignment - 1

Submission Due: 08.02.2024

Mapping with Course Outcome: CO1

Mapping with Program Outcome: PO1,2,3,4,6,7,9,11,12 PSO1,2,3

Instructions:

- ANSWER NEATLY AND LEGIBLY on A4 sheets only and not in sheets torn from a book.
- Sketch diagrams wherever relevant. Explain your notations explicitly and clearly.
- An incomplete assignment is not acceptable for submission.
- Once you submit your assignment, you will be expected to answer all the questions there **INDEPENDENTLY**. You may be asked to answer any question of the assignment in the class.
- All other instructions as in this and all subsequent assignments also.

1. Explain in detail Cyber Crime and Punishment.

Assignments are evaluated as per the given Rubrics as follows:

Criteria	Low (1)	Medium (2)	Strong (3)
Analytical Skills	Minimal ability to analyze the given task	Some ability to analyze the given task	Able to analyze the given task
Writing Skills	The content is quite relevant to the given task.	The content is relevant to the given task.	The content is highly relevant to the given task
Organization	The organization of the paper is weak and support is in substantial or unconvincing	The organization of the paper is good and generally supported with little evidence	The organization of the paper is well supported with evidence
Language	Sentences are somewhat varied, and some are in appropriate with minimal grammatical errors	Sentences are correctly Constructed	Sentences are correctly Constructed and well-articulated
Knowledge Skills and Creative idea	The Student demonstrates a moderate level of the subject knowledge	The Student demonstrates a sufficient level of the subject knowledge with some creative idea	The Student demonstrates sound subject knowledge with a creative idea


Course Coordinator


HOD




Dr. V. VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode - 638 057.



ERODE SENGUNTHAR ENGINEERING COLLEGE

Approved by AICTE, New Delhi. Perpetually Affiliated to Anna University, Chennai.
Accredited by National Board of Accreditation (NBA), New Delhi & All India Council for Technical Education (AICTE), New Delhi.
PERUNDURAI - 638 057, TAMILNADU, INDIA.



Assignment Number - I

Name of the Student : S. Venkatesh
Roll No : 152KJ18
Class / Section : R9904-CSE
Subject Code : J1C904
Name of the Subject : Cyber Security and Critical Thinking
Assignment given on : 29.1.24
Submission date : 8.2.24

S.No.	Criteria for Evaluation	Max. Marks	Marks obtained
1	Analytical Skills	05	05
2	Writing Skills Content	05	05
3	Organization	05	05
4	Language	05	05
5	Knowledge Skills and Creative Idea	05	05
Total		25	25

Signature of the Course Coordinator

Cyber crime and punishments.

Cyber crime refers to illegal activities conducted via the internet or other digital means. It can range from hacking and data breaches to identity theft and financial fraud. Punishments for cyber crime vary by jurisdiction and the severity of the offense, often guided by local laws and international conventions.

Types of cyber crime.

1. Hacking:

Unauthorized access to computer system.

2. Phishing:

Fraudulent attempt to obtain sensitive information by posing as a legitimate entity.

3. Identity Theft:

Stealing personal information to commit fraud.

Ransomware:

Malware that encrypts victim data and demands payment for decryption.

Cyberstalking:

Harassing or threatening individuals online.

Online fraud:

Manipulating victims to transfer money or disclose sensitive information.

Punishments:

Punishments for cybercrime vary depending on the type and severity of the offense, as well as the laws of jurisdiction.

They commonly include fines, imprisonment, or to compensate victims for damages caused.

Severe offenses such as hacking, identity theft, and cyber terrorism often result in lengthy prison sentences.

Fines:

Monetary penalties for lesser offenses or violations like spamming or minor data breaches.

Imprisonment:

Jail sentences for serious crimes like hacking, identity theft, or cyber terrorism.

Restitution:

Payment to victims for damages caused by the cybercrime.

Community service:

For minor offenses in some jurisdictions.

Probation:

Supervised release instead of or following imprisonment.

Restrictions or bans:

Preventing offenders from accessing the internet or specific technologies.



Dr. V. VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode - 638 057.



ERODE SENGUNTHAR ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna

University-

Chennai, Accredited by National Board of Accreditation (NBA), New

Delhi &

National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade

PERUNDURAI-638057, TAMILNADU,
INDIA.



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

(5 YEARS INTEGRATED)

21CSX04-CYBER SECURITY AND ETHICAL HACKING

Innovative Assignment - 2

Submission Due: 23.02.2024

Mapping with Course Outcome: CO2

Mapping with Program Outcome: PO1,2,3,4,6,7,9,11,12 PSO1,2,3

Instructions:

- ANSWER NEATLY AND LEGIBLY on A4 sheets only and not in sheets torn from a book.
- Sketch diagrams wherever relevant. Explain your notations explicitly and clearly.
- An incomplete assignment is not acceptable for submission.
- Once you submit your assignment, you will be expected to answer all the questions there INDEPENDENTLY. You may be asked to answer any question of the assignment in the class.
- All other instructions as in this and all subsequent assignments also.

1. Explain in detail about Types Malicious attacks in Cyber Security

Assignments are evaluated as per the given Rubrics as follows:

Criteria	Low (1)	Medium (2)	Strong (3)
Analytical Skills	Minimal ability to analyze the given task	Some ability to analyze the given task	Able to analyze the given task
Writing Skills	The content is quite relevant to the given task.	The content is relevant to the given task.	The content is highly relevant to the given task
Organization	The organization of the paper is weak and support is in substantial or unconvincing	The organization of the paper is good and generally supported with little evidence	The organization of the paper is well supported with evidence
Language	Sentences are somewhat varied, and some are in appropriate with minimal grammatical errors	Sentences are correctly Constructed	Sentences are correctly Constructed and well-articulated
Knowledge Skills and Creative idea	The Student demonstrates a moderate level of the subject knowledge	The Student demonstrates a sufficient level of the subject knowledge with some creative idea	The Student demonstrates sound subject knowledge with a creative idea

Course Coordinator

HOD



Dr. V. VENKATACHANDRAN, M.S., A.Tech., Ph.D.
PRINCIPAL
Erode Sengunthar Engineering College
(Autonomous)
Thudupathi, Perundurai, Erode - 638057



ERODE SENGUNTHAR
ENGINEERING COLLEGE
Autonomous
(Approved by AICTE, New Delhi, Perundurai, Tamil Nadu, India)
Accredited by National Board of Accreditation (NBA), New Delhi
NBA Accredited Institution (Autonomous), Erode, Tamil Nadu, India
PERUNDURAI, ERODE-638 057



ASSIGNMENT NUMBER - 2

Name of the Student : G. Kannan
Roll No : E S 21 C J 19
Class/Session : M Tech CSE
Subject Code : 21CS404
Name of the Subject : Cyber Security and Ethical Hacking
Assignment given on : 15.02.21
Submission date : 23.2.21

S.No.	Rubrics for Evaluation	Max. Marks	Marks obtained
1	Analytical Skills	05	05
2	Writing Skills Content	05	05
3	Organization	05	05
4	Language	05	05
5	Knowledge Skills and Creative Idea	05	05
Total		25	25

Signature of the Course Coordinator

Types of malicious attack in cyber security

In cyber security, malicious attack are deliberate action aimed at disrupting, stealing or damaging data, systems or networks.

* Malware

- (i) Viruses : Attach themselves to legitimate files or programs and spread when executed
- (ii) Worms : self-replicating malware that spread across networks without user action.
- (iii) Trojans : Disguise themselves as legitimate software to deceive users.
- (iv) Ransomware : Encrypt a victim's data, demanding payment for decryption.

* Phishing and Spear phishing

Phishing : Hackers use email or messages trick users into revealing sensitive information.
Spear phishing : Targeted phishing attack tailored to specific individuals or organization.

* Denial of Service

Overwhelm a system, server or network with traffic, rendering it unavailable to legitimate users.

* Man-in-the-middle

Attacker intercept and manipulate communication between two parties without their knowledge.

* SQL Injection

Inserting malicious SQL code into a database query to gain unauthorized access to data.

* Cross-site Scripting

Embedding malicious scripts into websites which then execute in users' browsers.

* Zero-day exploit

Exploiting vulnerabilities in software before the vendor patches them.

* Brute force attack

Attempting to guess passwords or encryption keys by systematically trying all possibilities.

* Social Engineering

Manipulating individuals to divulge confidential information.

* Insider Threats

Malicious action by employees or trusted individuals exploiting internal access to data or systems.

* Cryptjacking

Unauthorized use of devices to mine cryptocurrency.

* Botnet

Network of infected devices (bots) controlled remotely to launch attacks.



Dr. V.VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.



ERODE SENGUNTHAR ENGINEERING COLLEGE

(An Autonomous Institution)

Approved by AICTE, New Delhi, Permanently Affiliated to Anna University-
Chennai, Accredited by National Board of Accreditation (NBA), New Delhi &

National Assessment and Accreditation Council (NAAC), Bangalore with 'A' Grade
**PERUNDURAI-638057, TAMILNADU,
INDIA.**



DEPARTMENT OF M.TECH COMPUTER SCIENCE AND ENGINEERING

(5 YEARS INTEGRATED)

21CSX04-CYBER SECURITY AND ETHICAL HACKING

Innovative Assignment - 3

Submission Due: 13.03.2024

Mapping with Course Outcome: CO3

Mapping with Program Outcome: PO1,2,3,4,6,7,9,11,12 PSO1,2,3

Instructions:

- ANSWER NEATLY AND LEGIBLY on A4 sheets only and not in sheets torn from a book.
- Sketch diagrams wherever relevant. Explain your notations explicitly and clearly.
- An incomplete assignment is not acceptable for submission.
- Once you submit your assignment, you will be expected to answer all the questions there INDEPENDENTLY. You may be asked to answer any question of the assignment in the class.
- All other instructions as in this and all subsequent assignments also.

1. Point out the Use of Banner Grabbing and OS Finger Print Techniques

Assignments are evaluated as per the given Rubrics as follows:

Criteria	Low (1)	Medium (2)	Strong (3)
Analytical Skills	Minimal ability to analyze the given task	Some ability to analyze the given task	Able to analyze the given task
Writing Skills	The content is quite relevant to the given task.	The content is relevant to the given task.	The content is highly relevant to the given task
Organization	The organization of the paper is weak and support is in substantial or unconvincing	The organization of the paper is good and generally supported with little evidence	The organization of the paper is well supported with evidence
Language	Sentences are somewhat varied, and some are in appropriate with minimal grammatical errors	Sentences are correctly Constructed	Sentences are correctly Constructed and well-articulated
Knowledge Skills and Creative idea	The Student demonstrates a moderate level of the subject knowledge	The Student demonstrates a sufficient level of the subject knowledge with some creative idea	The Student demonstrates sound subject knowledge with a creative idea

Course Coordinator

HOD



Dr. V. Venkatesh
Erode Sengunthar Engineering College
(Autonomous)
Thudupathi, Perundurai, Erode - 638 057



**ERODE SENGUNTHAR
ENGINEERING COLLEGE**
Autonomous
(Approved by AICTE, New Delhi, Permanently Affiliated to Anna University, Chennai)
Accredited by National Board of Accreditation (NBA), New Delhi
National Accreditation Assessment Council, Bangalore (NAAC)
PERUNDURAI, ERODE-638 057



ASSIGNMENT NUMBER - 2

Name of the Student : G. K. ANAND
Roll No : E S A E C J 14
Class/Session : MTech CSE
Subject Code : 21CSA04
Name of the Subject : Cyber security and Ethical hacking
Assignment given on : 15.02.24
Submission date : 23.2.24

S.No.	Subrics for Evaluation	Max. Marks	Marks obtained
1	Analytical Skills	05	05
2	Writing Skills Content	05	05
3	Organization	05	05
4	Language	05	05
5	Knowledge Skills and Creative Idea	05	05
Total		25	25

Signature of the Course Coordinator

Types of malicious attack in cyber security

In cyber security, malicious attack are deliberate action aimed at disrupting, stealing or damaging data, systems or networks.

a. Malware

- (i) Viruses : Attach themselves to legitimate files or programs and spread when activated
- (ii) Worms : self-replicating malware that spread across networks without user action
- (iii) Trojans : Disguise themselves as legitimate software to deceive users.
- (iv) Ransomware : Encrypt a victim's data, demanding payment for decryption.

a. Phishing and Spear phishing

Phishing : Mass-function email or messenger trick users into revealing sensitive information
Spear phishing : Targeted phishing attacks tailored to specific individuals or organizations.

a. Denial of Services

overwhelm a system, server or network with traffic, rendering it unavailable to legitimate users.

* Man-in-the middle

Attackers intercept and manipulate communications between two parties without their knowledge

* SQL Injection

Inserting malicious SQL code into a database query to gain unauthorized access to data

* Cross-site scripting

Embedding malicious scripts into websites which then execute in users' browsers

* Zero-day exploits

Exploiting vulnerabilities in software before the vendor patches them.

* Brute Force Attack

attempting to guess passwords or encryption keys by systematically trying all possibilities

* Social Engineering

manipulating individuals to divulge confidential information

* Insider Threats

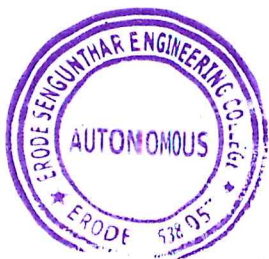
Malicious action by employees or trusted individuals exploiting internal access to data or systems.

* Cryptjacking

Unauthorized use of devices to mine cryptocurrency

* Botnets

network of infected devices (bots) controlled remotely to launch attacks



Dr. V. VENKATACHALAM, M.S., M.Tech., Ph.D.,
PRINCIPAL
Erode Sengunthar Engineering College,
(Autonomous)
Thudupathi, Perundurai, Erode -638 057.