SACRED HEART COLLEGE (AUTONOMOUS)
Tirupattur – 635 601, Tamil Nadu, S.India
Resi : (04179) 220103
College : (04179) 220553
Fax : (04179) 226423
Ready for
Every Good Work

A Don Bosco Institution of Higher Education, Founded in 1951 * Affiliated to Thiruvalluvar University, Vellore * Autonomous since 1987
Accredited by NAAC (4th Cycle – under RAF) with CGPA of 3.31 / 4 at 'A+' Grade

Postgraduate Diploma in Cyber Security

PGDCS

PG Diploma in Cyber Security

Semester	Code	Title of the Subject	L	TCP	P	IM	SM	TM	CD
I	CADC111	Fundamentals of Information Security	4			50	50	100	4
	CADC112	Data Communication and Networking	4			50	50	100	4
	CADC113	Vulnerability Analysis, Penetration Testing, and Incident Handling	4			50	50	100	4
	CADC114	Security Strategies in Operating Systems	4	1		50	50	100	4
			16	**1**		**200**	**200**	**400**	**16**
II	CADC211	Network Cyber Security	4			50	50	100	4
	CADC212	Cyber Forensics	4			50	50	100	4
	CADC213	Application Cyber Security	3	1		50	50	100	4
	CADC214	IOT Security	3	1		50	50	100	4
	CADC215	Advanced Ethical Hacking	3	1		50	50	100	4
	CADC216J	Internship			10	50	50	100	9
			17	**3**	**10**	**300**	**300**	**600**	**29**
	Total Credits								**45**

I SEMESTER

FUNDAMENTALS OF INFORMATION SECURITY 4-0-0:100

Introduction

Information Security refers to the technique to prevent unauthorized access, use, deletion or disruption of information. The concept of information security rests in ensuring the four basic security principles viz. confidentiality, authentication, integrity and non-repudiation. The security principles are enforced through cryptographic algorithms, protocols or standards.

This course aims to deliver the basics of information security, outlines on the four basic principles of information security, highlights the cryptographic algorithms, teaches the symmetric and asymmetric cipher algorithms, stresses on the internet security protocols and user authentication methods.

PREREQUISITE

Network architecture, TCP/IP Model.

COURSE OUTCOMES

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

CO. No.	Course Outcome Statement	Cognitive Level
CO1	Observe and Discuss the basic principles of security.	K1,K2
CO2	Observe and Apply the substitution and transposition methods.	K1,K3
CO3	Recognize and Compute symmetric ciphers	K1,K3
CO4	Tabulate and Compute Asymmetric ciphers	K1,K3
CO5	Observe , Discuss and Correlate the concept of digital signatures with security	K1,K2,K4
CO6	Recognize and Express the structure of Public Key Interfaces.	K1,K2
CO7	Observe and Explain the basic concepts in Internet Security.	K1,K2
CO8	Observe and Use the Internet Security Protocols.	K1,K3
CO9	Recognize and Operate the User Authentication Methods.	K1,K3
CO10	Recognize and Assess the architecture of kerberos.	K1,K5

Mapping of CO with PO and PSO

CO	Programme Outcomes (PO)					Programme Specific Outcomes (PSO)					Mean Scores of COs
	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5	
CO1	3	2	2	3	2	3	3	3	2	2	2.5
CO2	3	2	3	3	3	2	3	3	2	2	2.6
CO3	2	3	2	3	2	3	3	2	3	2	2.5
CO4	3	2	2	3	2	3	3	3	2	2	2.5
CO5	3	2	3	3	2	3	3	3	2	2	2.6
CO6	3	2	3	2	2	3	3	2	2	2	2.4
										Mean Overall Score	2.51666667
										Result	High

Assessment Pattern

Bloom's Category	CA Tests (Marks Allotment)		Term End Exam (100) Marks Allotment
	I CA (50)	II CA (50)	
Remember	10	10	20
Understand	15	15	30
Apply	15	15	30
Analyze	5	5	10
Evaluate	5	5	10
Create	-	-	-

Participatory Assessment

Quiz on basics of Data and Information Security
Problem Solving in Cryptography
Problem Solving in Symmetric Ciphers
Problem Solving in Asymmetric Ciphers
Discussions on Internet Security Protocols
Discussions on User Authentication Methods

Course Content

1. ATTACKS ON COMPUTERS AND COMPUTER SECURITY

Concepts of Security: Need for Security, Security Approaches, Principles of Security, Types of Attacks - Cryptography: Plain Text and Cipher Text, Substitution Techniques, Transposition Techniques, Encryption and Decryption.

2. SYMMETRIC KEY ALGORITHMS

Algorithm Types and Modes, Data Encryption Standard (DES) - Asymmetric Key Algorithms: The RSA Algorithm – Diffie-Hellman Key Exchange Algorithm.

3. DIGITAL SIGNATURES AND DIGITAL CERTIFICATES

Digital Signatures, Attacks on Digital Signature - Public Key Infrastructure (PKI): Digital Certificates, Private Key Management, PKIX Model.

4. INTERNET SECURITY PROTOCOLS

Basic Concepts, Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Hyper Text Transfer Protocol (SHTTP) , Secure Electronic Transaction (SET).

5. USER AUTHENTICATION AND KERBEROS

Authentication Basics, Passwords, Authentication Tokens, Certificate-based Authentication, Key Distribution Center (KDC).

TEXT

A. Kahate, "Cryptography and Network Security", Third Edition, Tata McGraw Hill, New Delhi, 2013.

REFERENCE

1. B.A. Foronzan, "Cryptography & Network Security", Tata McGraw Hill, New Delhi, 2007.
2. S. Stalling, "Cryptography and Network Security", Pearson Education, New Delhi, 2006.

Course Designer Dr. A.George Louis Raja

VULNERABILITY ANALYSIS, PENETRATION TESTING, AND INCIDENT HANDLING

4-0-0:100

OBJECTIVES

- To Learn the core concepts of Vulnerability Analysis.
- To understand the process of penetration testing.
- To learn about incident handling technique.

Unit I

Vulnerability Analysis – Introduction – Hardware and Software defects – Unsecured Networks – Vulnerability management programs – Maintaining an Asset Inventory

Unit II

Vulnerability Analysis – Establishing Secure Connections – Maintaining awareness and Detecting vulnerabilities – Mitigating and remediating identified vulnerabilities – Continuously monitoring the organizations IT environment.

Unit III

Penetration Testing – introduction – method – penetration testing vs vulnerability analysis – types – Manual – Automated – Tools – Infrastructure – Testers – Limitations – Remediation – Legal Issues.

Unit IV

Incident Handling – Preparing for a cyber security incident – Detecting and Identifying potential cyber security incidents – categories of incidents – methods to detect incidents.

Unit V

Incident Handling - Handling and actual incident – contain , eradicate and recover – Communication during a cyber security incident – Incident follow-up and closure.

TEXT

1. http://www.amazon.com/dp/0470170778.

2. http://www.amazon.com/The-Tangled-Web-Securing-Applications/dp/1593273886.

SECURITY STRATEGIES IN OPERATING SYSTEMS 4-1-0:100

Introduction

The course introduces the concept of security in operating systems and software. The main subjects are software vulnerabilities and malicious software, and techniques for mitigating these threats.

Prerequisite

It is recommended with basic knowledge in mathematics and programming

Course Outcomes

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

CO. No.	Course Outcome Statement	Cognitive Level
CO 1	Observe and Discuss the basics of Information security.	K1,K2
CO 2	Recognize, Elicit and Apply the Authorization and access control	K1,K2,K3
CO 3	Observe and Discuss about Laws and Regulations of the privacy policy	K1,K2
CO 4	Recognize and Apply the fundamentals of security strategies in Operating Systems.	K1,K3
CO 5	Demonstrate and Practice the concepts of the network security.	K2,K3
CO 6	Analyze and Evaluate the Operating system security tools	K2,K4

Mapping of CO with PO and PSO

CO	Programme Outcomes (PO)					Programme Specific Outcomes (PSO)					Mean Scores of COs
	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5	
CO1	3	2	2	2	1	3	2	3	1	2	2.1
CO2	3	3	2	3	1	3	3	1	1	2	2.2
CO3	3	2	2	2	1	3	2	1	1	1	1.8
CO4	3	3	2	3	1	3	2	1	2	2	2.2
CO5	3	3	3	2	1	3	2	1	1	2	2.1
CO6	3	2	2	3	1	3	2	1	2	1	2
									Mean Overall Score		2.06666667
									Result		High

Assessment Pattern

Bloom's Category	CA Tests (Marks Allotment)		Term End Exam (100) Marks Allotment
	I CA (50)	II CA (50)	
Remember	10	10	20
Understand	10	10	20
Apply	10	10	20
Analyze	10	10	20
Evaluate	10	10	20
Create	-	-	-

Course Content

Unit I

Introduction-Information Security-Models for discussing security-Attacks-Defense in depth-Identification-Authentication-Additional resources.

Unit II

Introduction – Authorization and Access Control-Authorization–Access control-Access control methodologies-Auditing and Accountability-Security benefits of accountability-Auditing-Logging-Monitoring-Assessments.

Unit III

Operations Security-Origins of operations security-Additional resources-operations security process-Haas' Laws of operations security.

Unit IV

Operating System Security-Operating system hardening-Operating system hardening-Anti-malware tools-Executable space protection-Software firewalls-Host intrusion detection-Operating system security tools.

Unit V

Laws and Regulations-Regulatory compliance-Industry compliance-Privacy-Human Element Security-Security awareness-Effectively reaching users.

TEXT

1. Jason Andress "The Basics of Information Security", Second Edition, Syngress,2014

Course Designer Prof. R. Veeraragavan

II SEMESTER

NETWORK CYBER SECURITY **4-0-0:100**

Introduction:

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. The term applies in a variety of contexts, from business to mobile computing. Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

This course provides the basics of cybersecurity and an in-depth knowledge about various intrusion detection mechanisms. It explores various cyber-attacks and cyber defense mechanisms.

Prerequisites:
Basic understanding of computer networks.

Course Outcomes:

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

CO. NO.	Course Outcome Statement	Cognitive Level
CO1	Understand and Describe about the basic cyber security and Network security aspects.	K1, K2
CO2	Describe and infer about the mechanisms of firewall, intrusion detection system and public cryptography.	K1, K4
CO3	Apply various cryptographic techniques and analyze the protocols used.	K3, K4
CO4	Compare different types of firewalls	K5
CO5	Explore and understand different cyber threats	K5
CO6	Understand different defense mechanism and develop a model for a specific problem	K1, K6

Mapping of CO with PO and PSO

CO	Programme Outcomes (PO)					Programme Specific Outcomes (PSO)					Mean Scores of COs
	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5	
CO1	3	2	2	2	2	2	1	2	2	2	2
CO2	3	2	2	2	3	2	2	2	2	2	2.2
CO3	3	3	2	2	3	2	2	2	3	2	2.4
CO4	3	3	2	3	3	3	2	2	3	3	2.7
CO5	2	2	2	2	3	3	2	3	2	2	2.3
CO6	3	3	3	3	3	3	2	2	3	3	2.8
										Mean Overall Score	2.4
										Result	High

Assessment Pattern

Bloom's Category	CA Tests (Marks Allotment)		Term End Exam (100) Marks Allotment
	I CA (50)	II CA (50)	
Remember	15	15	30
Understand	15	15	30
Apply	10	10	20
Analyze	10	10	20
Evaluate	-	-	-
Create	-	-	-

Participatory Assessment
Online Quiz
Assignments on firewalls, Public cryptography.
Case studies.

Course Content

Unit I
Cyber Security Overview – Introduction – Trends in types of Attacks and Malware - Vulnerability Naming Schemes and Security Configuration Settings - Obfuscation and Mutations in Malware - Network and Information Infrastructure Defense Overview.

Unit II
Firewalls - Unified Threat Management - Firewalls - Stateful/Session Filtering - Application-Level Gateways - Circuit-Level Gateways - A Comparison of Four Types of Firewalls - The Architecture for a Primary-Backup Firewall - Emerging Firewall Technology.

Unit III
Intrusion Detection/Prevention System - IDS/IPS Building Blocks - Anomaly-Based Detection Methods - Network-Based IDS/IPS - Distributed Intrusion Detection Systems and Standards – SNORT.

Unit IV
Public Key Cryptography – The Diffie-Hellman (DH) Protocol – Rivest, Shamir and Adleman (RSA) Public-Key Cryptography – Handshake Protocol – Attacks on the Handshake Protocol.

Unit V
Cyber Threats and Their Defense - Domain Name System (DNS) Protection - A Cache Poisoning Attack – Router Security - The Sender Policy Framework (SPF) – Uniform Resource Locator (URL) Filtering – Botnet Attacks.

TEXT
1. Chwan – Hwa(John) Wu, J, David Irwin, "Introduction to Computer Networks and Cuber Security", CRC Press, 2013.

Course Designer Prof. K. Saravanapriya

CYBER FORENSICS 4-0-0:100

Introduction

Cyber forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of cyber forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

This course aims to provide the basics of cyber forensics, evidence collection, analysis, validation and cyber forensic tools.

Prerequisite

Fundamentals in computer security.

Course Outcomes

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

CO. No.	Course Outcome Statement	Cognitive Level
CO 1	Observe and Elicit the relevance of cyber forensics.	K1,K2
CO 2	Observe, Recognize and Use methods to perform IR.	K1,K2,K3
CO 3	Draft and Develop systems capable of doing analysis and validation.	K5, K6
CO 4	Discuss and Apply evidence collection and forensic tools.	K1,K3
CO 5	Observe and Discuss the basics of network forensics.	K1,K2
CO 6	Compare and Correlate various aspects of cyber forensics.	K2,K4

Mapping of CO with PO and PSO

CO	Programme Outcomes (PO)					Programme Specific Outcomes (PSO)					Mean Scores of COs
	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5	
CO1	3	3	3	2	2	3	3	2	2	2	2.5
CO2	2	3	2	3	2	3	3	2	2	3	2.5
CO3	2	3	2	3	2	3	3	3	2	2	2.5
CO4	3	3	3	2	2	3	3	2	2	3	2.6
CO5	2	3	2	3	2	3	2	2	2	2	2.3
CO6	3	3	3	2	2	3	3	2	2	2	2.5
									Mean Overall Score		2.5
									Result		High

Assessment Pattern

Bloom's Category	CA Tests (Marks Allotment)		Term End Exam (100) Marks Allotment
	I CA (50)	II CA (50)	
Remember	10	10	20
Understand	10	10	20
Apply	10	10	20
Analyze	10	10	20
Evaluate	10	10	20
Create	-	-	-

Participatory Assessment

Quiz in basics of cyber forensics.

Problem Solving in Data Acquisition, evidence collection, analysis and validation.

Course Content

Unit 1

Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques - Incident and incident response methodology - Forensic duplication and investigation.

Unit II

Preparation for IR: Creating response tool kit and IR team. - Forensics Technology and Systems - Understanding Computer Investigation – Data Acquisition.

Unit II1

Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools.

Unit IV

Analysis and validation – introduction - Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition.

Unit V

Network Forensics – Introduction – need for Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics.

TEXT

1. Bill Nelson, Amelia Phillips, Frank Enfinger, Christopher Steuart, ―Computer Forensics and Investigations‖, Cengage Learning, India Edition, 2016.

REFERENCES

1. John R.Vacca, Computer Forensics‖, Cengage Learning, 2005.
2. MarjieT.Britz, Computer Forensics and Cyber Crime‖: An Introduction, 3rd Edition, Prentice Hall, 2013.

Course Designer Dr. A.George Louis Raja

APPLICATION CYBER SECURITY 3-1-0:100

OBJECTIVES

- To learn the concepts in application level cyber security.
- To understand the concepts of ethical hacking and cyber laws.

Unit I

System Security - Desktop Security - Programming Bugs and Malicious code - Database Security

Unit II

Operating System Security – Designing Secure Operating System – OS Security Vulnerabilities – Security Management – Disaster recovery – Digital signature

Unit III

Ethical Hacking – Penetration testing – Computer Forensics

Unit IV

Cyber Laws and Standards - ISO 27001, Cyber Law (Information Technology Act, 2000)- International Standards maintained for Cyber Security

Unit V

Security Audit ,Investigation by Investing Agency - Cyber Security Solutions

TEXT

1. Andrew Honig and Michael Sikorski "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software", , Pearson, 2019

BIG DATA & IOT SECURITY 3-1-0:100

Introduction

IoT security is the family of techniques, strategies and tools used to protect these devices from becoming compromised. Ironically, it is the connectivity inherent to IoT that makes these devices increasingly vulnerable to cyber-attacks, because IoT is so broad and IoT security is even broader.

The course focuses on the basics of why we need security in IoT and the related mechanisms. Next in the flow it elaborates the idea on its architecture and the various threats in the main IoT layers such as Perception layer, Networking layer, and Processing layer.

Prerequisite

Any programming skill.
Role of security in any domains or in computer discipline.

Course Outcomes

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

CO. No.	Course Outcome Statement	Cognitive Level
CO 1	Observe and Discuss the need of security in IoT.	K1,K2
CO 2	Recognize and Elicit the security mechanisms of IoT	K1,K2
CO 3	Identify and Classify the details of IoT Security Architecture	K1,K2
CO 4	Determine and Correlate the details on Security threat in IoT Perception Layer	K3, K4
CO 5	Determine and Correlate the details on Security threat in IoT Networking Layer	K2, K3
CO 6	Determine and Correlate the details on Security threat in IoT Processing Layer	K2, K3

Mapping of CO with PO and PSO

CO	Programme Outcomes (PO)					Programme Specific Outcomes (PSO)					Mean Scores of COs
	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5	
CO1	3	1	2	3	3	3	1	2	3	3	2.4
CO2	3	1	2	3	2	3	1	2	3	2	2.2
CO3	3	1	1	1	1	3	1	1	1	1	1.4
CO4	3	1	1	1	1	3	1	1	1	1	1.4
CO5	3	1	1	1	1	3	1	1	1	1	1.4
CO6	3	1	1	1	1	3	1	1	1	1	1.4
										Mean Overall Score	1.7
										Result	High

Assessment Pattern

Bloom's Category	CA Tests (Marks Allotment)		Term End Exam (100)
	I CA (50)	II CA (50)	
Remember	15	15	30
Understand	10	10	20
Apply	15	15	30
Analyze	5	5	10
Evaluate	5	5	10
Create	-	-	

Participatory Assessment

Paper work to be prepared in related to IoT security techniques and the regulation.
Identifying any free tool which can used to test or analyze the security process.
MCQ can be practiced

Course Content

Unit I

Techniques and applications of IoT-The Components of IoT System –Security and privacy issues in IoT-Architectures of the IoT: Three layer Architecture of IoT - IoT Architecture based on IoT Devices-Four layer-Five layer-Six layer architecture of IoT.

Unit II

IoT Security Architecture: Layer IoT Security Architecture - IoT Perception Layer Security Mechanisms – IoT perception layers Security- IoT Network Layer Security Mechanisms- IoT Processing Layer Mechanism – Security Layer Mechanism – Establishment of Trust and Key management- Operational Supervision and Security evaluation.

Unit III

Security Threats in IoT Perception Layer- Security threat and countermeasures against Eavesdropping attack, Traffic analysis attack, Impersonation attack, data modification attack, Laboratory analysis, cloning attack, Sybil attack, Energy Exhaustion Attack, Reply Attack, Botnet Control.

Unit IV

IoT Network Layer Security- Security Threats in IoT Network Layer- Network Security- Security Techniques in Mobile Communications- Security Techniques in LPWAN.

Unit V

IoT Processing Layer Security- Security Threats in IoT Processing Layer- Database for IoT Processing Layer- Access Control Policies Applicable to IoT Processing Layer- Security Mechanisms in Cloud computing.

TEXT

Chuan-Kun Wu, "Internet of Things Security: Architectures and Security Measures (Advances in Computer Science and Technology)" 1st ed. 2021 Edition.

REFERENCE

1. Harley Hahn, "Internet Complete Reference", Second Edition, Osborne/McGrawHill 1996,

2. Ramesh Bangia Firewall Media, "Internet and Web Design", (An imprint of Lakshmi Publications Pvt. Ltd.). Second Edition 2006

Course Designer Prof. V. Thomas Immanuel

ETHICAL HACKING **3-1-0:100**

Introduction

Ethical hacking course is for network security officers and practitioners, site administrators, IS/IT specialists and analysts, IS/IT auditors, IT operations managers, IT security officers, network specialists, technical support engineers, senior systems engineers, and systems analysts.

Prerequisite

Cyber Laws

Course Outcomes

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

CO No.	Course Outcome Statement	Cognitive Level
CO1	Outline and Elicit ethical considerations of hacking	K1,K2
CO2	Outline and Apply legal considerations of hacking	K1,K3
CO3	Execute, Analyze and Evaluate a penetration test using standard hacking tools in an ethical manner.	K2,K4,K5
CO4	Plan and Draft a vulnerability assessment and penetration test for a network	K1,K3
CO5	Compare and Correlate on the strengths and vulnerabilities of the tested network	K2,K4
CO6	Recognize and Identify legal and ethical issues related to vulnerability and penetration testing.	K2,K4

Mapping of CO with PO and PSO

CO	Programme Outcomes (PO)					Programme Specific Outcomes (PSO)					Mean Scores of COs
	PO1	PO2	PO3	PO4	PO5	PSO1	PSO2	PSO3	PSO4	PSO5	
CO1	3	2	2	2	1	3	2	3	1	2	2.1
CO2	3	3	2	3	1	3	3	1	1	2	2.2
CO3	3	2	2	2	1	3	2	1	1	1	1.8
CO4	3	3	2	3	1	3	2	1	2	2	2.2
CO5	3	3	3	2	1	3	2	1	1	2	2.1
CO6	3	2	2	3	1	3	2	1	2	1	2
									Mean Overall Score		2.1
									Result		High

Assessment Pattern

Bloom's Category	CA Tests (Marks Allotment)		Term End Exam (100) Marks Allotment
	I CA (50)	II CA (50)	
Remember	10	10	20
Understand	10	10	20
Apply	10	10	20
Analyze	10	10	20
Evaluate	10	10	20
Create	-	-	-

Participatory Assessment

Paper work to be prepared in related to IoT security techniques and the regulation.

Identifying any free tool which can used to test or analyze the security process.

MCQ can be practiced

Course Content

Unit I

Ethics of Ethical Hacking- Recognizing the Gray Areas in Security- Vulnerability Assessment- Penetration Testing- The Dual Nature of Tools- Emulating the Attack- The Rise of Cyberlaw- Understanding Individual Cyberlaws- Cyber Security Enhancement Act of 2002- Securely Protect Yourself Against Cyber Trespass Act (SPY Act)- Organization for Internet Safety (OIS).

Unit II

Physical Penetration Attacks- Conducting a Physical Penetration- Common Ways into a Building- Defending Against Physical Penetrations-Insider Attacks- Simulating an Insider Attack- Conducting an Insider Attack- Defending Against Insider Attacks.

Unit III

Windows Exploits- Compiling and Debugging Windows Programs- Writing Windows Exploits- Structured Exception Handling- Windows Memory Protections- Bypassing Windows Memory Protections.

Unit IV

VoIP Attacks- Protocols Used by VoIP- Types of VoIP Attacks- Protect Against VoIP Attacks.

Unit V

SCADA Attacks- Protocols Does SCADA Use- SCADA Fuzzing- Stuxnet Malware- Protect Against SCADA Attacks.

TEXT

1. Allen Harper, Shon Harris, Jonathan Ness,Chris Eagle, Gideon Lenkey, and Terron Williams "Gray Hat Hacking The Ethical Hacker's Handbook" 3rd Edition. The McGraw-Hill 2017.

Course Designer Prof. R. Veeraragavan