### M. Sc. Cyber Security

# **Syllabus**

### **UNIVERSITY DEPARTMENT**

## Program Code: \*\*\*

### 2021-2022 onwards



### **BHARATHIAR UNIVERSITY**

(A State University, Accredited with "A" Grade by NAAC, Ranked 13<sup>th</sup> among Indian Universities by MHRD-NIRF, World Ranking: Times -801-1000,Shanghai -901-1000, URAP - 982)

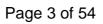
Coimbatore - 641 046, Tamil Nadu, India

The M.Sc. Cyber Security program describe accomplishments that graduates are expected to attain within five to seven years after graduationPEO1To equip with the technical knowledge and skills needed to protect and defend computer systems and networksPEO2To assimilate and use state of the art computing technologies, tools and techniques necessary to provide security to the computing platforms.PEO3To equip with skill to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social and ethical contexts.PEO4To develop graduates that can identify, analyze, and remediate computer security breaches.PEO5To prepare, report and effectively communicate with the stakeholders about Information security process, standards and controls.PEO6To practice managing security relevant projects and function effectively in cyber space as an individual, and as a member or leader in diverse teams.PEO7To appeal self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society.PEO9To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.PEO10To systematically educate the necessity to understand the impact of cyber crimes and threats with solutions in a global and societ context	<b>Program</b>	Educational Objectives (PEOs)
PEO1computer systems and networksPEO2To assimilate and use state of the art computing technologies, tools and techniques necessary to provide security to the computing platforms.PEO3To equip with skill to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social and ethical contexts.PEO4To develop graduates that can identify, analyze, and remediate computer security breaches.PEO5To prepare, report and effectively communicate with the stakeholders about Information security process, standards and controls.PEO6To practice managing security relevant projects and function effectively in cyber space as an individual, and as a member or leader in diverse teams.PEO7To appeal self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society.PEO9To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.		
PEO2techniques necessary to provide security to the computing platforms.PEO3To equip with skill to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social and ethical contexts.PEO4To develop graduates that can identify, analyze, and remediate computer security breaches.PEO5To prepare, report and effectively communicate with the stakeholders about Information security process, standards and controls.PEO6To practice managing security relevant projects and function effectively in cyber space as an individual, and as a member or leader in diverse teams.PEO7To plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.PEO8To appeal self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society.PEO9To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.PEO10To systematically educate the necessity to understand the impact of cyber	PEO1	
PEO3needs within realistic constraints such as economic, environmental, social and ethical contexts.PEO4To develop graduates that can identify, analyze, and remediate computer security breaches.PEO5To prepare, report and effectively communicate with the stakeholders about Information security process, standards and controls.PEO6To practice managing security relevant projects and function effectively in cyber space as an individual, and as a member or leader in diverse teams.PEO7To plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.PEO8To appeal self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society.PEO9To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.PEO10To systematically educate the necessity to understand the impact of cyber	PEO2	
PEO4security breaches.PEO5To prepare, report and effectively communicate with the stakeholders about Information security process, standards and controls.PEO6To practice managing security relevant projects and function effectively in cyber space as an individual, and as a member or leader in diverse teams.PEO7To plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.PEO8To appeal self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society.PEO9To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.PEO10To systematically educate the necessity to understand the impact of cyber	PEO3	needs within realistic constraints such as economic, environmental, social and
PEOSInformation security process, standards and controls.PEO6To practice managing security relevant projects and function effectively in cyber space as an individual, and as a member or leader in diverse teams.PEO7To plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.PEO8To appeal self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society.PEO9To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.PEO10To systematically educate the necessity to understand the impact of cyber	PEO4	
PEO6cyber space as an individual, and as a member or leader in diverse teams.PEO7To plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.PEO8To appeal self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society.PEO9To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.PEO10To systematically educate the necessity to understand the impact of cyber	PEO5	
PEO7protection of information technology assets.PEO8To appeal self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society.PEO9To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.PEO10To systematically educate the necessity to understand the impact of cyber	PEO6	
PEO8       the betterment of individuals, organizations, research community and society.         PEO9       To select suitable ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.         PEO10       To systematically educate the necessity to understand the impact of cyber	PEO7	
PEO9       and human values and also contribute value and wealth for the benefit of the society.         PEO10       To systematically educate the necessity to understand the impact of cyber	PEO8	
	PEO9	and human values and also contribute value and wealth for the benefit of the
ermites and threats with solutions in a grobal and societal context	PEO10	To systematically educate the necessity to understand the impact of cyber crimes and threats with solutions in a global and societal context

The Barton

Program	Specific Outcomes (PSOs)
After the to	successful completion of M.Sc. Cyber Security program, the students are expected
PSO1	To understand the cyber space and frame the foundations of security principles, enterprise and models to suit the needs of the industry.
PSO2	To select and operate the cloud infrastructure and enterprise system based on the security and storage needs.
PSO3	To ensure the credibility of the information systems by managing the security standards and protocols.
PSO4	To enumerate system vulnerability and provide solutions for vulnerabilities and other potential threats.
PSO5	To code and execute python programming with a higher level of expertise.
PSO6	To develop and assist in designing security software architecture and testing its credibility against threats.
PSO7	To understand and carry out the digital forensics process for evidence collection under investigative techniques.
PSO8	To develop basic understandings of IoT structures and develop familiarity with basic security attacks and its measures.
PSO9	To develop a deeper understanding and familiarity with various types of cyber attacks and vulnerable frames to tackle them.
PSO10	To raise skill in dealing with advanced web technologies allied with complex and sophisticated IT infrastructure.

Program	n Outcomes (POs)
On succe	essful completion of the M. Sc. Cyber Security program
PO1	Analyze and evaluate the cyber security needs of an organization
PO2	Conduct a cyber security risk assessment
PO3	Perform Network and Application Vulnerability Assessment
PO4	Implement sustainable cyber security solutions for various cyber threats as per business requirements.
PO5	Articulated reporting and effective communication with the stakeholders, about security process, standards and controls.
PO6	Spear head and run cyber security relevant projects and function effectively in cyber space as an individual, and as a member or leader in diverse teams.
PO7	Design and Develop secure architecture for an organization
PO8	Habit of self-learning for continual development as a cyber professional for the betterment of individuals, organizations, research community and society.
PO9	Implementation of ethical principles and commit to professional responsibilities and human values and also contribute value and wealth for the benefit of the society.
PO10	Evaluate the impact of cyber crimes and threats in a global and societal context.



#### M.Sc. CYBER SECURITY 2021-2022 Univ.Dept. in collaboration with CSCC Lab (*Effective from the academic Year 2021-2022*)

#### SCHEME OF EXAMINATIONS

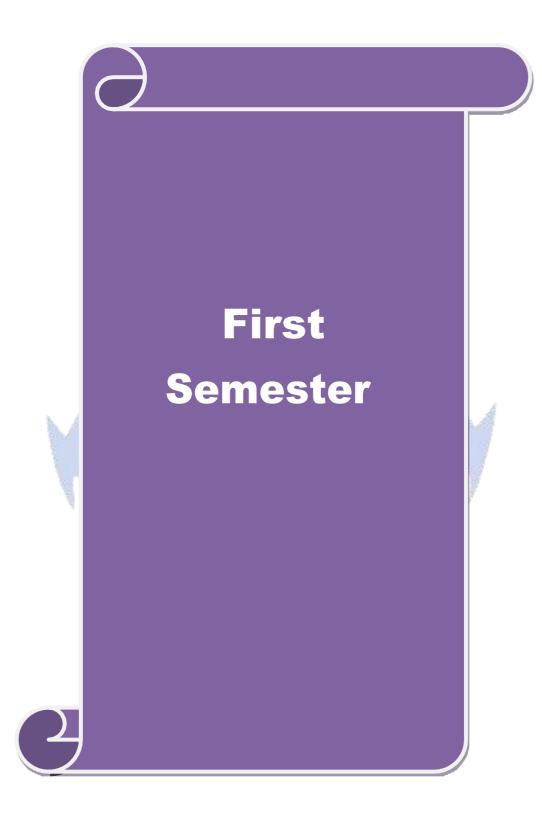
<b>Course Code</b>	Title of the Course	Credits	He	ours	Max	<b>/larks</b>	
Course Code			Theory	Practical	CIA	ESE	Total
		TIRST SEMEST	ER				
21CSESC01	Core I: Security Principles an Governance	nd 4	62	0	50	50	100
21CSESC02	Core II: Network Technologies and Security	4	62	0	50	50	100
21CSESC03	Core III: Basics of Ethical Hacking for Cyber Security	4	32	60	50	50	100
21CSESC04	Core IV: Python Programm	ning 4	32	60	50	50	100
21CSESC05	Core V: Soft Skills	4	32	30	50	50	100
	Elective I						
Supportive	Offered by other Department	ts 2	31		25	25	50
	<i>ž</i> 1	Total 22	220	150	275	275	550
		COND SEMES					
21CSESC07	Core VI: Secure Software Design & Analysis	4	62	0	50	50	100
21CSESC08	Core VII: Digital Forensics & Best Practices	& 4	62	0	50	50	100
21CSESC09 -	Core VIII: Mobile & IoT	4	32	60	50	50	100
21CSESC10	Core IX: Advanced Ethical Hacking & Penetration Testing	4	32	60	50	50	100
21CSESC11	Core X: Information System Risk Management	s 4	62	0	50	50	100
	Elective II			1.00			60.0
		Total 20	250	120	300	300	600
		HIRD SEMEST	TER	T	1	1	T
21CSESC12	Core XI: Evolving Technolo and Threats	4	62	0	50	50	100
21CSESC13	Core XII: Security Standards Compliance	4	62	0	50	50	100
21CSESC14	Core XIII: Case studies of C Security – Paper 1	6	0	0	50	100	150
21CSESC15	Core XIV: Case studies of C Security – Paper 2	yber 6	0	0	50	100	150
	Elective III						
	Elective IV						
Supportive	Offered by other Department		31		25	25	50
		Total 22	124	0	225	325	550
		OURTH SEMES	TER				1
	Project / Dissertation + V voce	<sup>/iva-</sup> 14			175	175	350
		Total 14			175	175	350
	Grand T	Total 94	594	270	975	1075	2050

СО-ЅСНО	LASTIC	COURSES				
ONLI	INE COU	JRSES				
Swayam, MOOC Course etc.,	2	-	-	-	-	-
VALUE A	<b>DDED</b>	COURSES				
Value Added Course - I	2	30	-	50	-	50
Value Added Course - II	2	30	-	50	-	50
CERTIF	ICATE C	COURSES				
Certificate Course - I	4	30-40	-	100	-	100
Certificate Course - II	4	30-40	-	100	-	100
The scholastic courses are only counted award of the degree, the completion of co						or the

#### Electives for M.Sc Cyber Security(CBCS)

Elective	Suggested Code	Title OfthePaper	L	Р
Elective	21CSESE01	IT Infrastructure and Cloud Security	0	4
Elective	21CSESE02	Malware Analysis	2	2
Elective	21CSE <mark>SE03</mark>	Incident Response and Handling	4	0
Elective	21CSE <mark>SE</mark> 04	Cyber Threat and Intelligence	4	0
Elective	21CSESE05	Cyber Law	4	0
Elective	21CSESE06	Artificial Intelligence & Machine Learning	4	0

1



Course code	21CSESC01	SECURITY PRINCIPLES & GOVERNANCE	L	Т	Р	(
Core/Elect	tive/Supportive	Core	4			4
Pre-requisite		Terminologies and fundamentals of Risk Management	Syllab Versio		2021- 2022	
	bjectives:					
	objectives of this					
		ndamental functioning of securitypatterns.	10	•,		
		nterprise Security and Risk Management, A eed for Authentication, Access controls, Sec			ne	
		ity Assessment and Testing.	uniyope	1 <b>u</b> 10	115.	
Expected	<b>Course Outcome</b>	es:				
On the suc	ccessful completio	on of the course, student will be able to:				
1 Und	erstand the fundan	nental functioning of security patterns			K2	
2 Und	erstand the Enterp	rise Security and Risk Management, Asset	Security		K2	
3 Und	erstand the Auther	ntication, Access controls, Security operation	ons		K2	
4 Und	erstand the Securit	ty Assessment and Testing			K2	
5 Ana	lyze, Apply <mark>, Creat</mark>	e and Evaluate the Security Assessment and	d Testing	5	K3	
	per la	A RE COA			K6	
KI - Rem	ember; <mark>K2</mark> - Unde	erstand; <b>K3</b> - Apply; <b>K4</b> - Analyze; <b>K5</b> - Ev	aluate;	X6 –	Creat	e
Unit:1 Overview c	f Security, Securit	<b>Foundations of Security</b> ty Taxonomy, General Security Resources,	Security	10 Patte	hour erns-	S
<b>Unit:1</b> Overview of The Histor	f Security, Security y of Security Pa Security Pattern I	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics o Mining and Types of Patterns.	Security	<b>10</b> Patte ity P	hour erns-	r <b>s</b> ns,
Unit:1 Overview of The Histor Sources for Unit:2	of Security, Security by of Security Pa Security Pattern I Enterprise	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics o Mining and Types of Patterns.	Security of Securi	10 Patte ity P	hour erns- atterr 2 hou	rs ns,
Unit:1 Overview of The Histor Sources for Unit:2 Security N	of Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  E Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation,	Security of Security	10 Patte ity P 12 Asse	hour erns- atterr 2 hou	ns,
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili	of Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification ty Assessment, R	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns. e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap	Security of Security Threat proaches	10 Patte ity P 12 Asse s, En	Phour erns- atterr 2 hou ssmer terpri	ns,
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se	of Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification ty Assessment, R rvices and Enterprise	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  E Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation,	Security of Security Threat proaches and Aut	10 Patte ity P 12 Asse s, En henti	hour erns- eatterr 2 hou ssmer terpri catior	ns. nrs. nt. sen
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require	of Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification ty Assessment, R ervices and Enterprise ments, Automate	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  E Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification	Security of Security Threat proaches and Aut	10 Patte ity P 12 Asse s, En henti	hour erns- eatterr 2 hou ssmer terpri catior	ns,
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I	of Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification ty Assessment, R ervices and Enterprise ments, Automate	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  E Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives.	Security of Security Threat proaches and Aut	10 Patte ity P 12 Asse s, En hentio Alter	hour erns- eatterr 2 hou ssmer terpri catior native	ns, ns, nt, se
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3	of Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification ty Assessment, R revices and Enterprise ments, Automate Design and Use, Bi	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns. e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives. Access Control Models	Security of Security Threat proaches and Autl Design	10 Patte ity P 12 Asse s, En hentie Alter	hour erns- eatterr 2 hou ssmer terpri catior native 2 hou	nt. sent
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3 Authorizati	of Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification ty Assessment, R prvices and Enterprise ments, Automate Design and Use, Bi on, Role-Based A	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics o Mining and Types of Patterns.  e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives.  Access Control Models Access Control, Multilevel Security, Refer	Security of Security of Security Threat proaches and Auti Design A	10 Patte ity P 12 Asse s, En hentio Alter 12 onito	2 hour erns- eatterr 2 hou ssmer terpri catior native 2 hou or, Ro	ns, nt, se n es, ole
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3 Authorizati Rights Def	on, Role-Based A if Security, Security Pattern I Enterprise En	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  E Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives.  Access Control Models Access Control, Multilevel Security, Refer Access Control Architecture - Access Co	Security of Security Threat proaches and Auti Design A rence M ontrol Re	10 Patte ity P 12 Asse s, En hentio Alter 12 onito equir	Phour erns- eatterr 2 hou ssmer terpri catior native 2 hou or, Ro emen	ns ns nt se n es lers
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3 Authorizati Rights Def Single Acc	on, Role-Based A Sinition, System A Security Pattern I Enterprise	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns. e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives. Access Control Models Access Control Architecture - Access Co c Point, Security Session, Full Access w	Security of Security Threat proaches and Auth Design A rence M ontrol Re vith Erro	10 Patte ity P 12 Asse s, En hention Alter 12 onito equir prs, 1	hour erns- eatterr 2 hou ssmer terpri catior native 2 hou or, Ro emen Limit	nt nt se nt se nt se nt se nt se nt se nt se nt se se se
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3 Authorizati Rights Def Single Acc Access. Op	of Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification ty Assessment, R prvices and Enterprise ments, Automate Design and Use, Bi on, Role-Based A inition, System A cess Point, Check perating System A	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives.  Access Control Models Access Control, Multilevel Security, Refer Access Control Architecture - Access Co c Point, Security Session, Full Access w Access Control – Authenticator, Controll	Security of Security of Security Threat proaches and Auti Design A cence M ontrol Re vith Erro ed Proc	10 Patte ity P 12 Asse s, En hentio Alter 12 onito equir ors, 1 ess (	hour erns- eatterr 2 hou ssmer terpri catior native 2 hou or, Ro emen Limit	nt nt se nt se nt se nt se nt se nt se nt se nt se se se
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3 Authorizati Rights Def Single Acc Access. Op Controlled	f Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification ty Assessment, R ervices and Enterpr ments, Automate Design and Use, Bi on, Role-Based A finition, System A cess Point, Check perating System A	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns. e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives. Access Control Models Access Control Architecture - Access Co c Point, Security Session, Full Access w	Security of Security Threat proaches and Autl Design A cence M ontrol Re vith Erroc ed Proc dressSpa	10 Patte ity P 12 Asse s, En hentio Alter 12 onito equir ors, 1 ess (	hour erns- eatterr 2 hou ssmer terpri catior native 2 hou or, Ro emen Limit	nt nt se nt se nt se nt se nt se nt se nt se nt se se se
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3 Authorizati Rights Def Single Acc Access. Op Controlled Execution I	f Security, Security y of Security Pattern I Security Pattern I Enterprise eeds Identification ty Assessment, R ervices and Enterpr ments, Automate Design and Use, Bi on, Role-Based A finition, System A cess Point, Check perating System A	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives.  Access Control Models Access Control, Multilevel Security, Refer Access Control Architecture - Access Co c Point, Security Session, Full Access w Access Control – Authenticator, Controll ntrolledObjectMonitor,ControlledVirtualAd ed Execution Environment and File Authorized	Security of Security Threat proaches and Autl Design A cence M ontrol Re vith Erroc ed Proc dressSpa	10 Patte ity P 12 Asse s, En hentio Alter Dis, 1 ess ( ace,	hour erns- eatterr 2 hou ssmer terpri catior native 2 hou or, Ro emen Limit Create	ns, nt, sen sed ole ole
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3 Authorizati Rights Def Single Acc Access. Op Controlled Execution I Unit:4	f Security, Security y of Security Pattern I Enterprise eeds Identification ty Assessment, R revices and Enterpr ments, Automate Design and Use, Bi on, Role-Based A finition, System A cess Point, Check Derating System A DbjectFactory,Cor Domain, Controlle	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives.  Access Control Models Access Control, Multilevel Security, Refer Access Control Architecture - Access Co c Point, Security Session, Full Access w Access Control – Authenticator, Controll ntrolledObjectMonitor,ControlledVirtualAd ed Execution Environment and File Authoriz  Security Operations	Security of Security Threat proaches and Auti Design A rence M ontrol Re vith Erroc dressSpa zation.	10 Patte ity P 12 Asse s, En hention Alter onito equir ors, 1 ess ( ace, 12	2 hour erns- eatterr 2 hou ssmer terpri catior native 2 hou or, Ro emen Limit Creato	ns, nt, sen sed ole ole
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3 Authorizati Rights Def Single Acc Access. Op Controlled Execution I Unit:4 Investigatio	on, Role-Based A inition, System A cess Point, Check perating System A comparison of the system A comparison of the system A cons, Role-Based A controlled by the system A construction of the	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification D iometrics DesignAlternatives.  Access Control Models Access Control, Multilevel Security, Refer Access Control Architecture - Access Co c Point, Security Session, Full Access w Access Control – Authenticator, Controll ntrolledObjectMonitor,ControlledVirtualAd ed Execution Environment and File Authorit Security Operations Types, Logging and Monitoring, Provisionity	Security of Security of Security Threat proaches and Auti Design A cence M ontrol Re vith Erro ed Proc dressSpa zation.	10 Patte ity P 12 Asse s, En hention Alter onito equir ors, 1 ess ( ace, 12 source	hour erns- eatterr 2 hou ssmer terpri catior native 2 hou or, Ro emen Limit Create	s ns, nt. se nt. se ole ts ed or
Unit:1 Overview of The Histor Sources for Unit:2 Security N Vulnerabili Security Se – Require Password I Unit:3 Authorizati Rights Def Single Acc Access. Op Controlled Execution I Unit:4 Investigatio	of Security, Security y of Security Pattern I Enterprise eeds Identification ty Assessment, R ervices and Enterprise ments, Automate Design and Use, Bi on, Role-Based A inition, System A cess Point, Check perating System A DbjectFactory,Cor Domain, Controlle	Foundations of Security ty Taxonomy, General Security Resources, tterns, Scope of Pattern Characteristics of Mining and Types of Patterns.  e Security and Risk Management, Asset Security n for Enterprise Assets, Asset Valuation, isk Determination, Enterprise Security Ap rise Partner Communication. Identification ed Identification and Authentication D iometrics DesignAlternatives.  Access Control Models Access Control, Multilevel Security, Refer Access Control Architecture - Access Co c Point, Security Session, Full Access w Access Control – Authenticator, Controll ntrolledObjectMonitor,ControlledVirtualAd ed Execution Environment and File Authoriz  Security Operations	Security of Security of Security Threat proaches and Auti Design A cence M ontrol Re vith Erro ed Proc dressSpa zation.	10 Patte ity P 12 Asse s, En hentio Alter 12 onito equir ors, 1 ess ( ace, 12 sourc ciden	hour erns- eatterr 2 hou ssmer terpri catior native 2 hou or, Ro emen Limit Create	s ns nt sec n sec rs eccor

Assessment and Test Strategies, Security Control, Collect Security Process Data, Test Output, Conduct or Facilitate Internal and Third-Party Audits. Software security – Security in the software development life cycle, Security controls in the development environment Theeffectivenessofsoftwaresecurity, Assesssoftwareacquisitionsecurity.Casestudies-Web Security and Mobile Security.         Unit:6       Contemporary Issues       2 hour         Security Challenges in Robotics, Security challenges in Distributed Networks.       62 hour         Text Book(s)       1       Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frant Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems Engineering", Wiley Publications, 2013.       2         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition, 2015			
Output, Conduct or Facilitate Internal and Third-Party Audits. Software security – Security in the software development life cycle, Security controls in the development environment Theeffectivenessofsoftwaresecurity,Assesssoftwareacquisitionsecurity.Casestudies-Web Security and Mobile Security.         Unit:6       Contemporary Issues       2 hour         Security Challenges in Robotics, Security challenges in Distributed Networks.       62 hour         Text Book(s)       1       Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frant Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems Engineering", Wiley Publications, 2013.         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition, 2015         3       Tony Hsiang-Chih Hsu, "Practical Security Automation and Testing", Pack Publishing, 2019         Reference Books : EBooks       1         1       https://repo.zenk_security@20Assessment%20_software%20%20%20%20%20Failles/The%20Art%20of%20	Unit:5	Security Assessment & Testing	14hour
in the software development life cycle, Security controls in the development environment Theeffectivenessofsoftwaresecurity,Assesssoftwareacquisitionsecurity.Casestudies- Web Security and Mobile Security. Unit:6 Contemporary Issues 2 hour Security Challenges in Robotics, Security challenges in Distributed Networks. Total Lecture hours 62 hour Text Book(s) 1 Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems Engineering", Wiley Publications, 2013. 2 Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition,2015 3 Tony Hsiang-Chih Hsu, "Practical Security Automation and Testing", Pack Publishing,2019 Reference Books : EBooks 1 https://repo.zenk- security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20 Software%20Security%20Assessment%20-	Assessmen	t and Test Strategies, Security Control, Collect Security I	Process Data, Tes
Theeffectivenessofsoftwaresecurity, Assesssoftwareacquisitionsecurity. Casestudies-Web Security and Mobile Security.         Unit:6       Contemporary Issues       2 hour         Security Challenges in Robotics, Security challenges in Distributed Networks.       62 hour         Total Lecture hours       62 hour         Text Book(s)       62 hour         1       Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank       Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security and Systems Engineering", Wiley Publications, 2013.         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition, 2015         3       Tony Hsiang-Chih Hsu, "Practical Security Automation and Testing", Pack Publishing, 2019         Reference Books : EBooks       1         1       https://repo.zenk-security.com/Techniques% 200, 20, % 20% 20, % 20% 20Failles/The% 20Art% 20of% 20 Software% 20Security% 20Assessment% 20-	Output, Co	onduct or Facilitate Internal and Third-Party Audits. Software	security - Security
Web Security and Mobile Security.         Unit:6       Contemporary Issues       2 hour         Security Challenges in Robotics, Security challenges in Distributed Networks.       62 hour         Text Book(s)       62 hour         1       Markus       Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Franl Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems Engineering", Wiley Publications, 2013.         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition,2015         3       Tony       Hsiang-Chih         Publishing,2019       Reference Books : EBooks         1       https://repo.zenk- security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20 Software%20Security%20Assessment%20-			
Unit:6       Contemporary Issues       2 hour         Security Challenges in Robotics, Security challenges in Distributed Networks.       62 hour         Text Book(s)       62 hour         1       Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Franl Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems Engineering", Wiley Publications, 2013.       62 hour         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition, 2015       70ny Hsiang-Chih Hsu, "Practical Security Automation and Testing", Pack Publishing, 2019         Reference Books : EBooks       71       https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20%20for Software%20Security%20Assessment%20-			sestudies-
Security Challenges in Robotics, Security challenges in Distributed Networks.         Total Lecture hours       62 hour         Text Book(s)         1       Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems Engineering", Wiley Publications, 2013.       1         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition,2015       1         3       Tony Hsiang-Chih Hsu, "Practical Security Automation and Testing", Pack Publishing,2019       1         https://repo.zenk- security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20 Software%20Security%20Assessment%20-	Web Secur	ity and Mobile Security.	
Security Challenges in Robotics, Security challenges in Distributed Networks.         Total Lecture hours       62 hour         Text Book(s)         1       Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Fran Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems Engineering", Wiley Publications, 2013.       1         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition,2015       1         3       Tony       Hsiang-Chih       Hsu, "Practical Security Automation and Testing", Pack Publishing,2019         Reference Books : EBooks         1       https://repo.zenk- security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20 Software%20Security%20Assessment%20-	Unit:6	Contomnorary Issues	2 hour
Total Lecture hours       62 hour         Text Book(s)       62 hour         1       Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems Engineering", Wiley Publications, 2013.       62 hour         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition, 2015       62 hour         3       Tony       Hsiang-Chih       Hsu, "Practical Security Automation and Testing", Pack Publishing, 2019         Reference Books : EBooks       1       https://repo.zenk- security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20 Software%20Security%20Assessment%20-			
1       Markus       Schumacher, Eduardo       Fernandez-Buglioni, Duane       Hybertson, Frank         Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems       Engineering", Wiley Publications, 2013.         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition, 2015         3       Tony       Hsiang-Chih       Hsu, "Practical Security Automation and Testing", Pack Publishing, 2019         Reference Books : EBooks         1       https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20         Software%20Security%20Assessment%20-			02 11001
1       Markus       Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank         Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems       Engineering", Wiley Publications, 2013.         2       Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition, 2015         3       Tony       Hsiang-Chih         Publishing, 2019       Hsiang-Chih         Reference Books : EBooks       1         1       https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20	Tort Dools		
Buschmann, Peter Sommerlad, "Security Patterns: Integrating Security andSystems Engineering", Wiley Publications, 2013.         Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition,2015         Tony Hsiang-Chih Hsu, "Practical Security Automation and Testing", Pack Publishing,2019         Reference Books : EBooks         1       https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20         Software%20Security%20Assessment%20-	I EXI BOOK		
Engineering", Wiley Publications, 2013.         Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition,2015         Tony       Hsiang-Chih         Hsu, "Practical Security Automation and Testing", Pack Publishing,2019         Reference Books : EBooks         1       https://repo.zenk- security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20 Software%20Security%20Assessment%20-		,	Hybertson, Fran
<ul> <li>Adam Gordon, Official (ISC)2 Guide to the CISSP CBK, Apple Academic Press Inc., Fourth Edition,2015</li> <li>Tony Hsiang-Chih Hsu, "Practical Security Automation and Testing", Pack Publishing,2019</li> <li>Reference Books : EBooks</li> <li><u>https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20</u> Software%20Security%20Assessment%20-</li> </ul>	1 Markus	Schumacher, Eduardo Fernandez-Buglioni, Duane	
3       Tony Hsiang-Chih Hsu, "Practical Security Automation and Testing", Pack Publishing,2019 <b>Reference Books : EBooks</b> 1 <u>https://repo.zenk-security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20</u> Software%20Security%20Assessment%20-	1 Markus Buschr	Schumacher, Eduardo Fernandez-Buglioni, Duane nann, Peter Sommerlad, "Security Patterns: Integrating Security	
Publishing,2019         Reference Books : EBooks         1       https://repo.zenk- security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20 Software%20Security%20Assessment%20-	1 Markus Buschr Engine 2 Adam Go	Schumacher, Eduardo Fernandez-Buglioni, Duane nann, Peter Sommerlad, "Security Patterns: Integrating Security ering", Wiley Publications, 2013. rdon, Official (ISC)2 Guide to the CISSP CBK, Apple Academ	andSystems
Reference Books : EBooks         1       https://repo.zenk- security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20 Software%20Security%20Assessment%20-	1 Markus Buschr Engine 2 Adam Go Fourth	Schumacher, Eduardo Fernandez-Buglioni, Duane nann, Peter Sommerlad, "Security Patterns: Integrating Security ering", Wiley Publications, 2013. rdon, Official (ISC)2 Guide to the CISSP CBK, Apple Academ Edition, 2015	andSystems nic Press Inc.,
1         https://repo.zenk-           security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20           Software%20Security%20Assessment%20-	1 Markus Buschr Engine 2 Adam Go Fourth 3 Tony	Schumacher, Eduardo Fernandez-Buglioni, Duane nann, Peter Sommerlad, "Security Patterns: Integrating Security ering", Wiley Publications, 2013. rdon, Official (ISC)2 Guide to the CISSP CBK, Apple Academ Edition,2015 Hsiang-Chih Hsu, "Practical Security Automation and	andSystems nic Press Inc.,
security.com/Techniques%20d.attaques%20%20.%20%20Failles/The%20Art%20of%20 Software%20Security%20Assessment%20-	<ol> <li>Markus Buschr Engine</li> <li>Adam Go Fourth</li> <li>Tony Publish</li> </ol>	Schumacher, Eduardo Fernandez-Buglioni, Duane nann, Peter Sommerlad, "Security Patterns: Integrating Security ering", Wiley Publications, 2013. rdon, Official (ISC)2 Guide to the CISSP CBK, Apple Academ Edition,2015 Hsiang-Chih Hsu, "Practical Security Automation and ing,2019	andSystems nic Press Inc.,
Software%20Security%20Assessment%20-	1 Markus Buschr Engine 2 Adam Go Fourth 3 Tony Publish <b>Reference I</b>	Schumacher, Eduardo Fernandez-Buglioni, Duane nann, Peter Sommerlad, "Security Patterns: Integrating Security ering", Wiley Publications, 2013. rdon, Official (ISC)2 Guide to the CISSP CBK, Apple Academ Edition,2015 Hsiang-Chih Hsu, "Practical Security Automation and ing,2019 Books : EBooks	andSystems nic Press Inc.,
	1     Markus       Buschr       Engine       2     Adam Go       3     Tony       Publish <b>Reference I</b> 1 <u>https://</u>	Schumacher, Eduardo Fernandez-Buglioni, Duane nann, Peter Sommerlad, "Security Patterns: Integrating Security ering", Wiley Publications, 2013. rdon, Official (ISC)2 Guide to the CISSP CBK, Apple Academ Edition,2015 Hsiang-Chih Hsu, "Practical Security Automation and ing,2019 Books : EBooks repo.zenk-	andSystems nic Press Inc., d Testing", Pack
<u>%201dentifying%20and%20Preventing%20Software%20Vulnerabilities.pdf</u>	1     Markus       Buschr       Engine       2     Adam Go       Fourth       3     Tony       Publish <b>Reference I</b> 1 <u>https:///security</u>	Schumacher, Eduardo Fernandez-Buglioni, Duane nann, Peter Sommerlad, "Security Patterns: Integrating Security ering", Wiley Publications, 2013. rdon, Official (ISC)2 Guide to the CISSP CBK, Apple Academ Edition,2015 Hsiang-Chih Hsu, "Practical Security Automation and ing,2019 Books : EBooks repo.zenk- y.com/Techniques%20d.attaques%20%20.%20%20Failles/The	andSystems nic Press Inc., d Testing", Pack
	1     Markus       Buschr       Engine       2     Adam Go       Fourth       3     Tony       Publish <b>Reference I</b> 1 <u>https://</u> Softwa	Schumacher, Eduardo Fernandez-Buglioni, Duane nann, Peter Sommerlad, "Security Patterns: Integrating Security ering", Wiley Publications, 2013. rdon, Official (ISC)2 Guide to the CISSP CBK, Apple Academ Edition,2015 Hsiang-Chih Hsu, "Practical Security Automation and ing,2019 Books : EBooks repo.zenk- y.com/Techniques%20d.attaques%20%20.%20%20Failles/The re%20Security%20Assessment%20-	andSystems ic Press Inc., 1 Testing", Pack 20Art%20of%20

	Related Online Contents [MOOC, SWAYAM, NP]	TEL, Websites e	etc.]
	Course Title	Duration	Provider
1	IBM Cyber security Analyst Professional Certificate( 8-courses)		Coursera
We	b link		
1.	http://softwaretestingfundamentals.com/security-testing/		
2.	https://www.ibm.com/in-en/cloud/devops/		
Cou	rse Designed by: Dr.M. Punithavalli & CSCC Labs		

Map	Mapping with Programme Outcomes									
COs	PO 1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	L	L	М	М	L	L	L	L	М	М
CO2	L	S	М	М	L	L	Μ	L	М	S
CO3	L	М	М	М	L	L	Μ	L	М	М
CO4	L	М	S	S	М	L	L	L	М	S
CO5	L	М	S	S	М	L	L	L	М	S

Course code	21CSESC03	Network Technologies and Security	L	Т	Р	С	
<b>Core/Electiv</b>	e/Supportive	Core	4	0	0	4	
Pre-requisi	te	Nil	Syllabus 2021- Version 2022				
Course Obje	ectives:		vers		2022	2	
The main obj 1. To un 2. To un 3. To dis 4. To kn 5. To un <b>Expected Co</b> On the succe 1 Learn 2 Explai 3 Under 4 Illustr 5 Explai 6 Demo K1 - Remer Unit:1 Overview of	ectives of this cou derstand the basic derstand the types scuss about the ne ow about assessm derstand the secur ourse Outcomes: essful completion basics of compute in the Reference N stand network securi ate the security att in Network Securi nstrate about Cryp nber; K2 - Unders Introduction t	es of networks, and reference models s protocols and its usage twork security attacks and network security assi- nent of network security and remote Information rity techniques used in cryptography of the course, student will be able to: er networks and hardware Models (OSI and TCP/IP) curity and identify protocols tacks ty Assessment and RIS otography algorithms stand; <b>K3</b> - Apply; <b>K4</b> - Analyze; <b>K5</b> - Evaluate <b>o Computer Networks and Reference Models</b> <b>works:</b> Introduction – Business and Home Ap	s   5   5   5   5   5   5   5   5   5	es K1,H K2,H K2,H K2,H K2,H Create 12 ns –	<ul> <li>ζ4</li> <li>ζ5</li> <li>ζ5</li> <li>ζ3,Κ.</li> <li>2 hou</li> <li>Mobi</li> </ul>	rs ile	
Models: OS	SI – TCP/IP - C SFNET – Mobile	Network Hardware: PAN – LAN – MAN – omparisons of OSI and TCP/IP. <b>Example Ne</b> Phone Networks – Wireless LAN – RFID and ork and Transport Layer Protocols	etworks	: Int Netw	ernet		
Network I Congestion Internet: Ar Types – Ba	<b>Layer Protocols:</b> control in VC su chitecture– IP pr using – Location	Routing algorithms Congestion control: Pr bnets –congestion control in datagram subnet otocol -IP Address – IPv6. <b>Firewalls:</b> Need and Configuration – IP Security Transport P <b>rotocols</b> : TCP and UDP – Transport Level Secu	s-Netwo – Chara rotocols	ork l	olicie ayer istics	s– in –	
Unit:3	(	Challenges of Security attacks		12	2 hou	rs	
	tacks. Challenge	a of Comming Information Threat Actors	Defen	ding	agair		
Security At Attacks. At Server Attac mobile devi	tacking using Ma cks. Wireless Net ce risks – securing	s of Securing Information – Threat Actors – lware – Social Engineering Attacks. Network work Security Attacks and solutions. Types of g mobile devices – embedded systems and Inter-	ing bas of mobil	e de hings	vices 8.	_	
Security At Attacks. At Server Attac mobile devi	tacking using Ma cks. Wireless Net ce risks – securing Assessment of N	lware – Social Engineering Attacks. Network work Security Attacks and solutions. Types of	ing bas f mobil net of T	e de hings 12	vices 5. 2 hou	_ rs	

Unit	t <b>:5</b>		Basics	of Cryp	tograph	y Algori	thms			12 hour
Secu Bloc RSA - co	urity Attac k Cipher A <b>Hash F</b> u	ks – Secu Structure unctions: A and GC	urity Serv – DES – SHA CM. <b>Digi</b>	vices – S – AES. – SHA 3	Security 1 Asymm 3. Messa	Mechani etric Ci ge Auth	sms. <b>Syn</b> phers: P enticatio	n <b>metric</b> Public Ke on: Requ	Ciphers ey Crypt irements	rchitecture s: Traditiona tography an s – Function Algorithms
Unit	+·6			Contem	porary I	551165				2 hour
	mit an assi	gnment b			<b>-</b>					2 11001
						Tota	l Lectur	e hours		62 hour
	t Book(s)									
	Computer									
	Behrouz Edition, 2		zan, —	Data con	nmunica	tion and	l Networ	king, Ta	ita McG	braw Hill, 4
	Cryptogra Stallings,				rity: Pri	nciples	and Pra	ctice (6 <sup>1</sup>	<sup>h</sup> Editio	on), Willian
4	CompTIA CENGAC	Security- E, 2017.	+ Guide 1	o Netwo	a series					ark Ciampa,
5	Network S	Security A	<mark>Assess</mark> me	ent (2 <sup>nd</sup> E	dition),	Chris Mo	Nab, O'	<mark>RÉ</mark> ILLY	, 2008.	
		1		a state					1	
	ted Onlir							es etc.]		
	nttps://onli					-		1	1	
	nttps://ww					-			<u>s</u>	
	nttps://ww					-		27	1	
<u>h</u>	nttps://npte	el.ac.in/nc	oc/course	<u>s/noc20/</u>	SEM1/n	<u>oc20-cs3</u>	<u>3/</u>	F /		
Web 1	Link		100	1000		1.5	150	1		
1. <u>k</u>	nttps://ww	w.cisco.c	om/c/en_	in/soluti	ons/smal	ll-busine	ss/resour	ce-		
<u>c</u>	center/netv	vorking/n	etworkin	g-basics	<u>.html</u>	e umo	Contraction of the second			
2. <u>k</u>	<u>nttps://doc</u>	<u>s.microso</u>	ft.com/e	n-us/lear	n/module	es/netwo	rk-funda	<u>mentals/</u>		
Cou	rse Design	ed By: M	r. S.Pala	nisamy						
	Mappi	ng with l	Program	me Out	comes					
Cos	PO1	PO2	PO3	PO4	PO5	<b>PO6</b>	<b>PO7</b>	<b>PO8</b>	PO9	PO10
C01	l S	S	М	S	S	L	L	М	М	М
CO <sub>2</sub>		М	М	S	S	L	L	М	М	М
CO3		Μ	L	М	S	L	М	М	Μ	М
CO4		L	L	М	М	М	М	М	S	S
00	- 3.6	C	3.6		1 36	1 3 4	1 3 4	1 36		0

CO6SS\*S-Strong; M-Medium; L-Low

М

CO5

S

М

S

Μ

S

М

S

S

S

S

S

Μ

S

S

S

М

	21CSESC03	BASICS OF ETHICAL HACKING FOR CYBER SECURITY	L	Т	Р	C
Core/Electiv	ve/Supportive	Core	2		2	4
Pre-re	equisite	Basics of Computers, Network, Linux Usage and Cyber Security Terminology	•	abus sion	2021-2022	
	<b>Objectives:</b>					
	5	his course are to:				
		ormation Security, Cyber threats, attacks, w		•		1
	know about dif ethodologies.	fferent modes of hacking tools and phases of	t pene	etration	1 tests	and
	Course Outco	omes:				
		etion of the course, student will be able to:				
		sics of information security, threats and its a	ttack	8	K1.	, K2
		ndamentals of ethical hacking with the hacki			K6	
Meth	nodologies		_		K0	
	• •	s of the penetration test with the methods			K4	4
4	derstand the vul erabilities by se	Inerabilities and use the frameworks to identer the scan	tify			2-K4
5 Uno	derstand the we	b security issues with the fundamentals of C	)WA	SP	K4 K6	4-K5
KI - Ren Create	iember; <b>K2</b> - U	nderstand; K3 - Apply; K4 - Analyze; K5 -	Eval	uate; <b>F</b>	<u> </u>	
Unit:1	<b>Fu</b>	Indamentals of Ethical Hacking			18ho	ours
spoofing -	Access control	eats – Data and Network Security Attack Network protocol and services–Hacking te				MAC king
	N N A	cal Hacking – Ethics and Legality.		4		
Unit:2	Hack	ing Methodology Reconnaissance		4	18ho	ours
Unit:2 Foot pri Penetration Terminolo –NetCraft	Hack nting: Reconn n test - Metho gies of Foot pri – Extract Infor		tion n gat lirecti	test – hering ives –	<b>18ho</b> Phase proce Whois	ours es of ess – s tool
Unit:2 Foot pri Penetration Terminolo –NetCraft Dig – Meta Unit:3	Hack nting: Reconn n test - Metho gies of Foot pri – Extract Infor aGooFil – Socia	<b>Scanning and Enumeration</b>	tion n gat lirecti ail se	test – hering ives – rvers -	18ho Phase proce Whois - Shoc 18ho	es of ess – s tool dan – ours
Unit:2 Foot pri Penetration Terminolo –NetCraft Dig – Met Unit:3 Scanning Nmap Ping TCP Scan Enumerat	Hack nting: Reconn n test - Metho gies of Foot pri – Extract Infor aGooFil – Socia ( c: Concept of N gs and Ping swe – Nmap UDP S ion: Service Fi	<b>Sing Methodology Reconnaissance</b> asissance - Footprinting theory – Penetra ds of Footprinting – Network Information inting –Footprinting through search engine of mation from DNS - Foot printing from Em al Engineering.	tion n gat lirecti ail se - Scat Syn so t Eng sic Ba	test – hering ives – rvers - nning cannin ine anner (	<b>18ho</b> Phase proce Whois - Shoc <b>18ho</b> IPs wi g – Nr Grabbi	es of ess – s tool dan – <b>purs</b> th nap
Unit:2 Foot pri Penetration Terminolo –NetCraft Dig – Meta Unit:3 Scanning Nmap Ping TCP Scan Enumerat – Common NetBIOS	Hack nting: Reconn n test - Metho gies of Foot pri – Extract Infor aGooFil – Socia s: Concept of N gs and Ping swe – Nmap UDP S ion: Service Fi n Network servi	<b>Scanning and Enumeration</b> Mapping and Enumeration Mapping – Port scanning with Nmap – Subnet Scan - Bypass of IPS and IDS – Nmap Scrip Mapping – Vulnerability Scanners – Bas	tion n gat lirecti ail se - Scar Syn so t Eng sic Ba ion –	test – hering ives – rvers – nning cannin ine anner ( SMB	I8ho Phase proce Whois - Shoc I8ho IPs wi g - Nr Grabbi -	es of ess – s tool lan – ours th nap ng

Unit:5	Software Vulnerability (OWASP 10)	18hours
Fundame	ntals of OWASP Zed Attack Proxy (ZAP) - Web app vul	nerability scan - Code
Injection A	Attacks - Broken Authentication - Sensitive Data Expos	sure – XML External
Entities – I	BrokenAccess Control– Security misconfiguration– Website	e pen testing-
	Scripting (XSS) - Insecure Deserialization - Using Con-	nponents with known
vulnerabili	ties – Insufficient logging and monitoring.	
		1
Unit:6	Contemporary Issues	2 hours
Seminar,	Workshop, Training and Webinars	
<b>Text Boo</b>	k(s)	
	lure, S., Scambray, J. and Kurtz, G., 2012. Hacking Expose s and Solutions. New York: McGraw-Hill.	ed 7Network Security
	bretson, P., 2013. The Basics Of Hacking And Penetration ess, an imprint of Elsevier.	Testing. Amsterdam:
Referenc	e Books : EBooks	
	Sabih, Learn Ethical Hacking from Scratch, 2018, PACKT -78862-205-9	publishing, ISBN:
/	h Bothra, Hack <mark>ing be a hacker with ethics, Khanna Pu</mark> blish 3-86173-05-8	ing, 2016, ISBN:
Related (	Online Contents <mark>[M</mark> OOC, SWAYAM, N <mark>PTE</mark> L, <mark>Web</mark> sites	setc.]

	Course Title	Duration	Provider
1.	Ethical Hacker (Free)	6 hours	Alison
2.	The Complete Ethical Hacking Course Bundle	22 hours	StationX
3.	Learn Ethical Hacking From Scratch	14 hours	Udemy
4.	The Complete Cyb <mark>er Security and Hacking Course</mark>	5 Weeks	EH Academy
5.	Introduction to Ethical Hacking and Cyber Security (Free)	5 hours	Udemy
6.	The Art of Exploitation (Free)	3 hours	Cybrary
We	b link		
1.	https://www.guru99.com/what-is-hacking-an-introduction.html		
2.	https://www.besanttechnologies.com/ethical-hacking-tutorial		
3.	https://www.edureka.co/blog/ethical-hacking-tutorial/		
4.	https://www.hackingtutorials.org/		
Cour	se Designed by: Prof. T. Devi and CSCC Labs		

Марр	ing with	Program	me Outo	comes						
COs	<b>PO1</b>	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S	L	М	L	L	L	L	L	L	L
CO3	L	L	L	L	S	М	L	L	L	L
CO3	L	S	М	L	L	L	L	S	L	L
CO4	L	L	L	L	L	L	L	L	L	М
CO5	L	L	L	L	L	L	L	М	S	S

Course code	21CSESC04	PYTHON PROGRAMMING	L	Т	Р	C
Core/Elect	ive/Supportive	Core	2		2	4
Pre-	requisite	Understanding of Programming Concepts	•	abus sion		21- )22
Course Ob	-					
	bjectives of this					
		he basics of Python and Ethical Hacking fromScratc	h.			
Ζ.	To suenguien n	indamental skills in NetworkCommunication.				
Expected (	Course Outcom	es:				
-		etion of the course, student will be able to:				
1 To	describe the env	vironment setup and program basics.			K1	
		Python data structures and data types.			K2	
3 To	demonstrate mo	dular programming and to explain network concept	s		K1/	K3
		environment of virtual environment and understand			K3/	K4
vari	ous library in py	thon				
	understand testi niques.	ng methods and analyze the use cases with suitable			K5/	K6
	1	tand; K3 - Setup; K4 - Analyze; K5 - Evaluate; K6	– Crea	ite		
Unit:1		Python – An Overview		1	5 ho	urs
Editors –I	Python – Jupyte	es - Basic Data Types – Python Built-in Functio er Notebook - Importing and Exporting Files: CSV File – DelimitedFormats.				
Unit:2	1	Python Data Structure		2	0 ho	urs
values– L Tuples –	ist Manipulation Accessing and y – Functions –	iction – Num <mark>Py Package</mark> - Python List: Introdu n – List Operations - Python Tuples: Creating Tup Functions in Tuples – Python Dictionary: Access Namespaces - Indexing – Slicing – Matrices – A	oles - ng –	Oper Func	ation tions	in in
	U	bal and Local Variables.				
		The second se		1	5 ho	urs
Exception Unit:3		bal and Local Variables.	Server			
Exception Unit:3 Modular hostname	Programming - IP – Banner gra	bal and Local Variables. Modular Programming		- Ret	rievii	ng
Exception Unit:3 Modular hostname	Programming - IP – Banner gra	bal and Local Variables. Modular Programming TCP Server- Client – UDP Server- Client – HTTP S bbing - Socket Server Framework – Scapy: Syn Flo		- Ret ack S	rievii	ng 

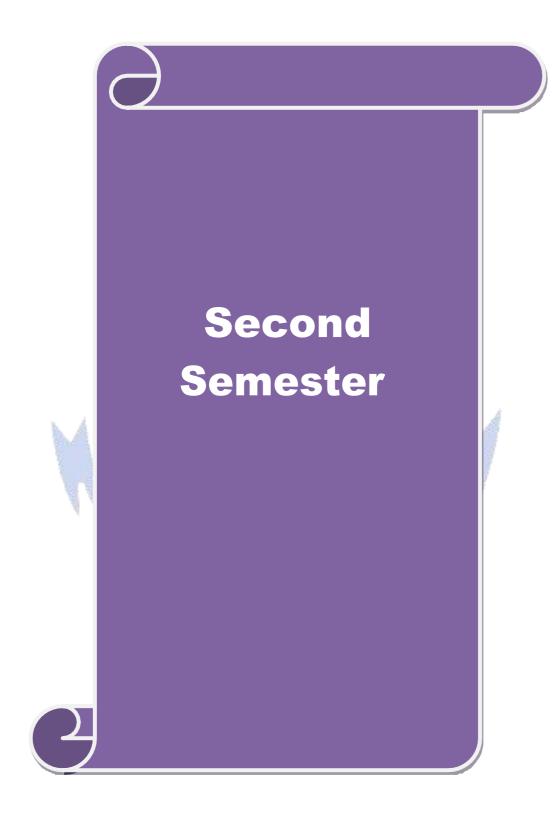
Unit:5	Penetration Testing	20 hours
Penetratio	n Test Introduction – Categories – Pentesting Process – Use Cases:I	Developing Ethical
<u> </u>	Cools: Automating Information Gathering – Keylogger – Bruteforcin	g ZIP Passwords.
Unit:6	Contemporary Issues	2Hours
	in Assignment on any of the following:	
	plete any one Online Courses related to Python and Cybersecurity.	
2. Elab	orate any one Password Encryption Tool usingPython.	
	Total Lecture hours	92hours
Text B		
Referenc		
	ley J. Chun, "Core Python Programming", 2nd Edition, Pearson Edu	
	rew S. Tanenbaum, "Computer Networks", PHI, Fourth Edition, 200	03
	k Summerfield, "Programming in Python", Pearson Education.	
4 Beh	rouz A. Forouzan, "Data communication and Networking", Tata Mc	Graw-Hill, 2004.
	nce Books	
	L. Drake, Guido Van Russom, "An Introduction to Python", Networ	
	am Stallings, "Data and Computer Communication", Sixth Edition, I	Pearson Education,
2000		
	watUssaruyakul, Ekram Hossain, Introduction to Network Simulato	or NS2, Springer,
2009	A DE LEAN	
4 Mag	us Lie Hetland, "Beginning Python: From Novice to Professional",	2nd Edition.
Related	l Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]	A
WWW	onlinecourse <mark>s.swaya</mark> m2.ac.in [Introduction to Cyber Security – Utta	rakhand Open
	rsity, Haldwani] – 12 weeks	
WWW	coursera.com [Penetration Testing, INCIDENT Response and Foren	sics] – 4 weeks
WWW	coursera.com [Python for Everybody] – 17 weeks	
Web L	ink S	1
1. ht	p://python.org	
2. ht	ps://www.computer-pdf.com/programming/802-tutorial-python-tutu	irial.html
	ps://www.pdfdrive.com/penetration-testing-a-hands-on-introduction	i-to-hacking
Course	Designed By: Dr. V. Bhuvaneswari	
	Colling and an and a starting	
7	Learning and the Development of the second	

	Mapping with Programme Outcomes									
COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO1 0
CO1	L	L	L	L	L	L	М	L	L	М
CO2	L	L	L	L	L	L	М	L	L	М
CO3	S	M	Μ	S	L	L	S	L	Μ	S
<b>CO4</b>	S	M	Μ	S	L	L	S	L	Μ	S
CO5	M	M	L	S	L	L	S	L	L	S

Course code	21CSESC05	SOFT SKILLS	L	Т	Р	C
Core/Ele	ctive/Supportive	Core	2		2	4
Pre	e-requisite	Fundamentals in English speaking and writing	Sylla Ver	abus sion		21- 22
	Objectives:					
The mai	n objectives of thi	s course are to:				
		ics of communicationskills				
	Inderstand the log					
	evelop interpersor					
	mprove the writing					
	1 0	e in technicalprogramming				
6. To a	cquired knowledg	e in technical programming and quantitativeaptitude				
-	ed Course Outcor	nes: tion of the course, student will be able to:				
	1	of communication skills and Develop confidence, clar	ity		K2	
	ency through acti		ny,		κ2	
		ls, analytical skills and apply in software applications			K2	
	evelop interperson eaking)	al skills, listening through (seminar, self intro, stage			K3	
4 Im	prove writing skil	lls through various modes (letter writing, resume writ	ing)		K3	
5 Pr	actice technical pr	ogramming, <mark>cracking</mark> code, simple logic and concept	s		K1/	K4
<b>K1</b> - Re	member; <b>K2</b> - Un	derstand; <b>K3 - App</b> ly; <b>K4</b> - Analyze; <b>K5 - Evaluate</b> ; 1	K6- (	Creat	e	
Unit:1		Introduction to Communication		1	2 hou	ir
Commu Introduc	nication – Comn tion - Traits of a C	Communication – Purpose and Audience - Langua nunicative Skills - Modes of Communication – A Good Listener – Listening Modes – Effective Speakin luency – Paralinguistic Features – Types of Speaking	Activ g: Ao	e Li	steni	
Unit:2		Personality Development	18	/1	2 hou	ır
Develop	ment – Interperso	nd Career Growth – Swami Vivekananda"s Conce onal Skills -Soft Skills: Introduction to Soft Skills – sume Writing-Email-letter Writing-Self Introduction	Clas			-
Unit:3		Technical programming skill			4 hou	
		Operators in C – Decision Making– Looping - Branc	hing	State	ment	ts
Variable	- Functions.					
Variable –Array – Unit:4		Quantitative Aptitude1 portion and Partnership – Problems on Ages - Average			2 hou	urs

Unit:5	Quantitative Aptitude 2	10 hours
Simple In	terest - Compound Interest - Time and Work - Time and Distance.	
Unit:6	Contemporary Issues	2 hours
Write an a	assignment on any one of the following:	
1. Traits r	eeded for a softwareEngineer.	
2. Traits r	eeded for a software projectManager.	
3. Traits r	eeded for a Teacher (Software Tester).	
	Total Lecture hours	62 hours
Text Boo		02 110015
	an Sharma, "Technical Communication", 2ndEdition, Oxford Unive	projety Proge 2011
		-
2 Baru	n K. Mitra"Personality Development and Soft Skills", Oxford Univ	ersity Press 2011.
Referenc		<u></u>
	Balagurusamy, "Programming in C", Tata McGraw – Hill Edition, 2	008. 4. S. Chand
and A	AshishAggarwal, "Quick Arithmetic" Sixth Revised Edition.	
D.1.4.14		
	Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]	
	coursera.com [E-mail letter writing- Write Professional Emails in	<u> </u>
	v.coursera.com[Improve your English Communication Skills specia	lization course]
	udemy.com [Personality and Soft Skills Development]	1
	v.coursera.com[ The Science of Well Being]	<u></u>
Web Lin		
	://owl.purdue.edu/ [Online Writing Lab]	1
	<u>/.grammarbook.com</u>	
Course D	esigned By:Dr. M. Punithavalli	
	S. S. State up S. S.	

Mappin	Mapping with Programme Outcomes									
COs	PO1	PO2	PO3	PO4	PO5	<b>PO6</b>	<b>PO7</b>	PO8	PO9	PO10
CO1	L	М	L	S	S	S	S	М	М	L
CO2	L	М	L	S	S	S	S	М	М	М
CO3	М	М	М	М	L	М	М	L	S	L
CO4	S	L	М	L	L	М	М	L	L	L
CO5	S	L	М	L	L	М	М	L	L	L



Course code	21CSESC06	SECURE SOFTWARE DESIGN AND ANALYSIS	L	Т	Р	0
	ve/Supportive	Core	4			4
Pre-r	requisite	Basic Coding Knowledge, Security Concepts, SDLC Process	•	labus sion	202 202	
Course O	bjectives:		1			
The main of	objectives of this	course are to:				
1. To	understand the f	undamentals of security requirement, architect	ure a	ndprin	ciples	5
		hreats and issues insecurity				
3. To	understand the s	ecure coding, testing anddeployment				
Expected	Course Outcom	ies:				
-		on of the course, student will be able to:				
	1	security principles			K2	2
		ems with secure coding and testing			K4	
3 Could	apply the secur	e techniques in coding and testing			K3	3
	rstand the securit	ty violations thatcompromisessecure softw	vare		K2	2
		e techniques in secure software deployment			K3	3
		erstand; K3 - Apply; K4 - Analyze; K5 - Eval	uate;	K6 –	Create	e
			2			
Unit:1		Nee <mark>d of S</mark> ecure Software	Se.	1	2houi	rs
		s, Securit <mark>y Requir</mark> ements, The Proactive Secur SD3 <mark>- Secur</mark> e by Design, by Default, and in De			ment	
						4
Unit:2		ure Design and Secure Architecture			2hour	rs
•		fe Cycle Process, Comparing the secure software software lifecycle, assessing the secure development of the secure develop				
Wildels, Aua	plation of secure	software meeyere, assessing the secure dever	opine	in mo	cycic.	
Unit:3		Threat Modeling		ŝ /1	2 hou	ır
Authorization MACs, and I	Digital Signature	Threat Modeling, Security Techniques stant and Privacy-Enhanced Technologies, E s, Auditing, Filtering, Throttling, andQuality of Service Attacks.	ncry			
Unit:4		Secure Coding		1	4 hou	ırs
Cryptograph Representation	ic Foibles, Pro on Issues, Databa	ining Appropriate Access Control, Running work otecting Secret Data. Issues in secure of ase Input Issues, Web-Specific Input Issues an Security Issues in Documentation and Secur	codin d	g: Ca	nonic	al

	Unit:5	Security Testing and Test Plans	10 hours
Se	curity Test	ting - The Role of the Security Tester, Security Testing Is Diffe	rent, Building
Se	curity Test	Plans from a Threat Model, Testing Clients with Rogue Serve	rs, Testing with
Se	curity Ten	plates, Test the End-to-End Solution, Determining Attack Surf	face. Secure
De	eployment:	Secure Software Installation. Case Study: Socket Security.	
	Unit:6	Contemporary Issues	2 hours
Ch	allenges in	n Secure Web Applications, Application of Penetration Testing	in Software.
		Total Lecture hours	62 hours
Te	xt Book(s)		
1	Michael I	Howard, Steve Lipner, "The Security Development Lifecycle: S	DL, a Process for
	Developi	ng Demonstrably More Secure Software", Microsoft Press, 200	)6
2	Michael I	Howard, David LeBlanc, "Writing Secure Code", Microsoft Pre	ss, 2002
Re	ference B	ooks : EBooks	
1		ww.cybok.org/media/do <mark>wnloads/Sec</mark> ure_Software_Lifecycle_K r_review_April <mark>_2019.pdf</mark>	KA
2	https://sat	fecode.org/wp-	
	-	ploads/2018/03/SAFECode_Fundamental_Practices_for_Secur	e_Software_Develop
		rch_2018.pdf	1
3	https://ww	ww.csiac.org/wp-content/uploads/2016/02/stn8_2.pdf	
Re	lated Onli	ine Con <mark>tents [</mark> MOOC, SWAYAM, NPTEL, Websites etc.]	4

	Course Title	Duration	Provider
1	Foundations of Cyber security	8 weeks	Coursera
2	Fundamentals of Computer Network Security Specialization (4- Courses)	Se !	Coursera
We	eb link	1	
1.		ase/how-to-approa	ch-secure-
	software-development/		
2.	https://www.synopsys.com/blogs/software-security/secure	-sdlc/	
Cou	rse Designed by: Dr.M. Punithavalli and CSSC Labs		

	Mapping with Programme Outcomes												
COs	PO1	PO2	PO3	PO4	PO5	PO6	<b>PO7</b>	PO8	PO9	PO10			
CO1	L	S	L	L	М	Μ	Μ	S	S	S			
CO2	М	М	S	S	S	Μ	М	М	М	S			
CO3	М	М	S	S	L	Μ	L	М	М	S			
CO4	М	М	S	S	L	Μ	L	М	М	S			
CO5	М	М	S	S	L	L	М	L	L	S			

Course code	21CSESC07	DIGITAL FORENSICS & BEST PRACTICES	L	T	Р	C
Core/Elect	tive/Supportive	Core	4			4
Pre-	requisite	Operating Systems and Computer Networks	Syllabu Versior			)21- )22
Course Obje	ectives:					
	jectives of this cou					
	1	s and vocabulary of digital forensics and ur				
		tal information is a perquisite for the study				
		s exist for use when performing Digital Fo				
		play a major role in getting that evidence a	dmitted int	ocou	rt.	
	•	m artifacts and anti forensicsconcepts.				
		aspect of digitalforensics. ork and mobile deviceforensics.				
J. 10 ul		Six and mobile devicerorensics.				
Expected Co	ourse Outcomes:					
<u> </u>		of the course, student will be able to:				
	1	s and vocabulary of digital forensics.			K2	
			uning and			
		exist for use when performing Digital Fore			K2, K	<b>\</b> 4
	nce admitted into c	e is handled will play a major role in getting	g that			
		artifacts and anti forensics concepts			K2	
		-	coorching		K2 K2	
	and without a warra	le expectations of privacy, private searches int.	, searching		K2	
5 To u	nderstand the netw	ork and mobile device forensics.	C.A.		K2	
K1 - Reme	ember; <b>K2</b> - Under	stand; <b>K3 - A</b> pply; <b>K4</b> - Analyze; <b>K5 - E</b> va	a <mark>luate; K6</mark> -	- Cre	eate	
	Γ		1.2		_	
Unit:1		Digital Forensics			hour	
		gital Forensics – Organizations of Note				
		l. Key Technical Concepts: Bits, Bytes and				
		tures – Storage and Memory – Computing	Environme	ents –	- Data	L
Types – File	e Types – Anocate	d and Unallocated Space.				
Unit:2	Evi	idence Collection, Labs and Tools	1 18	12	hour	
		n – Forensic Laboratories - Policies and	Procedure			
		Tools – Accreditation. Collecting Eviden	and the second s		-	•
		enting The Scene - Chain Of Custody – Clo				na
	d System – Hashin		Ert.	e e je		
	,	A STEIL BISING				
Unit:3	Sys	tem Artifacts, Anti Forensics		12	hour	S
System Ar	tifacts:Deleted Dat	a - Hibernation File – Registry – Print Spo	oling Recy	cle B	in –	
		l Shadow Copy –Link Files.Anti Forensics	Introductio	on – 1	Hidin	g
	word Attacks – Da		1			
Unit:4		al Aspect, Internet and E-Mail			hour	
<b>U</b> 1		Searches Without a Warrant – Search with			ectron	ic
•		il: Internet Overview – Web Browsers – E	Mail – Soc	ial		
Networking	Sites.					

Network Fundamentals – Network Security Tools – Network Fundamentals – Incident Responses         – Network Evidence and Investigations – Mobile Cellular Networks – Operating Systems – Cell         Phone Evidence - Cell Phone forensic tools - Global Positioning Systems. Challenges and         Concerns: Standards And Controls - Cloud Forensics - Solid State Drives.         Unit:6       Contemporary Issues       2 hours         Write an assignment on any one of the following:       1. Legal and privacy issues in computerforensics       2. Open and Proprietary tools for DigitalForensics         2. Open and Proprietary tools for Digital Forensics.       Total Lecture hours       62hours         Text Book(s)         1       John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.         2       Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.         Reference Books         1       Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://ollinecourse.swayam2.ac.in (2 courses) - University of Illinois]         1       Digital Forensic       8 Weeks         Police Organization	Unit:5	Network and Device Forensics		12hours
Phone Evidence - Cell Phone forensic tools - Global Positioning Systems. Challenges and Concerns: Standards And Controls - Cloud Forensics - Solid State Drives.       2 hours         Write an assignment on any one of the following:       1. Legal and privacy issues in computerforensics       2 hours         Write an assignment on any one of the following:       1. Legal and privacy issues in computerforensics       62hours         2. Open and Proprietary tools for DigitalForensics       62hours         Text Book(s)       1       John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.       7         2 Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.       8         Reference Books         1 Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.       2         2 Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.       8         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]       1         1 Digital Forensic Science Services & 8 Weeks       8         9 Police Organization       8         1 https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link       1         1. https://dfir.scien	Network Fu	ndamentals – Network Security Tools – Network	Fundamentals -	- Incident Responses
Concerns: Standards And Controls - Cloud Forensics - Solid State Drives.         Unit:6       Contemporary Issues       2 hours         Write an assignment on any one of the following:       1. Legal and privacy issues in computerforensics       2. Open and Proprietary tools for DigitalForensics         2. Open and Proprietary tools for Digital Forensics.       Total Lecture hours       62hours         Text Book(s)         1       John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.         2       Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.         Reference Books         1       Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         1       Digital Forensic Science Services & 8 Weeks         Police Organization       8         Https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link       1. https://dif.science/2017/12/Getting-started-in-Digital-Forensics.html         2. https://dif.science/2017/1				
Unit:6       Contemporary Issues       2 hours         Write an assignment on any one of the following:       1. Legal and privacy issues in computerforensics       2. Open and Proprietary tools for DigitalForensics         2. Open and Proprietary tools for DigitalForensics       Total Lecture hours       62hours         Text Book(s)         1       John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.         2       Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.         Reference Books         1       Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         1       Digital Forensic         11       Introduction of Forensic Science Services & 8 Weeks         Police Organization       8         11       Introduction of Forensic Accomputer-forensics-7857 [Computer Forensics]         Web Link       1. https://www.gluru99.com/digital-forensics.html         2. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         2. https:				ms. Challenges and
Write an assignment on any one of the following:         1. Legal and privacy issues in computerforensics         2. Open and Proprietary tools for DigitalForensics <b>Total Lecture hours</b> 62hours         Text Book(s)         I John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.         2 Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007. <b>Reference Books</b> Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2 Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         I Digital Forensic       16 Weeks         II Introduction of Forensic Science Services & 8 Weeks         Police Organization         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1. https://www.guru99.com/digital-forensics.html         2. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs	Concerns: S	tandards And Controls - Cloud Forensics - Solid	State Drives.	
1. Legal and privacy issues in computerforensics         2. Open and Proprietary tools for DigitalForensics         Total Lecture hours       62hours         Text Book(s)         1       John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.         2       Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.         Reference Books         1       Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         1       Digital Forensic         10       Digital Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         Police Organization       16 Weeks         1       Introduction of Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         Police Organization       16 Web Link         1. https://www.guru99.com/digital-forensics.html       2. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         2. https://dfir.science/2017/12/Getting-started-in	Unit:6	Contemporary Issues		2 hours
2. Open and Proprietary tools for DigitalForensics       Total Lecture hours       62hours         Text Book(s)         I John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.         2 Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.         Reference Books         Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2 Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         I       Digital Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         Police Organization       16 Weeks         II       Introduction of Forensic Science Services & 8 Weeks         Police Organization       10         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link       1. https://www.guru99.com/digital-forensics.html         2. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html       Course Designed By: Dr. S. Gavaskar and CSSC Labs				
Total Lecture hours       62hours         Text Book(s)       62hours         I John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.       7         Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.       8         Reference Books       6         Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.       6         Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.       8         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]       1         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]       1         I       Digital Forensic       16 Weeks         II       Introduction of Forensic Science Services & 8 Weeks       8         Police Organization       8       8         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]       Web Link         1. https://www.guru99.com/digital-forensics.html       2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         2. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html       2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html	U	1 2 1		
Text Book(s)         I John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.         2 Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.         Reference Books         I Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2 Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         I Digital Forensic       16 Weeks         II Introduction of Forensic Science Services & 8 Weeks         Police Organization         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1. https://www.guru99.com/digital-forensics.html         2. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs	2. Open and			1
John Sammons, "The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics", Syngress, 2012.         Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.         Reference Books         Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         I       Digital Forensic         I       Digital Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         Police Organization       8 Weeks         Police Organization       10 Mittps://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link       1. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         2. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs		Total I	Lecture hours	62hours
Forensics", Syngress, 2012.         2       Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.         Reference Books         1       Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         1       Digital Forensic         10       Digital Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         Police Organization       8 Weeks         1.       https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs       Second	Text Bool	k(s)		
2       Tony Sammes, Brian Jenkinson, "Forensic Computing", Second edition, Springer, 2007.         Reference Books         1       Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         1       Digital Forensic         10       Digital Forensic Science Services & 8 Weeks         11       Introduction of Forensic Science Services & 8 Weeks         11       Introduction of Forensic Science Services & 8 Weeks         12       https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs       Course Designed By: Dr. S. Gavaskar and CSSC Labs			imer for Getting	g Started in Digital
Reference Books         1       Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         1       Digital Forensic         1       Digital Forensic Science Services & 8 Weeks         Police Organization         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs				
1       Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         1       Digital Forensic         1       Digital Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         Police Organization       16 Weeks         1       Introduction of Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         Police Organization       10         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link       1.         1.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs       10	2 Tony Sa	ammes, Brian Jenkinson, "Forensic Computing",	Second edition,	Springer, 2007.
Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 2011.         Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         I       Digital Forensic         I       Digital Forensic Science Services & 8 Weeks         Police Organization         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1.       https://www.guru99.com/digital-forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs				
2011.         2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         I       Digital Forensic         II       Introduction of Forensic Science Services & Police Organization         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1.       https://www.guru99.com/digital-forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs	Reference	e Books		
2       Bill Nelson, Amelia Philips, Chris Steuart, "Guide to Computer Forensics and Investigations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.         Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         I       Digital Forensic         II       Introduction of Forensic Science Services & Police Organization         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1.       https://www.guru99.com/digital-forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs		theide and Harlan Carvey, "Digital Forensics wit	th Open Source	Tools", Elsevier,
Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]         https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         I       Digital Forensic         I       Digital Forensic         II       Introduction of Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         Police Organization       1         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1.       https://www.guru99.com/digital-forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs       5	2 Bill N Investig	elson, Amelia Philips, Chris Steuart, "Gui ations", 5 <sup>th</sup> Edition, CENGAGE Learning, 2015.	ide to Compu	ater Forensics and
https://onlinecourses.swayam2.ac.in (2 courses) - University of Illinois]         I       Digital Forensic         II       Introduction of Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         Police Organization       9         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link       1.         https://www.guru99.com/digital-forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs	Related C	Online Contents [MOOC, SWAYAM, NPTEL,	Websites etc.]	
II       Introduction of Forensic Science Services & 8 Weeks         Police Organization       8 Weeks         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1.       https://www.guru99.com/digital-forensics.html         2.       https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs				
Police Organization         https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1. https://www.guru99.com/digital-forensics.html         2. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs	I	Digital Forensic	16 Weeks	
https://www.classcentral.com/course/edx-computer-forensics-7857 [Computer Forensics]         Web Link         1. https://www.guru99.com/digital-forensics.html         2. https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html         Course Designed By: Dr. S. Gavaskar and CSSC Labs	II	Introduction of Forensic Science Services &	8 Weeks	
Web Link         1. <a href="https://www.guru99.com/digital-forensics.html">https://www.guru99.com/digital-forensics.html</a> 2. <a href="https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html">https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html</a> Course Designed By: Dr. S. Gavaskar and CSSC Labs		Police Organization		
Web Link         1. <a href="https://www.guru99.com/digital-forensics.html">https://www.guru99.com/digital-forensics.html</a> 2. <a href="https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html">https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html</a> Course Designed By: Dr. S. Gavaskar and CSSC Labs		- 8- /		
Web Link         1. <a href="https://www.guru99.com/digital-forensics.html">https://www.guru99.com/digital-forensics.html</a> 2. <a href="https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html">https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html</a> Course Designed By: Dr. S. Gavaskar and CSSC Labs		and the second second		
Web Link         1. <a href="https://www.guru99.com/digital-forensics.html">https://www.guru99.com/digital-forensics.html</a> 2. <a href="https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html">https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html</a> Course Designed By: Dr. S. Gavaskar and CSSC Labs	https://w	ww.classcentral.com/course/edx-computer-foren	sics-7857 [Com	puter Forensics]
<u>https://dfir.science/2017/12/Getting-started-in-Digital-Forensics.html</u> Course Designed By: Dr. S. Gavaskar and CSSC Labs			15	<u> </u>
Course Designed By: Dr. S. Gavaskar and CSSC Labs	1. <u>https</u>	://www.guru99.com/digital-forensics.html	120	
	2. https	://dfir.science/2017/12/Getting-started-in-Digital-	-Forensics.html	
Superra man and Mills	Course De	esigned By: Dr. S. Gavaskar and CSSC Labs	and the second sec	
		BUCATE IN PLENNE		

Mappi	Mapping with Programme Outcomes												
Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO1 0			
CO1	S	S	М	L	L	M	L	М	S	L			
CO2	S	S	М	L	Μ	Μ	L	S	S	L			
CO3	S	S	М	L	L	M	L	М	S	L			
CO4	S	S	М	L	L	М	L	М	S	L			
CO5	S	S	М	L	L	М	L	М	S	L			

Course code	21CSESC08	Mobile and IoT	L T P							
Core/Electiv	ve/Supportive	Core	2	0	2	4				
Pre-re	equisite		Sylla		202					
Course Obje	•	OWASP Concepts	Vers	ion	202	22				
	ectives of this co	ourse are to:								
		ics of mobile computing, Principles and Techniques								
		ction of IoT, Architecture and ParticipatorySensing	g.							
3. To un	derstand the bas	ics of mobile securitytechniques								
Expected Co	ourse Outcomes	•								
*		on of the course, student will be able to:								
1     Learn basics of mobile computing principles and techniques     K1,K2										
2 Understand middleware and proposed applications K2										
		rd and Reference Architecture.		K2.	K4					
		curity and prevention techniques		K1.	K4					
5 Explair	n Commercial Bu	uilding Automation and Demonstrate simple		K2,	K3,					
buildin	g automation			K6						
<b>K1</b> - Reme	ember; <b>K2</b> - Und	erstand; <b>K3</b> - Apply; <b>K4</b> - Analyze; <b>K5</b> - Evaluate;	K6 –	Crea	te					
Unit:1		Introduction to Mobile Computing		18	hou	rs				
Mobile Co	mputing: Introd	uction – Adaptability – Mechanisms for Adaptati	on –	Deve	lop	or				
		Support for Building Adaptive Mobile Applic								
		anagement Principles and Techniques. Data Di								
						nu				
Managemen	t: Challenges - I	Data Dissemination - Data Caching - Cache mainter								
Managemen Web Cachin										
Web Cachin	ng.	Data Dissemination - Data Caching - Cache mainter		Sche	mes	-				
Web Cachin Unit:2	ng. Mobile	Data Dissemination - Data Caching - Cache mainter middleware and Networking Challenges	nance	Sche	mes hou	- rs				
Web Cachin Unit:2 Mobile Mi	ng. Mobile iddleware: Intro	Data Dissemination - Data Caching - Cache mainter middleware and Networking Challenges duction - Adaptation - Agents - Service Discover	nance	Sche 18 Ad Ho	mes hou	- rs nd				
Web Čachin Unit:2 Mobile Mi Sensor Netw	ng. Mobile iddleware: Intro works: Propertie	Data Dissemination - Data Caching - Cache mainter middleware and Networking Challenges	nance Pry. A	Sche 18 d Ho Netw	mes hou oc an vorks	- rs nd 3 -				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discover s of an Ad Hoc Network - Unique Features of Service Party - Servi	ery. A ensor	Sche 18 Ad Ho Netw Appro	mes hou oc an orks oach	- rs nd 3 -				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discove s of an Ad Hoc Network - Unique Features of Se illenges: Constrained Resources - Security - Mobil	ery. A ensor	Sche 18 Ad Ho Netw Appro	mes hou oc an orks oach	- rs nd 3 -				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discover s of an Ad Hoc Network - Unique Features of Se illenges: Constrained Resources - Security - Mobiliand and Configuration - Routing - Fault Tolerance and I	ery. A ensor	Sche 18 Ad Ho Netw Appro	mes hou oc an orks oach	rs nd s - es				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency.	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discove s of an Ad Hoc Network - Unique Features of Se illenges: Constrained Resources - Security - Mobi and Configuration - Routing - Fault Tolerance and I Mobile and IoT	ery. A ensor ility. Relial	Sche 18 Ad Ho Netw Appro- pility 18	mes hou oc an orks oach - hou	rs nd s - es rs				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introduction Overview: H	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discover s of an Ad Hoc Network - Unique Features of Sec illenges: Constrained Resources - Security - Mobile and Configuration - Routing - Fault Tolerance and I Mobile and IoT to IoT - M2M towards IoT the global context. nitecture - Main design Principles and Needed Capa	ery. A ensor ility. Relial An A abiliti	Sche 18 Ad Ho Netw Appro- pility 18 Archite es - 4	mes hou oc an oach - hou ectur An Io	rs nd s - es rs ral				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introduction Overview: H	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch	Data Dissemination - Data Caching - Cache mainter middleware and Networking Challenges duction - Adaptation - Agents - Service Discove s of an Ad Hoc Network - Unique Features of Se illenges: Constrained Resources - Security - Mobi and Configuration - Routing - Fault Tolerance and I Mobile and IoT to IoT - M2M towards IoT the global context.	ery. A ensor ility. Relial An A abiliti	Sche 18 Ad Ho Netw Appro- pility 18 Archite es - 4	mes hou oc an oach - hou ectur An Io	rs nd s - es rs ral				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effice Unit:3 Introduction Overview: H Architecture Art.	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch e Outline. Standa	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discovers s of an Ad Hoc Network - Unique Features of Sec illenges: Constrained Resources - Security - Mobile and Configuration - Routing - Fault Tolerance and I Mobile and IoT to IoT - M2M towards IoT the global context. nitecture - Main design Principles and Needed Capa ards Considerations. IoT Architecture: Introduction	ery. A ensor ility. Relial An A abiliti	Sche 18 Ad Ho Netw Appro- pility 18 Archite es - A te of t	mes hou oc ar vorks oach - hou ectur An Io he	- <b>rs</b> nd S - es <b>rs</b> cal DT				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introduction Overview: H Architecture Art. Unit:4	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch e Outline. Standa	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discovers s of an Ad Hoc Network - Unique Features of Sec illenges: Constrained Resources - Security - Mobile and Configuration - Routing - Fault Tolerance and I Mobile and IoT to IoT - M2M towards IoT the global context. hitecture - Main design Principles and Needed Capa ards Considerations. IoT Architecture: Introduction <b>T Reference Architecture Views</b>	An A abiliti	Sche 18 Ad Ho Netw Appro- Dility 18 Archito es - A re of t 18	mes hou oc an yorks oach - hou ectur An Io he hou	- <b>rs</b> nd S - es <b>rs</b> cal DT				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introduction Overview: H Architecture Art. Unit:4 IoT Reference	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch e Outline. Standa Io' e Architecture: I	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discovers s of an Ad Hoc Network - Unique Features of Sec illenges: Constrained Resources - Security - Mobile and Configuration - Routing - Fault Tolerance and I Mobile and IoT to IoT - M2M towards IoT the global context. nitecture - Main design Principles and Needed Capa ards Considerations. IoT Architecture: Introduction <b>T Reference Architecture Views</b> Introduction - Functional View - Information View	ery. A ensor ility. Relial An A abiliti - Stat	Sche 18 Ad Ho Netw Appro- pility 18 archite es - A re of t 18 18 18 18 18 18 18 18 18 18	mes hou oc an vorks oach - hou ectur An Io he hou	rs nd 3 - es ral oT rs				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introductio Overview: H Architecture Art. Unit:4 IoT Reference and Operation	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch e Outline. Standa Io' e Architecture: I nal View - Other	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discovers s of an Ad Hoc Network - Unique Features of Sec illenges: Constrained Resources - Security - Mobile and Configuration - Routing - Fault Tolerance and I Mobile and IoT to IoT - M2M towards IoT the global context. hitecture - Main design Principles and Needed Capa ards Considerations. IoT Architecture: Introduction <b>I Reference Architecture Views</b> ntroduction - Functional View - Information View Relevant Architectural Views. Participatory Sensite	An A abiliti - Dep ng: In	Sche 18 Ad Ho Netw Appro- pility 18 Archita es - A te of t 18 Alloym trodu	hou oc an vorks oach - hou ectur An Id he hou ent ction	rs nd s - es rs al oT <b>rs</b>				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introduction Overview: H Architecture Art. Unit:4 IoT Referenc and Operation - Roles, Acto	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch e Outline. Standa Io' e Architecture: I nal View - Other rs, Engagement	Data Dissemination - Data Caching - Cache mainter         e middleware and Networking Challenges         duction - Adaptation - Agents - Service Discovered         s of an Ad Hoc Network - Unique Features of Security - Mobile         and Configuration - Routing - Fault Tolerance and I         Mobile and IoT         to IoT - M2M towards IoT the global context.         aitecture - Main design Principles and Needed Capa         ords Considerations. IoT Architecture: Introduction <b>T Reference Architecture Views</b> ntroduction - Functional View - Information View         Participatory Sensing Process - Technology Overwards	An A abiliti - Dep ng: In	Sche 18 Ad Ho Netw Appro- pility 18 Archita es - A te of t 18 Alloym trodu	hou oc an vorks oach - hou ectur An Id he hou ent ction	rs nd s - es rs al oT <b>rs</b>				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introduction Overview: H Architecture Art. Unit:4 IoT Referenc and Operation - Roles, Acto	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch e Outline. Standa Io' e Architecture: I nal View - Other rs, Engagement	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discovers s of an Ad Hoc Network - Unique Features of Sec illenges: Constrained Resources - Security - Mobile and Configuration - Routing - Fault Tolerance and I Mobile and IoT to IoT - M2M towards IoT the global context. hitecture - Main design Principles and Needed Capa ards Considerations. IoT Architecture: Introduction <b>I Reference Architecture Views</b> ntroduction - Functional View - Information View Relevant Architectural Views. Participatory Sensite	An A abiliti - Dep ng: In	Sche 18 Ad Ho Netw Appro- pility 18 Archita es - A te of t 18 Alloym trodu	hou oc an vorks oach - hou ectur An Id he hou ent ction	rs nd s - es rs al oT <b>rs</b>				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introduction Overview: H Architecture Art. Unit:4 IoT Reference and Operation - Roles, Acton Scenario - Reference	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch e Outline. Standa Io' re Architecture: I nal View - Other rs, Engagement ecent Trends - A	Data Dissemination - Data Caching - Cache mainter <b>middleware and Networking Challenges</b> duction - Adaptation - Agents - Service Discovers s of an Ad Hoc Network - Unique Features of Sec illenges: Constrained Resources - Security - Mobile and Configuration - Routing - Fault Tolerance and I Mobile and IoT to IoT - M2M towards IoT the global context. nitecture - Main design Principles and Needed Capa ards Considerations. IoT Architecture: Introduction <b>T Reference Architecture Views</b> ntroduction - Functional View - Information View Relevant Architectural Views. Participatory Sensing - Participatory Sensing Process - Technology Overv modern Example.	An A abiliti - Dep ng: In view	Sche 18 Ad Ho Netw Appro- Dility 18 Archite es - A e of t 18 Notw Appro- 18 Network Appro- 18 Net	hou oc an vorks oach - hou ectur An Id he hou ent ction	rs nd s - es rs cal oT <b>rs</b>				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introduction Overview: H Architecture Art. Unit:4 IoT Reference and Operation - Roles, Acto Scenario - Re Unit:5 Mobile Sec	ng. Mobile iddleware: Intro works: Propertie pplications. Cha ns: Deployment a ciency. on - From M2M Building an Arch e Outline. Standa Io' e Architecture: I nal View - Other rs, Engagement ecent Trends - A Me curity: Overview	Data Dissemination - Data Caching - Cache mainter         e middleware and Networking Challenges         duction - Adaptation - Agents - Service Discoveres         s of an Ad Hoc Network - Unique Features of Security - Mobile         and Configuration - Routing - Fault Tolerance and I         Mobile and IoT         to IoT - M2M towards IoT the global context.         nitecture - Main design Principles and Needed Capater         ords Considerations. IoT Architecture: Introduction         T Reference Architecture Views         ntroduction - Functional View - Information View         • Relevant Architectural Views. Participatory Sensing         • Participatory Sensing Process - Technology Overvice         • Obile communication and Security         • of Mobile Communication: Introduction - Basics of	An A abiliti - Dep ng: In view	Sche 18 Ad Ho Netw Appro- pility 18 archite es - A te of t 18 bloym trodu - An e 18 bile	mes hou oc ar vorks oach - hou ectur An Io he hou ent ction early hou	rs nd s - es rs cal oT <b>rs</b>				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introductio Overview: H Architecture Art. Unit:4 IoT Referenc and Operation - Roles, Acto Scenario - Re Unit:5 Mobile Sec Communica	Mobile         iddleware: Intro         works: Propertie         pplications. Chans: Deployment a         ciency.         on - From M2M         Building an Arch         e Outline. Standa         Io'         e Architecture: I         nal View - Other         rs, Engagement         ecent Trends - A         Me         curity: Overview         utions - Wireless	Data Dissemination - Data Caching - Cache mainter         e middleware and Networking Challenges         duction - Adaptation - Agents - Service Discoveres         s of an Ad Hoc Network - Unique Features of Security - Mobile         and Configuration - Routing - Fault Tolerance and I         Mobile and IoT         to IoT - M2M towards IoT the global context.         nitecture - Main design Principles and Needed Capards Considerations. IoT Architecture: Introduction         T Reference Architecture Views         ntroduction - Functional View - Information View         Participatory Sensing Process - Technology Overwordern Example.         obile communication and Security         of Mobile Communication: Introduction - Basics of Vulnerabilities and Threats - Attacks in Mobile Environment	An A abiliti - Dep ng: In view	Sche 18 Ad Ho Netw Appro- pility 18 Archite es - A trodu - An o 18 bile ments	hou oc an vorks oach - he ectur An Ic he ent ction early hou	rs nd s - es rs cal oT rs n rs				
Web Cachin Unit:2 Mobile Mi Sensor Netw Proposed A and Solution Energy Effic Unit:3 Introductio Overview: H Architecture Art. Unit:4 IoT Referenc and Operation - Roles, Acto Scenario - Re Unit:5 Mobile Sec Communica	In the second se	Data Dissemination - Data Caching - Cache mainter         e middleware and Networking Challenges         duction - Adaptation - Agents - Service Discoveres         s of an Ad Hoc Network - Unique Features of Security - Mobile         and Configuration - Routing - Fault Tolerance and I         Mobile and IoT         to IoT - M2M towards IoT the global context.         nitecture - Main design Principles and Needed Capater         ords Considerations. IoT Architecture: Introduction         T Reference Architecture Views         ntroduction - Functional View - Information View         • Relevant Architectural Views. Participatory Sensing         • Participatory Sensing Process - Technology Overvice         • Obile communication and Security         • of Mobile Communication: Introduction - Basics of	An A abiliti - Dep ng: In view	Sche 18 Ad Ho Netw Appro- pility 18 Archite es - A trodu - An o 18 bile ments	hou oc an vorks oach - he ectur An Ic he ent ction early hou	rs rs rs ral oT rs rs rs				

U	J <b>nit:6</b>	Contemporary Issues	2 hours							
Stu	dy: Comn	nercial Building Automation: Phase one - Phase Two.								
		Total Lecture hours	92 hours							
Text Book(s)										
1 Fundamentals of Mobile and Pervasive Computing, Golden G. Richard III, Frank										
	Adelste	ein, Sandeep K. S. Gupta, Loren Schweibert, McGraw-Hill 2005								
2	. Fron	n Machine-to-Machine to the Internet of Things: Introduction to N	New Age of							
	Intellig	ence, Jan Ho <sup></sup> ller, VlasiosTsiatsis, Catherine Mulligan, StamatisK	Karnouskos, Stefan							
		d, David Boyle, Elsevier,2014								
3	Secur	ty Of Mobile Communication, NoureddineBoudriga, CRC Press,	2010							
-										
ŀ		nline Contents [MOOC, SWAYAM, NPTEL, Websites etc.]								
1	<u>https://o</u>	nlinecourses.nptel.ac.in/noc20_cs21/preview_								
2	https://n	ptel.ac.in/courses/106/105/106105166/								
3	https://w	ww.coursera.org/learn/security-awareness-training								
V	Veb Link									
1.		s.norton.com/internetsecurity-iot-securing-the-internet-of-things.l	<u>html</u>							
2.	https://w	/www.allot.com/service-providers/iot-security-solutions/								
C	Course De	signed By: Mr. S.Palanisamy& CSCC Labs								

	Mappin	g with <b>F</b>	Program	me Outo	comes					
Cos	PO1	PO2	PO3	PO4	PO5	PO6	<b>PO7</b>	PO8	PO9	PO10
CO1	S	S	М	S	L	М	S	М	М	S
CO2	S	M	М	М	L	М	S	М	М	S
CO3	S	M	М	М	S	Μ	S	М	Μ	S
CO4	S	S	S	S	S	М	S	М	S	S
CO5	S	S	S	S	S	S	S	S	S	S
CO6	S	S	S	S	S	S	S	S	S	S

code	21CSESC09	ADVANCED ETHICAL HACKING AND PENETRATION TESTING	L	Т	Р	C
	ve/Supportive	Core	4	2	2	4
Pre-r	equisite	Computer Networks, OWASP Concepts, and Wireless Standards	Sylla Vers		2021-	-2022
Course C	<b>Objectives:</b>					
The main	objectives of th	is course are to:				
		basics of penetration tools andmethodolog				
		ge in analyzing the vulnerabilities and atta	cks of	syster	n	
3. To	get familiar on t	the process of phishingattacks				
Exported	Course Outco	mag				
		etion of the course, student will be able to:				
		it the vulnerabilities and the weakness of s			K1.	, K2
	enetration testin		y stem		111	, 112
01		cripting for connecting to a port for scanni	ng the			
	k and host.				K6	
		ulnerabilities with wireless attacks and				
	tion process				K4	
		s of phishing attacks and the security level				-K4
		te the web application vulnerabilities and	the			-K5
-	with SQL Inject		A		K6	
K1 - Reme	nber; <b>K2</b> - Unde	erstand; <b>K3</b> - Appl <mark>y; K4</mark> - Analyze; K5 - I	Evalua	te; K	6 –Cre	ate
<b>T</b> T <b>1</b> / 4	<b>.</b>		_	34	10 1	
Unit:1		oduction to Penetration Testing				
T., 4.,	Durant's		771		<u>18—h</u>	
		n and Creating a Penetration Testing Lab		use a	nd cre	ation
of hacking	lab – Setting u	n and Creatin <mark>g a Pe</mark> netration Testing Lab 1p Virtual La <mark>b – U</mark> sing Kali Linux – Pro	gramn	use a ning -	nd cre - Usin	ation g the
of hacking Metasploit	lab – Setting u framework –	n and Creatin <mark>g a Penetration Testing Lab</mark> 1p Virtual Lab – Using Kali Linux – Pro - Phases of Penetration testReconnais	gramn sance	use a ning - – S	nd cre - Usin cannir	atior g the 1g –
of hacking Metasploit Exploitatio	i lab – Setting v framework – on – Maintaining	n and Creatin <mark>g a Pe</mark> netration Testing Lab 1p Virtual La <mark>b – U</mark> sing Kali Linux – Pro	gramn sance	use a ning - – S	nd cre - Usin cannir	ation g the 1g –
of hacking Metasploit Exploitatio	lab – Setting u framework –	n and Creatin <mark>g a Penetration Testing Lab</mark> 1p Virtual Lab – Using Kali Linux – Pro - Phases of Penetration testReconnais	gramn sance	use a ning - – S	nd cre - Usin cannir	ation g the 1g –
of hacking Metasploit Exploitatic backdoors	ab – Setting v framework – n – Maintaining and rootkits.	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main	gramn sance	use a ning - - S g Acc	nd cre Usin cannir cess wi	ation g the ng – ith
of hacking Metasploit Exploitatio backdoors Unit:2	i lab – Setting v framework – on – Maintaining and rootkits. Informa	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main tion Gathering and Vulnerabilities	gramn sance ntainin	use a ning - - S g Acc	nd cre - Usin cannir cess wi	ation g the ng – ith ours
of hacking Metasploit Exploitatio backdoors Unit:2 Netcraft	i lab – Setting v framework – on – Maintaining and rootkits. Informa – WhoisLookU	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main tion Gathering and Vulnerabilities p – DNS Reconnaissance – Searching t	gramn sance ntainin	use a ning - g Acc nail A	nd cre Usin cannir cess wi 18—h	ation g the ng – ith ours ses -
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. 1	lab – Setting u framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main tion Gathering and Vulnerabilities p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning –	gramn sance ntainin for En – Port	use a ning - S g Acc nail A sca	nd cre - Usin cannir ess wi 18—h Addres nning	ation g the ng - ith ours ses - with
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. Net	i lab – Setting v framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main tion Gathering and Vulnerabilities p – DNS Reconnaissance – Searching t	gramn sance ntainin for En – Port	use a ning - S g Acc nail A sca	nd cre - Usin cannir ess wi 18—h Addres nning	ation g the ng - ith ours ses - with
of hacking Metasploit Exploitatio backdoors Unit:2 Netcraft Maltego. 1 Nmap. Net Nmap Scri	lab – Setting u framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines –	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vu Metasploit Scanner Modules.	gramn sance ntainin for En – Port	use a ning - g Acc nail A sca pilities	nd cre - Usin cannir cess wi sess wi 18—h Addres nning s –The	ation g the ith ours ses - with
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. Nes Nmap Scrite Unit:3	ab – Setting u framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines –	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main tion Gathering and Vulnerabilities p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vu Metasploit Scanner Modules.	gramn sance ntainin for En - Port Inerab	use a ning - g Acc nail A sca jilities	nd cre - Usin cannir cess wi 18—h Addres nning s – The 18—h	ation g the ng – ith ours ses – with
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. Net Nmap Scrit Unit:3 Exploitat	lab – Setting v framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines – W ion – Metasplo	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vul Metasploit Scanner Modules. <b>Tires and Wireless Attacks</b> bit payloads – Running a script on the	gramn sance ntainin for En - Port Ilnerab	use a ning - S g Acc nail A sca pilities	nd cre Usin cannir cess wi 18—h Addres nning s –The 18—h o serv	ation g the ng – ith ours ses – with ours er –
of hacking Metasploit Exploitatio backdoors Unit:2 Netcraft Maltego. I Nmap. Nes Nmap Scri Unit:3 Exploitat Password	lab – Setting v framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines – W ion – Metasplo attacks – Clien	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vu Metasploit Scanner Modules. <b>Tires and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS	gramn sance ntainin for En - Port Inerat	use a ning - Sg Acc nail A sca pilities	nd cre - Usin cannir cess wi 18—h Addres nning s – The 18—h o serv – Wir	ation g the ig - ith ours ses - with ours er - eless
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. Nes Nmap Scrit Unit:3 Exploitat Password attacks: V	ab – Setting u framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines – W ion – Metasplo attacks – Clien iewing and scar	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vul Metasploit Scanner Modules. <b>Tres and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS nning for available access points – Captu	gramn sance ntainin for En - Port linerab	use a ning - g Acc g Acc nail A sca pilities t wel pads packe	nd cre Usin cannir cass wi 18—h Addres nning 5 —The 18—h 5 serv - Wirt ts – W	ation g the ng – ith ours ses – with ours er – eless /ired
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. Net Nmap Scrit Unit:3 Exploitat Password attacks: Vi equivalent	lab – Setting v framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines – W ion – Metasplo attacks – Clien iewing and scar privacy – WiFi	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vul- Metasploit Scanner Modules. <b>Tres and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS nning for available access points – Captur Protected access – WPA2 – The Enterprise	gramn sance ntainin for En - Port linerab	use a ning - g Acc g Acc nail A sca pilities t wel pads packe	nd cre Usin cannir cass wi 18—h Addres nning 5 —The 18—h 5 serv - Wirt ts – W	ation g the ng – ith ours ses – with ours er – eless /ired
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. Net Nmap Scrit Unit:3 Exploitat Password attacks: Vi equivalent	lab – Setting v framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines – W ion – Metasplo attacks – Clien iewing and scar privacy – WiFi	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vul Metasploit Scanner Modules. <b>Tres and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS nning for available access points – Captu	gramn sance ntainin for En - Port linerab	use a ning - g Acc g Acc nail A sca pilities t wel pads packe	nd cre Usin cannir cass wi 18—h Addres nning 5 —The 18—h 5 serv - Wirt ts – W	ation g the ng – ith ours ses – with ours er – eless /ired
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. Net Nmap Scrit Unit:3 Exploitat Password attacks: V equivalent – The pers	lab – Setting v framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines – W ion – Metasplo attacks – Clien iewing and scar privacy – WiFi	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to <b>vork Scanning:</b> Manual port scanning – Exporting Nessus results – Researching Vul Metasploit Scanner Modules. <b>Tres and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS nning for available access points – Captu Protected access – WPA2 – The Enterprise process – WiFi protected setup.	gramn sance ntainin for En - Port linerab	use a ning - S g Acc nail A sca pilities ot wel packe nectio	nd cre Usin cannir cess wi 18—h Addres nning 5 – The 18—h 5 serv - Wirt ts – Wirt ts – Wirt	ation g the ig - ith ours ses - with ours er - eless /ired cess
of hacking Metasploit Exploitatio backdoors Unit:2 Netcraft Maltego. I Nmap. Nes Nmap Scri Unit:3 Exploitat Password attacks: V equivalent – The pers	<ul> <li>lab – Setting u framework – on – Maintaining and rootkits.</li> <li>Informa – WhoisLookU Host and Netw ssus policies – E pting Engines –</li> <li>W ion – Metasplo attacks – Clien iewing and scar privacy – WiFi onal connection</li> </ul>	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vu Metasploit Scanner Modules. <b>Tres and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS nning for available access points – Captu Protected access – WPA2 – The Enterpriss process – WiFi protected setup. <b>Social Engineering</b>	gramn sance ntainin for En - Port llnerab	use a ning - S g Acc nail A sca pilities ot wel pads packe nectio	nd cre Usin, cannir cess wi 18—h Addres nning 5 –The 18—h 5 serv – Wird ts – W on Prod	ation g the ng - ith ours ses - with ours er - eless /ired cess
of hacking Metasploit Exploitatio backdoors Unit:2 Netcraft Maltego. I Nmap. Nes Nmap Scri Unit:3 Exploitati Password attacks: V equivalent – The pers Unit:4 The Socia	lab – Setting v framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines – W ion – Metasplo attacks – Clien iewing and scar privacy – WiFi onal connection	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vu Metasploit Scanner Modules. <b>Tres and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS nning for available access points – Captu Protected access – WPA2 – The Enterprise process – WiFi protected setup. <b>Social Engineering</b> polkit – Spear Phishing attacks – choosing	gramn sance ntainin for En - Port linerab range Payle uring p se Con	use a ning - S g Acc g Acc nail A sca pilities ot wel packe nectic	nd cre Usin cannir cannir cess wi 18—h Addres nning a—The 18—h o serv Wird ts — Wird ts — Wird ts — Wird ts — Wird ts — Wird ts — Creati	ation g the ng – ith ours ses – with ours er – eless /ired cess ours ing a
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. Net Nmap Scrit Unit:3 Exploitati Password attacks: V equivalent – The pers Unit:4 The Socia template –	lab – Setting v framework – on – Maintaining and rootkits. Informa – WhoisLookU Host and Netw ssus policies – E pting Engines – W ion – Metasplo attacks – Clien iewing and scar privacy – WiFi onal connection	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>Stion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning Exporting Nessus results – Researching Vu Metasploit Scanner Modules. <b>Sires and Wireless Attacks</b> it payloads – Running a script on the t side exploitation – HTTP and HTTPS uning for available access points – Captu Protected access – WPA2 – The Enterprise process – WiFi protected setup. <b>Social Engineering</b> polkit – Spear Phishing attacks – choosing mail – setting up target and listener – web	gramn sance ntainin for En - Port linerab range Payle uring p se Con	use a ning - S g Acc g Acc nail A sca pilities ot wel packe nectic	nd cre Usin cannir cannir cess wi 18—h Addres nning a—The 18—h o serv Wird ts — Wird ts — Wird ts — Wird ts — Wird ts — Wird ts — Creati	ation g the ng – ith ours ses – with ours er – eless /ired cess ours ing a
of hacking Metasploit Exploitatio backdoors Unit:2 Netcraft Maltego. I Nmap. Nes Nmap Scri Unit:3 Exploitati Password attacks: V equivalent – The pers Unit:4 The Socia template – attacks – N	<pre>I lab – Setting v framework – on – Maintaining and rootkits. Informa - WhoisLookU Host and Network ssus policies – E pting Engines – iewing Engines – W ion – Metasplo attacks – Clien iewing and scar privacy – WiFi onal connection al Engineering to single or mass in fultipronged attactactactactactactactactactactactacta</pre>	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro- Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vu Metasploit Scanner Modules. <b>Tres and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS nning for available access points – Captu Protected access – WPA2 – The Enterprise process – WiFi protected setup. <b>Social Engineering</b> polkit – Spear Phishing attacks – choosing mail – setting up target and listener – web acks	gramn sance ntainin for En - Port linerab range Payle uring p se Con	use a ning - S g Acc g Acc nail A sca jilities of wel oads oacke nectio	nd cre Usin, cannir cass wi 18—h Addres nning 5 – The 18—h o serv – Wird ts – Wird ts – Wird ts – Wird ts – Wird ts – Creati ass em	ation g the ng - ith ours ses - with ours er - eless /ired cess ing a nail
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. New Nmap Scrit Unit:3 Exploitation Password attacks: V equivalent – The pers Unit:4 The Sociate template – attacks – N	alb – Setting u framework – on – Maintaining and rootkits.           Informa           - WhoisLookU           Host and Netw           ssus policies – E           pting Engines –           Wion – Metasplo           attacks – Clien           iewing and scar           privacy – WiFi           onal connection           Al Engineering to           single or mass r           Multipronged attacks	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>Ation Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning Exporting Nessus results – Researching Vu Metasploit Scanner Modules. <b>Tres and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS aning for available access points – Captu Protected access – WPA2 – The Enterpriss process – WiFi protected setup. <b>Social Engineering</b> polkit – Spear Phishing attacks – choosing mail – setting up target and listener – web acks	gramn sance ntainin for En - Port llnerab a targe B Payle uring J se Con	use a ning - S g Acc g Acc nail <i>A</i> sca bilities bt wel bads backe nectic load - s - M	nd cre - Usin, cannir cess wi 18—h Addres nning - The 18—h o serv - Wird ts – Wird ts – Wird ts – Wird ts – Wird ts – Wird ts – Creati ass em	ation g the ng – ith ours ses - with ours er – eless /ired cess ours ing a nail
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. Nes Nmap Scrit Unit:3 Exploitat Password attacks: V equivalent – The pers Unit:4 The Sociat template – attacks – M Unit:5 Using bu	alb – Setting u framework – on – Maintaining and rootkits.           Informa           Informa           WhoisLookU           Host and Netw           ssus policies – E           pting Engines –           W           ion – Metasplo           attacks – Clien           iewing and scar           privacy – WiFi           onal connection           al Engineering to           Single or mass r           fultipronged attacts           Web           up proxy – St	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vu Metasploit Scanner Modules. <b>ires and Wireless Attacks</b> it payloads – Running a script on the t side exploitation – HTTP and HTTPS ming for available access points – Captu Protected access – WPA2 – The Enterprise process – WiFi protected setup. <b>Social Engineering</b> polkit – Spear Phishing attacks – choosing mail – setting up target and listener – web acks <b>Application Vulnerabilities</b> QL Injection – Testing for SQL Injection	gramn sance ntainin for En - Port Inerab	use a ning - S g Acc g Acc nail A sca jilities oads oacke nectio load - s - M	nd cre Usin, cannir cass wi 18—h Addres nning 5 – The 18—h o serv – Wird ts – W on Prod 18—h - creati ass em 18—h	ation g the ng ith ours ses with ours er eless /ired cess ours ing a nail
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. New Nmap Scrit Unit:3 Exploitati Password attacks: V equivalent – The pers Unit:4 The Sociation template – attacks – N Unit:5 Using bu Exploiting	<pre>i lab – Setting u framework – on – Maintaining and rootkits.  Informa WhoisLookU Host and Netw ssus policies – E pting Engines – Wi on – Metasplo attacks – Clien iewing and scar privacy – WiFi onal connection al Engineering to single or mass r fultipronged attack Web up proxy – Se using SQLMap</pre>	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro- Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning Exporting Nessus results – Researching Vu Metasploit Scanner Modules. <b>Tres and Wireless Attacks</b> bit payloads – Running a script on the t side exploitation – HTTP and HTTPS nning for available access points – Captu Protected access – WPA2 – The Enterprise process – WiFi protected setup. <b>Social Engineering</b> polkit – Spear Phishing attacks – choosing mail – setting up target and listener – web acks <b>Application Vulnerabilities</b> QL Injection – Testing for SQL Injector – Captul Articles (SQL Injector) – Social Articles (SQL Injector) – Social Articles (SQL Injector) – Local and Remote	gramn sance ntainin for En - Port Inerab range Payle uring p se Con se Con g a pay attack	use a ning - S g Acc g Acc nail A sca oilities oacke nectio load - s - M vulne clusio	nd cre Usin cannir cannir cess wi 18—h Addres nning a –The 18—h o serv – Wird ts – Won Proce 18—h - creati ass err 18—h rabiliti on – C	ation g the ng - ith ours ses - with ours er - eless /ired cess ing a hail ours es - cross-
of hacking Metasploit Exploitation backdoors Unit:2 Netcraft Maltego. I Nmap. New Nmap Scrit Unit:3 Exploitati Password attacks: V equivalent – The pers Unit:4 The Sociation template – attacks – N Unit:5 Using bu Exploiting	<pre>i lab – Setting u framework – on – Maintaining and rootkits.  Informa WhoisLookU Host and Netw ssus policies – E pting Engines – Wi on – Metasplo attacks – Clien iewing and scar privacy – WiFi onal connection al Engineering to single or mass r fultipronged attack Web up proxy – Se using SQLMap</pre>	n and Creating a Penetration Testing Lab p Virtual Lab – Using Kali Linux – Pro Phases of Penetration testReconnais g Access – Web based Exploitation – Main <b>tion Gathering and Vulnerabilities</b> p – DNS Reconnaissance – Searching to vork Scanning: Manual port scanning – Exporting Nessus results – Researching Vu Metasploit Scanner Modules. <b>ires and Wireless Attacks</b> it payloads – Running a script on the t side exploitation – HTTP and HTTPS ming for available access points – Captu Protected access – WPA2 – The Enterprise process – WiFi protected setup. <b>Social Engineering</b> polkit – Spear Phishing attacks – choosing mail – setting up target and listener – web acks <b>Application Vulnerabilities</b> QL Injection – Testing for SQL Injection	gramn sance ntainin for En - Port Inerab range Payle uring p se Con se Con g a pay attack	use a ning - S g Acc g Acc nail A sca oilities oacke nectio load - s - M vulne clusio	nd cre Usin cannir cannir cess wi 18—h Addres nning a –The 18—h o serv – Wird ts – Won Proce 18—h - creati ass err 18—h rabiliti on – C	ation g the ng - ith ours ses - with ours er - eless /ired cess ing a hail ours es - cross-

Unit:6	iit:6 Contemporary Issues 2 hours								
The stage of	f risk, Data Asset, Affect the confidentiality, Integrity – Des	struction – Disclosure							
<ul> <li>Modificat</li> </ul>	ion – Corruption of Data – Viruses and Malwares – Cyber A	Attacks –							
Misconfigu	ration – Risk Assessment.								
	Total Lecture hours	92—hours							
Text Boo	k(s)								
1 Dafy	ddStuttard, Marcus Pinto, "The Web Application Hacker"s	Handbook" Finding							
and E	xploiting Security Flaws, Second edition, Wiley Publishing	, Inc.,2011							
2 Geor	gia Weidman, "Penetration Testing", A Hands-On Introduc	tion to Hacking, 2014							
Referenc	e Books : EBooks								
1 Patri	ck Engenretson, "The Basics of Hacking Penetration Testin	g" Ethical Hacking							
and P	enetration T <mark>esting Made</mark> Easy, Second Edition, Syngress, 20	013.							
2 94	A McClaure La L Construction Construction Windows With the France	- 1 7. N 4							
	rt McClure, Joel Scambray, George Kurtz, "Hacking Expos	ed /: Network							
Secur	ity Secrets and Solutions, 2012.								

	Course Title	Duration	Provider
1.	Advanced Ethical Hacking	6 hours	Udemy
2.	Penetration Testing and Ethical Hacking(Free)	23 hours	Cybrary
3.	Ethical Hacking	12 Weeks	SWAYAM
4.	Hacking and Patching Certification by University	5 Weeks	Coursera
	of Colorado	and the second se	
5.	The complete Ethical Hacking Course	24.5 hours	Udemy
6.	Become an Ethical Hacker (Free)	32 hours	LinkedIn
	ALL THE THE PARTY AND A DECEMBER OF A DECEMBER		Learning
Wel	) link		
1.	http://www.cybersecurityafrica.com/advanced-ethical-ha	<u>cking.html</u>	
2.	https://www.digital4nxgroup.com/advanced-ethical-hack	ing/	
3.	https://gicseh.com/blog.php		
4.	https://www.isoeh.com/exclusive-blog.html		

Course Designed by: Prof. T. Devi and CSCC Labs

Map	Mapping with Programme Outcomes												
Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10			
CO1	M	L	S	L	L	L	L	L	L	L			
CO2	L	М	S	S	L	L	L	L	L	L			
CO3	L	L	S	S	М	L	L	L	L	L			
CO4	L	L	L	S	S	L	L	L	L	L			
CO5	L	L	L	L	L	L	S	L	L	L			

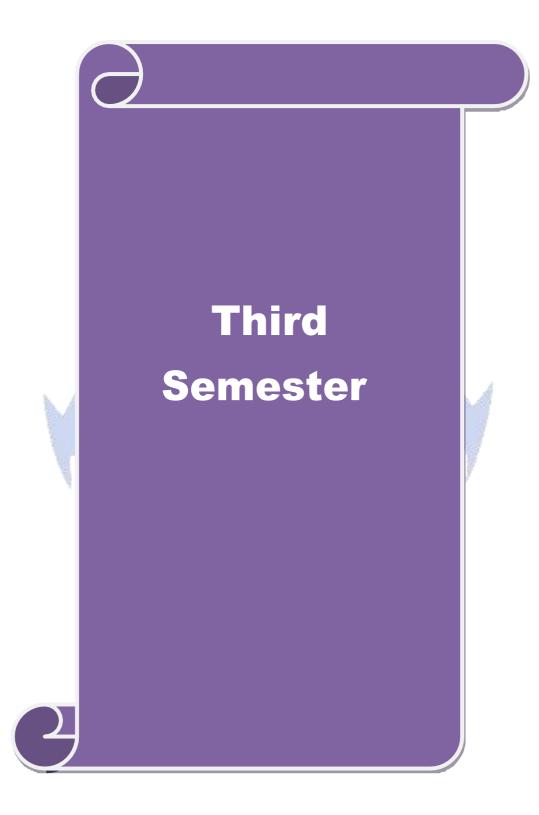
\*S-Strong; M-Medium; L-Low

**N** A

Course code       21CSESC10       Information Systems Risk Management       L       T         Core/Elective/Supportive       Core       4       4         Pre-requisite       Security Standards, Threat, Vulnerability, Risk and Audit Frameworks       Syllabus Version         Course Objectives:       Security Standards, Threat, Vulnerability, Risk and Audit Frameworks       Syllabus Version         Course Objectives:       Security Standards, Threat, Vulnerability, Risk and Audit Frameworks       Syllabus Version         The main objectives of this course are to:       1.       To understand the impacts of Information Systems.       2.         To identify the Risk factors by using Information Security.       Expected Course Outcomes:       Image: Course Outcomes:       Image: Course Outcomes:         On the successful completion of the course, student will be able to:       Image: Course Outcomes:       Image: Course Outcomes:         2       Analyze your integrity & availability of information Systems Risk Management Security       Security       Image: Course Outcomes:         2       Analyze your integrity & availability of information system risks.       Image: Course Outcomes:       Image: Course Outcomes:         3       Demonstrate the organization and system level securities and explain risk management framework concepts       Image: Course Outcomes:       Image: Course Outcomes:         4       Understand the basic knowl			Т	Р	C	
Core/Electi	ve/Supportive	Core	4			4
Pre-r	equisite		•		202 202	
Course O	bjectives:	•				
		· ·				
2. To i	dentify the Risk f	factors by using Information Security.				
	<u> </u>					
<u> </u>						
	1					
		knowledge in Information Systems Risk Manag	gement		K1	
	<i>v</i>	v & availability of information system risks			K2	
			risk		K2 K3	
			115K			
		*			K3/K6	5
			nent the	e	K4/K	5
				. ~		
K1 - Unde	rstand; <b>K2</b> - Rem	ember; <b>K3</b> – Analyze; <b>K4</b> - Apply; <b>K5</b> - Evalua	ate; K6	-C	reate	
TT		Information Annualization	a.			
Introduction	n Risk – Inform	Information: An overview - Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an	ing R	Mana isk ·	<b>12hou</b> Igemer – Sim	nt - nple
Informatio Introduction Statistical c Risk Asses Concepts - Likelihood Assessment	n Risk – Inform alculation and P sments - Risk M Risk Models - Ri	- Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz Parameters - PERT Technique - Analysing an Management Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple nent Hierarchy	ting R d Asse ponent sposing	Mana isk ssin s - ] g Coi	<b>12hou</b> Igemer – Sim g Risk Key R nditior	nt - nple ks - Risk
Informatio Introduction Statistical c Risk Assess Concepts - Likelihood	n Risk – Inform alculation and P sments - Risk M Risk Models - Ri – Impact – Risk -	- Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an Ianagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Appl	ting R d Asse ponent sposing	Mana isk ssin s - ] g Con ofR	<b>12hou</b> Igemer – Sim g Risk Key R nditior	nt - iple ks - kisk is -
Informatio Introduction Statistical c Risk Asses Concepts - Likelihood Assessment <b>Unit:2</b> Maintainin	a Risk – Inform calculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme	- Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz Parameters - PERT Technique - Analysing an Management Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple nent Hierarchy Risk Assessment ent - Information Risk Management Criteria -	ving R d Asse ponent sposing ication Risk I	Mana isk ssin s - 1 g Con ofR denti	12hou agemen - Sim g Risk Key R nditior isk 12hou ficatio	nt - nple (s - Cisk ns - <b>rs</b> (n -
Informatio Introduction Statistical c Risk Assess Concepts - Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys	n Risk – Inform alculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessma sis and Risk Eva	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz Parameters - PERT Technique - Analysing an Management Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and</li> </ul>	ting R d Asso ponent sposing ication Risk I Prese	Mana isk ssin s - ] g Cor ofR denti ntatio	12hou ngemen – Sim g Risk Key R nditior isk 12hou ficatio on – R	nt - ple (isk (isk (isk (isk (isk
Informatio Introduction Statistical of Risk Assess Concepts - Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring	a Risk – Inform calculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managerr g Risk Assessme sis and Risk Eva and Review - Or	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Enter Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach</li> </ul>	ting R d Asse ponent sposing ication Risk I Prese - Risk	Mana isk ssin s - ] g Cor ofR denti ntatio	12hou Igemen g Risk Key R Idition isk 12hou fication fication n – R nagem	nt - aple as - lisk ns - <b>rs</b> on - ask aent
Informatio Introduction Statistical c Risk Assess Concepts - Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework	a Risk – Inform calculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - On - Executing RMI	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen</li> </ul>	ting R d Asse ponent sposing ication Risk I Prese - Risk 1 Leve	Vlana isk ssin s - ] g Cor ofR denti denti ntatio 1 - C	12hou agemen – Sim g Risk Key R nditior isk 12hou ficatic on – R nagem Categor	nt - aple as - Aisk ns - <b>rs</b> on - Aisk nent
Informatio Introduction Statistical of Risk Assess Concepts - 1 Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Selec	A Risk – Inform calculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - On - Executing RMI ct Task - Imple	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz Parameters - PERT Technique - Analysing an Management Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task</li> </ul>	ting R d Asse ponent sposing ication Risk I Prese - Risk n Leve c - Ma	Vana isk ssin s - 1 g Con ofR denti ntation Ma 1 - Conito	12hou Igemen J Sim G Risk Key R Idition isk 12hou fication	nt - ple ss - tisk s - <b>rs</b> <b>rs</b> <b>rs</b> tisk hent rize k -
Informatio Introduction Statistical of Risk Assess Concepts - Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Seleo Information	A Risk – Inform calculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - On - Executing RMI ct Task - Imple	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task vacy in RMF - Requirements and Controls - Se</li> </ul>	ting R d Asse ponent sposing ication Risk I Prese - Risk n Leve c - Ma	Vana isk ssin s - 1 g Con ofR denti ntation Ma 1 - Conito	12hou Igemen J Sim G Risk Key R Idition isk 12hou fication	nt - ple ss - tisk s - <b>rs</b> <b>rs</b> <b>rs</b> tisk hent rize k -
Informatio Introduction Statistical of Risk Assess Concepts - Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Seleo Information	A Risk – Inform calculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - On - Executing RMI ct Task - Imple Security and Pri	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task vacy in RMF - Requirements and Controls - Se</li> </ul>	ting R d Asse ponent sposing ication Risk I Prese - Risk n Leve c - Ma	Vana isk ssin s - 1 g Con ofR denti ntatio Ma 1 - C onito and I	12hou Igemen J Sim G Risk Key R Idition isk 12hou fication	nt - ple ss - tisk ns - <b>rs</b> <b>rs</b> on - tisk nent rize k - y
Informatio Introduction Statistical c Risk Assess Concepts - Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Selec Information Posture - Su <b>Unit:3</b>	A Risk – Inform calculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - On - Executing RMI ct Task - Imple Security and Pri upply Chain Risk n Security Kn	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>Risk Assessment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task vacy in RMF - Requirements and Controls - Se Management</li> <li>Information Security</li> <li>owledge - Brief History - SystemAdmin</li> </ul>	cing R d Asse ponent sposing ication Risk I Prese - Risk n Leve c - M curity	Vana isk essin s - ] g Con ofR denti ntatio 1 - C onito and H	12hou Igemen J Sim g Risk Key R nditior isk 12hou ficatic on – R nagem categolor r Tas Privacy 14hou Syst	nt - pple (ss - Cisk (ss - (ss -
Informatio Introduction Statistical c Risk Assess Concepts - I Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Select Information Posture - Su <b>Unit:3</b> Informatio	A Risk – Inform calculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - On - Executing RMI ct Task - Imple Security and Pri- pply Chain Risk n Security Kne ion Utilities - Op	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task vacy in RMF - Requirements and Controls - Se Management</li> <li>Information Security</li> <li>owledge - Brief History - SystemAdmin perating System Structure - The command-line</li> </ul>	cing R d Asse ponent sposing ication Risk I Prese - Risk 1 Leve c - Me curity : istratic	Vana isk ssin s - 1 g Con ofR denti ntatio 1 - C onito and H on - ace -	12hou Igemen – Sim g Risk Key R nditior isk 12hou ficatic on – R nagem Categor r Tas Privacy 14hou Syst Files	nt - nple as - Aisk ns - <b>rs</b> on - Aisk nent rize k - y <b>rs</b> tem
Informatio Introduction Statistical of Risk Assess Concepts - 1 Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Select Information Posture - Su <b>Unit:3</b> Informatio Administrat Directories	A Risk – Inform alculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - Or - Executing RMH ct Task - Imple Security and Pri upply Chain Risk n Security Kno ion Utilities - Or -Moving around	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task vacy in RMF - Requirements and Controls - Se Management</li> <li>Information Security</li> <li>owledge - Brief History - SystemAdmin perating System Structure - The command-line the filesystem – pwd, cd - Listing files and dire</li> </ul>	cing R d Asse ponent sposing ication Risk I Prese - Risk 1 Leve c - Me curity : istratic	Vana isk ssin s - 1 g Con ofR denti ntatio 1 - C onito and H on - ace -	12hou Igemen – Sim g Risk Key R nditior isk 12hou ficatic on – R nagem Categor r Tas Privacy 14hou Syst Files	nt - pple (ss - Cisk (ss - (ss -
Informatio Introduction Statistical of Risk Assess Concepts - Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Seleo Information Posture - Su <b>Unit:3</b> Informatio Administrat Directories Expansions	A Risk – Inform alculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - Or - Executing RMH ct Task - Imple Security and Pri upply Chain Risk n Security Kne ion Utilities - Or -Moving around	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task vacy in RMF - Requirements and Controls - Se Management</li> <li>Information Security</li> <li>owledge - Brief History - SystemAdmin perating System Structure - The command-line the filesystem – pwd, cd - Listing files and dire ent - Viewing Files- Searching for files</li> </ul>	cing R d Asse ponent sposing ication Risk I Prese - Risk 1 Leve c - Me curity : istratic	Vlana isk ssin s - 1 g Con ofR denti denti denti ntation 1 - Con on to and H	12hou Igemen J Sim g Risk Key R nditior isk 12hou fication	nt - pple (isk isk s - rs on - Cisk hent rize k - y rs tem and
Informatio Introduction Statistical of Risk Assess Concepts - 1 Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Select Information Posture - Su <b>Unit:3</b> Informatio Administrat Directories Expansions <b>Unit:4</b>	A Risk – Inform alculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - On - Executing RMH ct Task - Imple Security and Pri- pply Chain Risk n Security Kne ion Utilities - Op -Moving around - File Manageme	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task vacy in RMF - Requirements and Controls - Se Management</li> <li>Information Security</li> <li>owledge - Brief History - SystemAdmin perating System Structure - The command-line the filesystem – pwd, cd - Listing files and dire ent - Viewing Files- Searching for files</li> <li>Information Security Model</li> </ul>	cing R d Asse ponent sposing ication Risk I Prese - Risk n Leve c - Me curity s istratic istratic	Vlana isk ssin s - 1 g Con ofR denti ntatio denti ntatio and H on - ace - - Sh	12hou Igemen Jgemen G Risk Key R nditior isk 12hou fication files a files a	nt - pple as - Cisk ns - <b>rs</b> on - Cisk con - Cisk Cisk con - Cisk con - Cisk con - Cisk con - Cisk con - Cisk con - Cisk con - Cisk con - Cisk con - Cisk con - Cisk Cisk con - Cisk con - Cisk con - Cisk con - Cisk Cisk Cisk Cisk Cisk Cisk Cisk Cisk
Informatio Introduction Statistical of Risk Assess Concepts - 1 Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Selec Information Posture - Su <b>Unit:3</b> Informatio Administrat Directories Expansions <b>Unit:4</b> Basic Infor	A Risk – Inform alculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - On - Executing RMH ct Task - Imple Security and Pri- pply Chain Risk n Security Kn- ion Utilities - Op -Moving around - File Manageme rmation Security	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz arameters - PERT Technique - Analysing an fanagement Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task vacy in RMF - Requirements and Controls - Se Management</li> <li>Information Security</li> <li>owledge - Brief History - SystemAdmin perating System Structure - The command-line the filesystem – pwd, cd - Listing files and dire ent - Viewing Files- Searching for files</li> <li>Information Security Model</li> <li>Model - Vulnerabilities, Threats and Controls - Se</li> </ul>	cing R d Asse ponent sposing ication Risk I Prese - Risk n Leve curity istratic interf ctories Acces	Vlana isk ssin s - 1 con ofR denti ntatio 1 - C onito and H on - ace - s cor	12hou Igemen Jgemen	nt - nple as - Cisk ns - <b>rs</b> on - Cisk non - Cisk Cisk Cisk Cisk non - Cisk Cisk Cisk Cisk Cisk Cisk Cisk Cisk
Informatio Introduction Statistical of Risk Assess Concepts - Likelihood Assessment <b>Unit:2</b> Maintainin Risk Analys Monitoring Framework Task -Select Information Posture - Su <b>Unit:3</b> Informatio Administrat Directories Expansions <b>Unit:4</b> Basic Infor	A Risk – Inform alculation and P sments - Risk M Risk Models - Ri - Impact – Risk - s: Risk Managem g Risk Assessme sis and Risk Eva and Review - On - Executing RMI ct Task - Imple Security and Pri- pply Chain Risk n Security Kno- ion Utilities - Op -Moving around to - File Manageme mation Security gement - Access O	<ul> <li>Life Cycle - Who Should Use Information nation Risk Management Needs – Categoriz Parameters - PERT Technique - Analysing an Management Process - Risk Assessment Com sk Factors: Threats - Vulnerabilities and Predis - Aggregation - Assessment Approaches - Apple ent Hierarchy</li> <li>Risk Assessment</li> <li>Risk Assessment</li> <li>ent - Information Risk Management Criteria - luation - Risk Treatment - Risk Reporting and rganization-Wide Risk Management Approach F Tasks - Prepare Task: Organization / Systen ment Task - Assess Task - Authorize Task vacy in RMF - Requirements and Controls - Se Management</li> <li>Information Security</li> <li>owledge - Brief History - SystemAdmin perating System Structure - The command-line the filesystem – pwd, cd - Listing files and dire ent - Viewing Files- Searching for files</li> <li>Information Security Model</li> </ul>	cing R d Asse ponent sposing ication Risk I Prese - Risk n Leve c - Mo curity s istratic istratic interf ctories Access	Vlana isk ssin s - 1 con ofR denti ntatio 1 - Con on to and H on - ace - s con - Sh	12hou Igemen J Sim g Risk Key R nditior isk 12hou ficatic on – R nagem categor r Tas Privacy 14hou Syst Files a ell 12hou ntrol an entity	nt - nple as - Cisk ns - <b>rs</b> on - Cisk non - Cisk Cisk Cisk Cisk non - Cisk Cisk Cisk Cisk Cisk Cisk Cisk Cisk

U	Jnit:5	Critical Thinking - Use Cases	10hours
C	ritical Th	inking - Use Cases- Google Executives sentenced to Prison over V	video - Offensive
Су	ber Effec	ts Operations (OCEO) - Risk Estimation Biases - Iraq cyber war p	lans in 2003 -
Us	ses of a Ha	acked PC - Deepfake Attack in 2017 – Social Engineering Attacks	in 2020 – Twitter
		0 – Zoom Credentials up for Sale in 2020 - Zero-day Attacks.	
U	J <b>nit6:</b>	ContemporaryIssues	2 hours
V	Vrite an as	ssignment on Social network security: Issues, challenges, threats, a	nd solution
		Total Lecture hours	62hours
Τ	'ext Book	(s)	
1	Bruce	Newsome, "A Practical Introduction to Security and Risk Manage	ement", First
	Edition	, ISBN: 9781483313405, 2013	
2		Sutton, "Information Risk Management: A practitioner'sguide",	bcsChartered
		e for IT, ISBN: 978-1- 78017-266-1, 2014	
3		al, Atle, Sohaug, "Cyber - Risk Management", First Edition, Sprin	ger International
		ing, ISBN: 978-3-319-23570-7, 2015	
4		h Agrawal, Alex Campoe, Eric Pierce, Information Security and I	
	0	ement, First Edition, Wiley Publisher, ISBN-13: 978-1118335895,	2014
R		nline Conten <mark>ts [MOOC, SWAYAM, NPTEL, We</mark> bsites etc.]	
		ursera.com – Information Security and Risk Management in Conte	
	www.u	<u>idamey.com</u> - Risk Management for Cybersecurity and IT Manage	rs
V	Veb Link		
		//nvlpubs. <mark>nist.go</mark> v/nistpubs/Legacy/SP/nistsp <mark>ec</mark> ialpublication800-3	
		//nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2	2.pdf
C	Course Des	signed By: Prof. M.Punithavalli and CSCC Labs	
	100	Contra Contra 1	

Map	ping wit	h Progra	amme O	utcomes	STATE A	- mark	1. 19	200	1	
Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	<b>PO9</b>	PO10
CO1	L		L.	L	L	L	M	L	L	М
CO2	L	L	L	L	L	L	М	L	L	М
CO3	S	M	М	S S	L	L	S	L	М	S
CO4	S	М	М	S	L	$-L_{con}$	S	L	М	S
CO5	М	М	L	S	L	L	S	L	М	S
*S-Str	ong: M-]	Medium:	L-Low	and the second	1 - 1 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -	3.Ins				



Course code	21CSESC11	EVOLVING TECHNOLOGIES AND THREATS	L	Т	Р	C
	ive/Supportive	Core	4			4
Pre-	requisite	Current and Future Technology Trends	•	abus sion	202 202	
Course O	bjectives:					
The main	objectives of this	course are to:				
1. To une	derstand Web Tec	hnology, Robotics and AutonomousSystem	ns			
		blems associated with bigdata				
3. To ana	alyze and Build B	ig dataApplications				
Expected	Course Outcome	26:				
-		on of the course, student will be able to:				
		curity in web technology			K2	
		problems associated with big data			K4	
		echniques in Big data Applications			K3	
4 Unders	tand the security	violations in Robotics			K2	
5 Unders	tand the security	violations in Autonomous Systems			K2	
<b>K1</b> - Reme	ember; <b>K2</b> - Unde	erstand; <b>K3</b> - Apply; <b>K4</b> - Analyze; <b>K5</b> - Ev	valuate;	; K6 –	Create	)
		and the second				
Unit:1		Advances in web technologies		1	2hour	S
mechanism Semantic V semanticall Ontological	for web session Web Technologie y extending the specification of	Veb Sessions- Special Management of n, management, Implementation and exp s for Access Control- Implementing RE XACML attribute model, Ontology-base f user preferences, Semantic access cor ical access controlmodel.	erimen BAC w d cont	ts. Le vith or ext av	everagi ntologi warene	ng es, ss,
mechanism Semantic V semanticall Ontological networks, E Unit:2	for web session Web Technologie y extending the specification of DEMONS ontolog	n, management, Implementation and exp s for Access Control- Implementing RE XACML attribute model, Ontology-base f user preferences, Semantic access cor ical access controlmodel. Complex & Distributed IT infrastruct	erimen 3AC w ed cont atrol in ure	ts. Le rith or ext av onlin	everagi ntologio warene ne soc	ng es, ss, ial
mechanism Semantic V semanticall Ontological networks, E Unit:2 System Se Established	for web session Web Technologie y extending the specification of DEMONS ontolog curity Engineerin system security e	n, management, Implementation and exp s for Access Control- Implementing RE XACML attribute model, Ontology-base f user preferences, Semantic access cor ical access controlmodel.	arimen BAC we d cont throl in ure y engin	ts. Le rith or ext av onlin	everagi ntologio warene ne soc	ng es, ss, ial rs
mechanism Semantic V semanticall Ontological networks, E Unit:2 System Se Established system secu	for web session Web Technologie y extending the specification of DEMONS ontolog curity Engineerin system security engineering r	n, management, Implementation and exp s for Access Control- Implementing RE XACML attribute model, Ontology-base f user preferences, Semantic access cor ical access controlmodel. Complex & Distributed IT infrastruct g for Information Systems, System securit engineering methods, processes, and tools, nethods, processes, and tools.	arimen BAC we d cont throl in ure y engin	ts. Le ith or ext av onlin 1 neering n and o	everagi ntologio warene ne soc <b>2hour</b> g histor emergi	ng es, ss, ial <b>rs</b> ry, ng
mechanism Semantic W semantically Ontological networks, D Unit:2 System Se Established system secu Unit:3	for web session Web Technologie y extending the specification of DEMONS ontolog curity Engineering system security engineering r	n, management, Implementation and exp s for Access Control- Implementing RE XACML attribute model, Ontology-base f user preferences, Semantic access cor ical access controlmodel. Complex & Distributed IT infrastruct g for Information Systems, System securit engineering methods, processes, and tools, nethods, processes, and tools. Privacy and Identity Theft	erimen BAC we d cont trol in ure y engir Modern	ts. Le ith or ext av onlin neering n and o	everagi ntologi warene ne soc <b>2hour</b> g histor emergi	ng es, ss, ial ry, ng
mechanism Semantic V semantically Ontological networks, E Unit:2 System Se Established system secu Unit:3 Fundamen profiling, a specificatio domains- n Examinatio	for web session Web Technologie y extending the specification of DEMONS ontolog curity Engineering system security engineering r Ital Concepts, De access control r ns, languages and nedical, financial n of privacy matter	n, management, Implementation and exp s for Access Control- Implementing RE XACML attribute model, Ontology-base f user preferences, Semantic access cor ical access controlmodel. Complex & Distributed IT infrastruct g for Information Systems, System securit engineering methods, processes, and tools, nethods, processes, and tools.	erimen AC we d cont ntrol in ure y engin Modern Modern ks, Dav ivacy s, priva es and	ts. Levith or ext avector online online in and online ta lini policionacy in best p	veragi ntologie warene ne soc <b>2hour</b> g histor emergi <b>2hour</b> king a es, the differe	ng es, ss, ial <b>s</b> ry, ng <b>s</b> nd eir es,
mechanism Semantic V semantically Ontological networks, E Unit:2 System Se Established system secu Unit:3 Fundamen profiling, a specificatio domains- n Examinatio Freedom of Unit:4	for web session Web Technologie y extending the specification of DEMONS ontolog curity Engineering system security engineering r tal Concepts, De access control r ns, languages and nedical, financial n of privacy matter Information Act	n, management, Implementation and exp s for Access Control- Implementing RE XACML attribute model, Ontology-base f user preferences, Semantic access cor ical access controlmodel. Complex & Distributed IT infrastruct g for Information Systems, System securit engineering methods, processes, and tools, nethods, processes, and tools. Privacy and Identity Theft efinitions, Statistics, Data Privacy Attac models, role based access control, pr l implementation, privacy policy language , etc Medical privacy legislation, policie ers specific to the World Wide Web, Prote or the requirement for search warrants. Threats of Big Data	erimen AC we d cont introl in ure y engin Modern Modern ks, Dav ivacy es and ctions p	ts. Levith or ext avector online i online online i online i online i online i online	veragi ntologio warene ne soc <b>2hour</b> g histor emergi <b>2hour</b> king a es, the differe practice ed by t	ng es, ss, ial rs ry, ng eir s nd eir es, he
mechanism Semantic V semantically Ontological networks, E Unit:2 System Se Established system secu Unit:3 Fundamen profiling, a specificatio domains- n Examinatio Freedom of Unit:4 An Approa Data Applic integration, Network In based techn Detection: 5	for web session Web Technologie y extending the specification of DEMONS ontolog curity Engineering system security engineering r urity engineering r tal Concepts, De access control r ns, languages and nedical, financial n of privacy matter Information Act cations, UML ext Integrating loca trusion Detection ologies, Survey o System architectu	n, management, Implementation and exp s for Access Control- Implementing RE XACML attribute model, Ontology-base f user preferences, Semantic access cor ical access controlmodel. Complex & Distributed IT infrastruct g for Information Systems, System securit engineering methods, processes, and tools, nethods, processes, and tools. Privacy and Identity Theft efinitions, Statistics, Data Privacy Attac models, role based access control, pr l implementation, privacy policy language , etc Medical privacy legislation, policie ers specific to the World Wide Web, Prote or the requirement for search warrants.	berimen BAC we d cont itrol in ure y engir Modern we we we we we we we we we we we we we	ts. Le ith or ext av onlin 1 neering n and of 1 ta linh polici- acy in best porovide change model icy, H iew or l-time aluatio	everagi ntologie warene ne soc <b>2hour</b> g histor emergi <b>2hour</b> g histor emergi <b>2hour</b> king a es, the differe practice ed by t <b>14hou</b> ge in Bi eling a Real-tin n Hado Intrusi on. CSI	ng es, ss, ial <b>s</b> ry, ng <b>s</b> nd eir es, he <b>urs</b> ig- nd ne on RF

Unit	t:5	<b>Robotics &amp; Autonomous Systems</b>	10hours
Propo	osed Prov	curity Challenges in Cloud Computing, from Infrastructure-Ba visioned Cloud Infrastructure - Infrastructure security, Cloud s ccess control infrastructure (DACI).	•
Unit	t:6	Contemporary Issues	2 hours
Challer	nges in tl	ne development of Chabot, Discuss the issues in Autonomous Sy	stem
		*	
		Total Lecture hours	62 hours
Text B	ook(s)		
	Babak Ak )13	chgar Hamid Arabnia, "Emerging Trends in ICT Security", Morg	an Kaufmann,
		pta Chowdhry, Rahul Verma, Manisha Mathur, "The Evolution of Age: Digital Transformation, Threats, and Security", CRC Press,	
3 S	Seema Ao	charya, SubhashniChellappan, "Big Data Analytics", Wiley, 2013	5.
		on, "Distributed information systems from client / server to distr a",Mcgraw-Hill, 1996	ibuted
		Benson John McAlaney, "Emerging Cyber Threats and Cognitiv ities, Academic Press,2019	ve
Refere	nce Boo	ks : EBo <mark>oks</mark>	
		ber-edge.com/wp- loads/2019/10/RecordedFutureSecondEditioneBook.pdf	
2 <u>h</u>	ttps://pa	per.b <mark>obylive</mark> .com/Security/threat-intellig <mark>en</mark> ce-handbook-second-	edition.pdf
		per.bobylive.com/Security/threat-intelligence-handbook-second- contents [MOOC, SWAYAM, NPTEL, Websites etc.]	edition.pdf

	Course Title	Duration	Provider
1	Big Data Fundamentals (3 – courses) Specialization	6 weeks	IBM
2	Big Data Specialization (6 – courses)	30 weeks	Coursera
3	Cyber Threat Intelligence (IBM)	5 weeks	Coursera
W	eb link Outare m presi		
	1. https://cognitiveclass.ai/learn/big-data		
	2. <u>https://www.fireeye.com/</u>		
	3. <u>https://www.ibm.com/in-en/security</u>		
	4. https://cognitiveclass.ai/courses/robots-are-comin	g	
Cou	urse Designed by: Dr.M. Punithavalli and CSCC Labs		

Map	ping wit	h Progra	amme O	utcomes	5					
COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	L	S	L	Μ	Μ	L	S	S	М	S
CO2	Μ	S	S	S	Μ	L	L	Μ	М	М
CO3	Μ	М	S	S	М	L	Μ	S	S	S
CO4	Μ	Μ	S	S	М	L	Μ	S	S	S
CO5	S	S	S	S	М	М	М	S	S	S

	21CSESC12	SECURITY STANDARDS AND COMPLIANCE	L	Т	Р	С
Core/Electi	ve/Supportive	Core	4			4
Pre-r	equisite	Basic knowledge of Policy, Process, Standard, Procedure and Compliance	Syllab Versio		202 202	
Course Obj	ectives:					
	jectives of this co					
		magement process for allorganizations.				
	•	y standards, compliance, security controls an		ontro	ols.	
		and understand how it applies to theorganize	ations.			
		logies referenced by PCIDSS Iding and maintaining a SecureNetwork.				
J. To unde		iding and maintaining a Secure Network.				
Expected C	ourse Outcomes:					
		of the course, student will be able to:				
		magement process for all organizations		]	K2	
		y standards, security controls and control libr	aries.	]	K2	
		DSS is and understand how it applies to the		]	K2	
Ŭ	nizations.					20
		lding and maintaining a Secure Network or organization using PCI DSS.			<u>K2,</u> K K3	.3
		tand; <b>K3</b> - Apply; <b>K4</b> - Analyze; <b>K5</b> - Evalu	ate: <b>K6</b> –			
				0100		
Unit:1	1	Security Risk Management		<b>14</b> ł	nour	S
<b>Best Practice</b>	the Risk Manage –Risk Manageme	tisk Management – Risk Types and Risk I ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for	ramewor al Shape	ks: S of th	tand le Rl	s - arc MI
Best Practice Process – R	the Risk Manage –Risk Manageme MF Impleme <mark>ntati</mark>	ment Process. Existing Risk Management F	Framewor al Shape Risk Ma	ks: S of th anage	tand le Rl	s - arc MI
Best Practice Process – R International Standards.	the Risk Manage –Risk Manageme MF Implementati Organization for S	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST	Framewor al Shape Risk Ma	ks: S of th anage 39	tand le Rl men	s - arc MI t -
Best Practice Process – R International Standards. Unit:2	the Risk Manage –Risk Managementati MF Implementati Organization for S Secu	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST	Framewor cal Shape Risk Ma SP 800-1	ks: S of th anage 39 12h	tand he Rl men	s - arc MI t -
Best Practice Process – R International Standards. Unit:2 Select Secur	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu ity Controls: Under	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST	Framewor ral Shape Risk Ma SP 800-2 SP 800-2 nation Pr	ks: S of th anage 39 <u>12h</u> ocess	tand le RI men nour ing	s - arc MI t - s
Best Practice Process – RI International Standards. Unit:2 Select Secur Standard Pub	the Risk Manage –Risk Managementati MF Implementati Organization for S Secu ity Controls: Under lication 200 – Door	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST urity Controls and Control Library erstanding Control Selection - Federal Inforr cument Collection and Relationship Building	Framewor cal Shape Risk Ma SP 800-1 SP	ks: S of th anage 39 <u>12h</u> ocess ol Lib	tand ne RI men nour ing rarie	s - arc MI t - $\overline{s}$
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu ity Controls: Und lication 200 – Doo ctives for Informa	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST	Framewor cal Shape Risk Ma SP 800-2 SP	ks: S of th anage 39 <u>12h</u> ocess ol Lib	tand ne RI men nour ing rarie	s - arc MH t - <u>s</u> s:
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Objec Industrial Au	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu ity Controls: Unden lication 200 – Door ctives for Informa tomation and Con	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC	ramewor ral Shape Risk Ma SP 800- SP 800- nation Pr g - Contro Security 27001.	ks: S of th anage 39 12h ocess of Lib y Con	tand ne RI men nour ing rarie trols	s - arc MI t - s s: -
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object Industrial Au Unit:3	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu ity Controls: Und lication 200 – Doo ctives for Informa tomation and Con Payment Card	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST writy Controls and Control Library erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC	Framewor ral Shape Risk Ma SP 800-2 SP	ks: S of th anage 39 12h ocess of Lib y Con	tand ne RI men nour ing rarie	s - arc MI t - s s: -
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Objec Industrial Au Unit:3 PCI Introduc	the Risk Manage –Risk Manageme MF Implementati Organization for S <u>Secu</u> ity Controls: Unden lication 200 – Doo ctives for Informator tomation and Con <u>Payment Card</u> ction – Electronic	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST with Controls and Control Library erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea	ramewor ral Shape Risk Ma SP 800- SP 800- SP 800- Contro SP 800- Contro SP 800- SP 800- Contro SP 800- SP 800-	ks: S of th anage 39 12h ocess of Lib y Con 12h	tand be RI men nour ing rarie trols	s - arc MI t - s s: -
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object Industrial Au Unit:3 PCI Introduc Compliance a	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu- ity Controls: Und- lication 200 – Doo ctives for Informa tomation and Con Payment Card ction – Electronic and Validation – H	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critica trol Systems Security Life Cycle – ISO/IEC Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea listory of PCI DSS – PCI Council – QSAs, P	ramewor ral Shape Risk Ma SP 800-2 SP 8	ks: S of th anage 39 12h ocess of Lib 7 Con 12h 2s, Ql	tand be RI men nour ing rarie trols	s - arc MI t - s s: 
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object Industrial Au Unit:3 PCI Introduc Compliance a	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu- ity Controls: Und- lication 200 – Doo ctives for Informa tomation and Con Payment Card ction – Electronic and Validation – H	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST writy Controls and Control Library erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea	ramewor ral Shape Risk Ma SP 800-2 SP 8	ks: S of th anage 39 12h ocess of Lib 7 Con 12h 2s, Ql	tand be RI men nour ing rarie trols	s - arc MI t - s s: -
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Objec Industrial Au Unit:3 PCI Introduc Compliance a ASVs – PCI I Unit:4	the Risk Manager –Risk Manager MF Implementati Organization for S Secu- ity Controls: Und- lication 200 – Doo ctives for Informa tomation and Con Payment Card ction – Electronic und Validation – H Requirements – PO PCO	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST Frity Controls and Control Library erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC I Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea listory of PCI DSS – PCI Council – QSAs, P CI DSS and Risk – Benefits of Compliance –	ramewor ral Shape Risk Ma SP 800-2 SP 800-2 SP 800-2 SP 800-2 Contro Security 27001. SS) adlines – PFIs, PCII - Case Stu	ks: S of th anage 39 12h ocess of Lib 7 Con 12h 2s, Ql ady. 10h	tand he RI men hour ing rarie trols URs,	s - arc MI t - s s: -
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object Industrial Au Unit:3 PCI Introduc Compliance a ASVs – PCI I Unit:4 Determining	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu- ity Controls: Und- lication 200 – Doc ctives for Informa tomation and Con Payment Card ction – Electronic und Validation – H Requirements – Po g and Reducing the	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST with Controls and Control Library erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea listory of PCI DSS – PCI Council – QSAs, P CI DSS and Risk – Benefits of Compliance –	Framewor ral Shape Risk Ma SP 800-1 SP 800-1 SP 800-1 nation Pr g - Contro SS) adlines – PFIs, PCII - Case Stu – Plannin	ks: S of th anage 39 12h ocess of Lib: 7 Con 12h Ps, Q1 ady. 10h ng PC	tand he RI men hour ing rarie trols URs,	s - arc MI t - s s: -
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object Industrial Au Unit:3 PCI Introduc Compliance a ASVs – PCI I Unit:4 Determining Project. Build	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu- ity Controls: Und- lication 200 – Doo ctives for Informa tomation and Con Payment Card ction – Electronic and Validation – H Requirements – Po PCO g and Reducing the ling and Maintain	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST writy Controls and Control Library erstanding Control Selection - Federal Inform cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea listory of PCI DSS – PCI Council – QSAs, P CI DSS and Risk – Benefits of Compliance –	ramewor ral Shape Risk Ma SP 800-2 SP 800-2 SP 800-2 nation Pr g - Contro Security 27001. SS) adlines – PFIs, PCII - Case Stu – Plannin Configura	ks: S of th anage 39 12h ocess of Lib 7 Con 12h Ps, Ql ady. 10h ng PC ation	tand he RI men hour ing rarie trols URs,	s - arc MI t - s s: -
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object Industrial Au Unit:3 PCI Introduc Compliance a ASVs – PCI I Unit:4 Determining Project. Build	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu- ity Controls: Und- lication 200 – Doo ctives for Informa tomation and Con Payment Card ction – Electronic and Validation – H Requirements – Po PCO g and Reducing the ling and Maintain	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST with Controls and Control Library erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea listory of PCI DSS – PCI Council – QSAs, P CI DSS and Risk – Benefits of Compliance –	ramewor ral Shape Risk Ma SP 800-2 SP 800-2 SP 800-2 nation Pr g - Contro Security 27001. SS) adlines – PFIs, PCII - Case Stu – Plannin Configura	ks: S of th anage 39 12h ocess of Lib 7 Con 12h Ps, Ql ady. 10h ng PC ation	tand he RI men hour ing rarie trols URs,	s - arc MI t - s s: -
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object Industrial Au Unit:3 PCI Introduc Compliance a ASVs – PCI I Unit:4 Determining Project. Build	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu- ity Controls: Und- lication 200 – Doo ctives for Informa tomation and Con Payment Card ction – Electronic and Validation – H Requirements – Po PCO g and Reducing the ling and Maintain	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST with Controls and Control Library erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea listory of PCI DSS – PCI Council – QSAs, P CI DSS and Risk – Benefits of Compliance – O Scope and Secure Network e PCI Scope: Basics – Scope Reduction Tips ing a Secure Network: Establishing Firewall ctices – Common Mistakes and Pitfalls – Ca	ramewor ral Shape Risk Ma SP 800-2 SP 800-2 SP 800-2 nation Pr g - Contro Security 27001. SS) adlines – PFIs, PCII - Case Stu – Plannin Configura	ks: S of th anage 39 12h ocess of Lib ocess of Lib Di Cocess of Lib Ocess of Lib Ocess Ocess Ocess Ocess Ocess Ocess Ocess	tand he RI men hour ing rarie trols URs,	s - s s s s s s
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object Industrial Au Unit:3 PCI Introduc Compliance a ASVs – PCI I Unit:4 Determining Project. Build Standards – T Unit:5 Principles of	the Risk Manage –Risk Manage MF Implementati Organization for S Secu- ity Controls: Unden- lication 200 – Door ctives for Information tomation and Con Payment Card ction – Electronic and Validation – H Requirements – PO PCO g and Reducing the ling and Maintaini Cools and Best Pra f Access Control –	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC I Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea listory of PCI DSS – PCI Council – QSAs, P CI DSS and Risk – Benefits of Compliance – O Scope and Secure Network e PCI Scope: Basics – Scope Reduction Tips ing a Secure Network: Establishing Firewall ctices – Common Mistakes and Pitfalls – Ca	ramewor ral Shape Risk Ma SP 800-3 SP 800-3 SP 800-3 ration Pr control Security 27001. SS) adlines – FIs, PCII - Case Stu - Plannin Configura se Study. n Basics	ks: S of th anage 39 12h ocess of Lib 7 Con 12h Ps, Ql ady. 10h ng PC ation 12h - Win	tand he RI men hour ing rarie trols IRs, IRs,	s - arc MI t - s s s s s s s s s s s s s s s s s s
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Object Industrial Au Unit:3 PCI Introduc Compliance a ASVs – PCI I Unit:4 Determining Project. Build Standards – T Unit:5 Principles of and PCI Com	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu- ity Controls: Und- lication 200 – Doc ctives for Informa tomation and Con Payment Card ction – Electronic and Validation – H Requirements – PC g and Reducing the ling and Maintaini cools and Best Pra f Access Control – pliance – POSIX	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST rity Controls and Control Library erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea listory of PCI DSS – PCI Council – QSAs, P CI DSS and Risk – Benefits of Compliance – O Scope and Secure Network e PCI Scope: Basics – Scope Reduction Tips ing a Secure Network: Establishing Firewall ctices – Common Mistakes and Pitfalls – Ca Strong Access Controls - Limitations of User Access – Authenticatio Access Control – CISCO and PCI Requirem	Framewor al Shape Risk Ma SP 800-2 SP 800-2 nation Pr control Security 27001. SS) adlines – FIs, PCII - Case Study. PFIs, PCII - Plannin Configura se Study. n Basics ents – CI	ks: S of th anage 39 12h ocess of Lib: 7 Con 12h Ps, Q1 dy. 10h ng PC ation 12h ng PC ation	tand he RI men hour ing rarie trols IRs, IRs,	s - arc MI t - s s: s s s
Best Practice Process – R International Standards. Unit:2 Select Secur Standard Pub Control Objec Industrial Au Unit:3 PCI Introduc Compliance a ASVs – PCI I Unit:4 Determining Project. Build Standards – T Unit:5 Principles of and PCI Com Enforce Sessi	the Risk Manage –Risk Manageme MF Implementati Organization for S Secu- ity Controls: Und- lication 200 – Doc ctives for Informa tomation and Con Payment Card ction – Electronic and Validation – H Requirements – PC g and Reducing the ling and Maintaini cools and Best Pra f Access Control – pliance – POSIX	ment Process. Existing Risk Management F ent Tangible – Formal Architecture – Gener on – Other Frameworks and Models for Standardization – NIST SP 800-30 and NIST erstanding Control Selection - Federal Inforr cument Collection and Relationship Building tion and Related Technologies – CIS Critical trol Systems Security Life Cycle – ISO/IEC Industry Data Security Standard (PCI D Card Payment Ecosystem – Compliance Dea History of PCI DSS – PCI Council – QSAs, P CI DSS and Risk – Benefits of Compliance – O Scope and Secure Network e PCI Scope: Basics – Scope Reduction Tips ing a Secure Network: Establishing Firewall actices – Common Mistakes and Pitfalls – Ca	Framewor al Shape Risk Ma SP 800-2 SP 800-2 nation Pr control Security 27001. SS) adlines – FIs, PCII - Case Study. PFIs, PCII - Plannin Configura se Study. n Basics ents – CI	ks: S of th anage 39 12h ocess of Lib: 7 Con 12h Ps, Q1 dy. 10h ng PC ation 12h ng PC ation	tand he RI men hour ing rarie trols IRs, IRs,	arciver arcive

Unit:	5		Co	ontempor	rary Issu	les				2 hours
Write a	n assignm	ent on any	one of	the follow	ving:			·		
1. PCIC	Council									
2. Build	ling Secur	eNetwork	-							
						Total Le	cture ho	urs	62	hours
Text l	Book(s)									
1 A	nne Kohn	ke, Ken S	igler, Da	an Shoma	ıker, "Im	plementi	ng Cyber	security:	A Guide	to the
	lational Sta									
2 E	randen R.	Williams	, Anton .	A. Chuva	l <mark>kin, "</mark> PC	I Compli	ance: Un	derstand	and Impl	ement
E	ffective P	CI Data S	ecurity S	tandard (	Compliar	nce", Fou	rth Editio	on,Syngr	ess,	
2	015.		1 State							
		1		-	-		34			
Refer	ence Book	is 🧹		697		1	2			
1	Barry L. V	Villiams 🏾	Informat	tion Secu	rity Polic	y Develo	opment fo	or Compl	iance: IS	O/IEC
2	7001, NIS	T SP 80 <mark>0</mark> -	- <mark>53</mark> , HIP.	AA Stand	dard, PCI	DSS V2	2.0, and A	UP V5.0	)", CRC I	Press,
2	013						<u> </u>			
Relat	ed Online	Contents	[MOO	C <mark>, SW</mark> AY	YAM, NI	PTEL, V	vebsites o	etc.]		
1	www.cours	sera.com[	Cybersed	curity Co	mpliance	Framew	ork & Sy	stem Ad	ministrati	on]
Web	Link	2	E.	in sources		12-5	- 87 - 1			
1. h	ttps://reso	urces.info	secinstit	ute.com/s	tep-step-	guide-da	ta-securit	y-compli	ance-	
i	ndustry/#g	ref		Card	the second	1.3				
2. h	ttps://www	v.tutorials	point.co	m/compu	ter_secur	rity/comp	uter_secu	urity_lega	al_compli	iance.ht
n	n		Sec. 1			and and		7 · / ·	_	
3. <u>h</u>	ttps://www	v.akamai.	com/uk/	en/resour	ces/secur	rity-com	liance.js	2		
Cours	e Designed	d By: Dr.	S. Gavas	kar and (	CSCC La	.bs	5 / ·			
Ma	pping wit	h Progra	mme Ou	itcomes	and the second	ast	- Alexander			
COs	Р	Р	Р	Р	660 ( <b>P</b> °	Р	Р	Р	Р	PO
	01	02	03	04	05	06	07	08	09	10
CO1	S	S	L	L	М	L	L	S	S	L
CO2	S	М	L	М	М	L	S	S	S	L
CO3	S	М	S	S	S	S	S	S	S	S
<b>CO4</b>	S	М	S	S	М	S	S	S	S	М
	S	S	М	S	М	S	S	S	S	

#### Course Title: <u>Case studies of Cyber Security - Paper 1</u>

No. of Credits :6 Course Code :21CSESC13

Every person would be doing 2 case studies with help of CSSC GSOC & Professors

#### Course Title: <u>Case studies of Cyber Security - Paper 2</u>

No. of Credits : 6 Course Code :21CSESC14

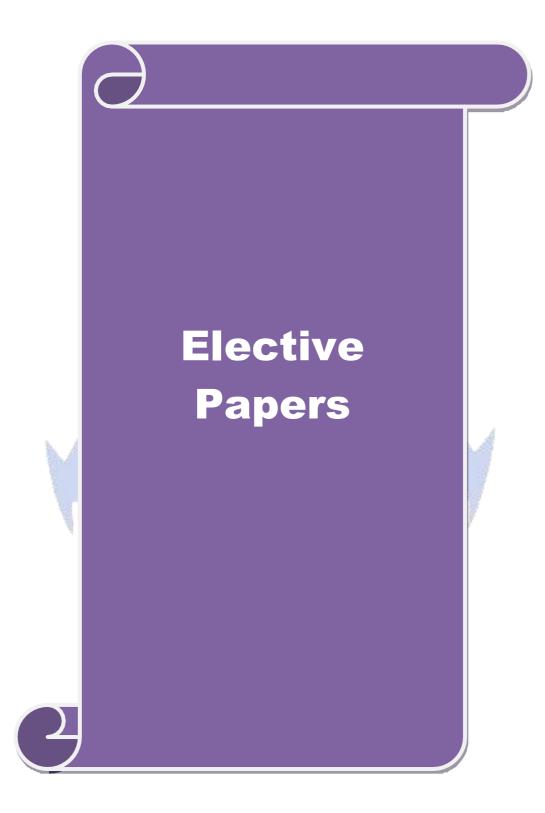
Every person would be doing 2 case studies with help of CSSC GSOC & Professors

#### **Course Title:** <u>Practice School</u>

CONC.

No. of Credits : 14 Course Code :21CSESC15

Every person would be doing a Cyber Security Based Project



code	21CSESE01	IT Infrastructure and Cloud Security	L	Т	Р	C
Core/Elect	tive/Supportive	Elective	4			4
	requisite	Cloud, Networking Basics	•	abus ·sion	202 202	
Course O	•					
The main	objectives of this c	ourse are to:				
		oncepts of Internet of Things				
	o learn how to use					
	o implementVirtua		form	nt and	futur	•••
	loud computingsec	blex technologies leading to the development o	or curre	ent and	Iutui	e
	ioud computingsec	unty				
Expected	<b>Course Outcomes</b>	5:				
-		n of the course, student will be able to:				
		malware, its capabilities, and how it is comba	ted		K	2
throug	th detection and cla	assification.				
		onomic, and historical context in which malwa	are occ	urs.	K	
3 Analyz	e malicious in win	ndows programs.	1		K	
	the tools and meth nown executable.	odologies used to perform static and dynamic	analys	18	K.	3
		ncepts to unpack, extract, decrypt, or bypass ne	w ant	i_	K	2
		ture malware samples.	w and	L	11.	,
	-		17.4			
INI - Keine		stanu, <b>NJ - A</b> ppiy, <b>N4</b> - Analyze, <b>NJ -</b> Evalua	ate; Ke	6 – Cre	ate	
NI - Keille	enioer, <b>112</b> - Onder	stand; <b>K3 - Apply; K4 -</b> Analyze; <b>K5 -</b> Evalua	ate; Ke	<u>6 – Cre</u>	ate	
Unit:1		to Networking & Communication Protocol	1 and		ate <b>hour</b>	S
Unit:1 Networkin	<b>Introduction</b> ng: Introduction to	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and	s I WAN	10 J. Inte	)hour ernet	of
Unit:1 Networkin Things: Int	<b>Introduction</b> ng: Introduction to roduction – Defini	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource	s I WAN e Mana	10 N. Inte Igemen	<b>)hour</b> e <b>rnet</b> nt — Ie	o Tc
Unit:1 Networkin Things: Int Data Mana	<b>Introduction</b> ng: Introduction to roduction – Defini gement and Anal	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit	s I WAN e Mana	10 N. Inte Igemen	<b>)hour</b> e <b>rnet</b> nt — Ie	<b>to</b> Tc
Unit:1 Networkin Things: Int Data Mana	<b>Introduction</b> ng: Introduction to roduction – Defini gement and Anal	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource	s I WAN e Mana	10 N. Inte Igemen	<b>)hour</b> e <b>rnet</b> nt — Ie	to Cc
Unit:1 Networkin Things: Int Data Mana Authenticat	<b>Introduction</b> ng: Introduction to roduction – Defini gement and Anal	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit vice Collaboration Framework.	s I WAN e Mana	10 N. Inte igemen nagemen	<b>hour</b> ernet nt – Ie ent a	of DT nc
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2	Introduction ng: Introduction to roduction – Defini gement and Anal ion – Privacy. Dev	to Networking & Communication Protocol o Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit rice Collaboration Framework. Fog Computing	s I WAN Mana y Man	10 N. Inten Igemen nagemen 14	Dhour ernet nt – Id ent a	of oT nc
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com	Introduction ng: Introduction to roduction – Defini gement and Anal ion – Privacy. Dev puting: Introducti	to Networking & Communication Protocol o Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit vice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectu	s I WAN Mana y Mar y Mar re – A	10 N. Inte agemen nagemo 14 Applica	Phour ernet nt – Id ent a hour ations	of oT nc s
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I	Introduction ng: Introduction to roduction – Defini gement and Anal ion – Privacy. Dev puting: Introducti Directions and En	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identity vice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectu nables – Commercial Products. Stream H	s I WAN Mana y Man y Man re – A	10 N. Inten igemen nagemo 14 Applica sing i	Phour ernet nt – Id ent a lhour ations n Io	of DT nc s T
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I	Introduction ng: Introduction to roduction – Defini gement and Anal ion – Privacy. Dev puting: Introducti Directions and En of Stream Process	to Networking & Communication Protocol o Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit vice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectu	s I WAN Mana y Man y Man re – A	10 N. Inten igemen nagemo 14 Applica sing i	Phour ernet nt – Id ent a lhour ations n Io	of DT nc s T
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future	Introduction ng: Introduction to roduction – Defini gement and Anal ion – Privacy. Dev puting: Introducti Directions and En of Stream Process	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identity vice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectu nables – Commercial Products. Stream H	s I WAN Mana y Man y Man re – A	10 N. Inten igemen nagemo 14 Applica sing i – Cha	Phour ernet at – Id ent a <b>lhour</b> ations <b>n Io</b> alleng	of pT nc s T: ges
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future 1 Unit:3	Introduction ng: Introduction to roduction – Defini gement and Anal ion – Privacy. Dev puting: Introducti Directions and En of Stream Process Direction.	to Networking & Communication Protocol o Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit rice Collaboration Framework. Fog Computing ton – Characteristics – Reference Architectu nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S	s I WAN Mana y Man y Man re – A Process	10 N. Inte agemen nagemen 14 Applica sing i – Cha	Phour ernet at – Id ent a <b>Phour</b> ations <b>n Io</b> alleng <b>Phour</b>	of pT nc s T ; ges
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co	Introduction ng: Introduction to roduction – Definit gement and Anal ion – Privacy. Dev puting: Introducti Directions and En of Stream Process Direction.	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identity vice Collaboration Framework. Fog Computing con – Characteristics – Reference Architectu nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen	s     WAN e Mana y Man y Man re – A Process System Cess –	10 N. Inten igemen nagemo 14 Applica sing i – Cha 12 Techno	Phour ernet at – Id ent a hour ations n Io alleng <b>Chour</b>	of oT nc s T s s s s
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co Influences	Introduction ng: Introduction to roduction – Defini- gement and Anal- ion – Privacy. Dev puting: Introducti- Directions and En- of Stream Process Direction. ( mputing: Introduction) ( mputing: Intro	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identity rice Collaboration Framework. Fog Computing ton – Characteristics – Reference Architectur nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen fluences. Cloud Computing Architecture:	s     WAN e Mana y Man y Man re – A Process System Cess –	10 N. Inten igemen nagemo 14 Applica sing i – Cha 12 Techno	Phour ernet at – Id ent a hour ations n Io alleng <b>Chour</b>	of oT nc s T s s s s
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co Influences	Introduction ng: Introduction to roduction – Defini- gement and Anal- ion – Privacy. Dev puting: Introducti- Directions and En- of Stream Process Direction. ( mputing: Introduction) ( mputing: Intro	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identity vice Collaboration Framework. Fog Computing con – Characteristics – Reference Architectu nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen	s     WAN e Mana y Man y Man re – A Process System Cess –	10 N. Inten igemen nagemo 14 Applica sing i – Cha 12 Techno	Phour ernet at – Id ent a hour ations n Io alleng <b>Chour</b>	of oT nc s T s s s s
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co Influences Deploymen	Introduction ng: Introduction to roduction – Definit gement and Anal ion – Privacy. Dev puting: Introducti Directions and En- of Stream Process Direction. ( mputing: Introduction – Operational Introduction t Model – Benefits	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identity rice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectur nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen fluences. Cloud Computing Architecture: s. Cloud SecurityServices.	s     WAN e Mana y Man y Man re – A Process System Cess –	10 N. Inten igemen nagemo 14 Applica sing i – Cha 12 Techno very N	Phour ernet at – Id ent a <b>Hour</b> ations <b>n Io</b> alleng <b>Chour</b> ologid fodel	of oT nc s T ges s s a -
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co Influences Deploymen Unit:4	Introduction ng: Introduction to roduction – Definit gement and Anal ion – Privacy. Dev puting: Introducti Directions and End of Stream Process Direction. ( mputing: Introduct – Operational Introduct t Model – Benefits	to Networking & Communication Protocol o Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit rice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectu nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen fluences. Cloud Computing Architecture: s. Cloud SecurityServices.	s WAN Mana y Mana y Man re – A Process System ces – Deliv	10 N. Inter agement nagement nagement agement 14 Applica sing i - Cha 12 Techno very N	Phour ernet at – Id ent a <b>Phour</b> ations <b>n Io</b> alleng <b>Phour</b> ologid fodel	of oT nc s <b>s</b> c s c a l s s
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co Influences Deploymen Unit:4 Cloud, Vi	Introduction ng: Introduction to roduction – Definit gement and Anal ion – Privacy. Dev puting: Introducti Directions and End of Stream Process Direction. ( mputing: Introduction – Operational Introduction t Model – Benefits V irtualization, and	to Networking & Communication Protocol o Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit rice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectu nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen fluences. Cloud Computing Architecture: s. Cloud SecurityServices. irtualization & Data Center IDataStorage & Data Center Network	s WAN Mana y Mana y Mana y Mana y Mana re – A Process System ces – Deliv ingFu	10 N. Inter agementagem	Phour ernet at – Id ent a <b>Phour</b> ations <b>n Io</b> alleng <b>Phour</b> ologic fodel <b>Phour</b> entals	of oT nc s <b>s</b> c s c a l s s
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future 1 Unit:3 Cloud Co Influences Deploymen Unit:4 Cloud, Vi Server and 1	Introduction ng: Introduction to roduction – Defini- gement and Anal- ion – Privacy. Dev puting: Introducti- Directions and En- of Stream Process Direction. ( mputing: Introduction mputing: Introduction ( mputing:	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identity rice Collaboration Framework. Fog Computing ton – Characteristics – Reference Architectur nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen fluences. Cloud Computing Architecture: s. Cloud SecurityServices. irtualization & Data Center IDataStorage & Data Center Network mentals – I/O Connectivity and Networking Fu	s     WAN e Mana y Mana y Mana y Mana re – A Process System cess – Deliv ingFu	10 N. Inten igemen nagema 14 Applica sing i – Cha 12 Techno very M 12 ndame entals	Phour ernet at – Ie ent a Hour ations n Io alleng Chour ologic fodel Chour entals – IT	
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co Influences Deploymen Unit:4 Cloud, Vi Server and S Clouds – Vi	Introduction ng: Introduction to roduction – Definit gement and Anal ion – Privacy. Dev puting: Introducti Directions and En- of Stream Process Direction. ( mputing: Introduct – Operational Int t Model – Benefits V irtualization, and Storage I/O Fundati irtualization: Serve	to Networking & Communication Protocol o Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit vice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectur nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen fluences. Cloud Computing Architecture: s. Cloud SecurityServices. irtualization & Data Center IDataStorage & Data Center Network mentals – I/O Connectivity and Networking Fu ers, Storage and Networking – Virtualization a	s WAN Mana y Mana y Mana y Man re – A Process System cess – Deliv ingFu undam nd Sto	10 N. Inter agementagem	Phour ernet at – Id ent a <b>Phour</b> ations <b>n Io</b> alleng <b>Phour</b> ologid fodel <b>Phour</b> entals – IT ervice	of of nc s - T ; es s - s : : s : : :
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co Influences Deploymen Unit:4 Cloud, Vi Server and S Clouds – Vi – Data and	Introduction ng: Introduction to roduction – Definit gement and Anal ion – Privacy. Dev puting: Introducti Directions and En- of Stream Process Direction. Model – Benefits V irtualization, and Storage I/O Fundar irtualization: Serve Storage Access. In	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identity rice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectur nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen fluences. Cloud Computing Architecture: s. Cloud SecurityServices. irtualization & Data Center IDataStorage & Data Center Network mentals – I/O Connectivity and Networking Fu ers, Storage and Networking – Virtualization at nfrastructure Resource Management: Introduction	s     WAN e Mana y Man y Man re – A Process System cess – Deliv ingFu undam nd Sto duction	10 N. Inten igemen nagemo 14 Applica sing i – Cha 12 Techno very N 12 ndamo entals rage So n - Ma	Phour ernet at – Id ent a <b>Hour</b> ations <b>n Io</b> alleng <b>Chour</b> ologid fodel <b>Chour</b> entals – IT ervice nagin	of oT nc s T ges s s a s s s s s s s s g
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co Influences Deploymen Unit:4 Cloud, V Server and Clouds – V – Data and Data Infrast	Introduction ng: Introduction to roduction – Definit gement and Anal ion – Privacy. Dev puting: Introducti Directions and En- of Stream Process Direction. ( mputing: Introduction C mputing: Introduction ( mputing: Introduction ( mputing	to Networking & Communication Protocol o Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identit vice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectur nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen fluences. Cloud Computing Architecture: s. Cloud SecurityServices. irtualization & Data Center IDataStorage & Data Center Network mentals – I/O Connectivity and Networking Fu ers, Storage and Networking – Virtualization a	s     WAN e Mana y Man y Man re – A Process System cess – Deliv ingFu undam nd Sto duction	10 N. Inten igemen nagemo 14 Applica sing i – Cha 12 Techno very N 12 ndamo entals rage So n - Ma	Phour ernet at – Id ent a <b>Hour</b> ations <b>n Io</b> alleng <b>Chour</b> ologid fodel <b>Chour</b> entals – IT ervice nagin	of oT nc s T ges s s a s s s s s s s s g
Unit:1 Networkin Things: Int Data Mana Authenticat Unit:2 Fog Com Research I Foundation and Future Unit:3 Cloud Co Influences Deploymen Unit:4 Cloud, Vi Server and S Clouds – Vi – Data and	Introduction ng: Introduction to roduction – Definit gement and Anal ion – Privacy. Dev puting: Introducti Directions and En of Stream Process Direction. Model – Benefits V irtualization, and Storage I/O Fundati irtualization: Serve Storage Access. In tructure for Cloud es	to Networking & Communication Protocol Corporate Infrastructure – LAN, MAN and ition Evolution – IoT Architecture – Resource lytics – Communication Protocols – Identity rice Collaboration Framework. Fog Computing on – Characteristics – Reference Architectur nables – Commercial Products. Stream H sing in IoT – Continuous Logic Processing S Cloud Computing Influences ction – Characteristics – Architectural Influen fluences. Cloud Computing Architecture: s. Cloud SecurityServices. irtualization & Data Center IDataStorage & Data Center Network mentals – I/O Connectivity and Networking Fu ers, Storage and Networking – Virtualization at nfrastructure Resource Management: Introduction	s     WAN e Mana y Man y Man re – A Process System cess – Deliv ingFu undam nd Sto duction	10 N. Inten igemen nagema 14 Applica sing i – Cha 12 Techno very M 12 ndamo entals rage So n - Ma s – Ma	Phour ernet at – Id ent a <b>Hour</b> ations <b>n Io</b> alleng <b>Chour</b> ologid fodel <b>Chour</b> entals – IT ervice nagin	of oT nd s s c s s s s s s g g

**Data and Storage Networking Security:** Security Threat Risks and Challenges – Securing Networks – Securing Storage – Securing Clouds. **Data Protection:** Data Protection Challenges and Opportunities – Protect, Preserve, and Serve Information Services – Virtual – Physical, and Cloud Data Protection – Modernizing and Protection and Backup.

Unit:6	Contemporary Issues	2 hours							
Internet of F	Internet of Robotic Things - Cloud-enabled Robotics.								
	Total Lecture hours	62hours							
Text Book	(s)								
	mar Buyya, Amir Vahid Dastjerdi, "Internet of Things: Principles N Kaufmann Publications, 2016.	and Paradigms",							
	d L.Krutz, Russell Dean Vines, "Cloud Security: A Comprehensiv Computing", Wiley Publishing, Inc, 2010.	ve Guide to Secure							
Reference	Books								
	a, "Security and Privacy in Internet of Things: Models, Algorithm nentations", CRC Press, 2016.	and							
2 John I	R.Vacca, "Cyber Security and IT Infrastructure Protection", Syngr	ress, 2013.							
	Dotson, "Practical Cloud Security: A Guide for Secure Design an ly Media Publications, 2019.	d Deployment",							
Related O	nline Contents [MOOC, SWAYAM, NPTEL, Websites etc.]								
https://	'onlinecour <mark>ses.npte</mark> l.ac.in [Two Courses]								
1	Components And Applications Of Internet Of Things	15 Weeks							
2	Introduction to Industry 4.0 and Industrial Internet of Things.	12 Weeks							
	<pre>www.classcentral.com/course/cloud-computing-security-11754[C ing Security]</pre>	Cloud							
Web Link		F							
Course De	signed By: Dr. S. Gavaskar & CSSC Labs								

Map	Mapping with Programme Outcomes											
COs	Р	Р	Р	Р	Р	Р	Р	Р	Р	PO		
COS	01	02	03	04	05	06	07	<b>O8</b>	<b>O9</b>	10		
CO1	Μ	L	L	L	L	L	L	S	L	М		
CO2	L	L	L	L	L	L	L	S	L	М		
CO3	S	S	S	М	S	М	М	S	S	S		
CO4	S	S	М	S	М	S	S	S	М	М		
CO5	М	М	М	S	М	S	S	S	М	М		

Course code	21CSESE02	MALWARE ANALYSIS	L	Т	Р	С
Core/Electi	ive/Supportive	Elective	4			4
Pre-1	requisite	Operating System, Basics of Malware, Security Concepts and Algorithms	Syllabus Version		2021 2022	
Course Obje	ectives:					
The main obj	jectives of this cou	irse are to:				
		ature of malware, its capabilities, and how it is	combated	lthr	ough	
	etection and classif					
		ools and methodologies used to perform static a	nd dynam	icar	nalysi	.S
	n unknownexecuta					
		ocial, economic, and historical context in which				
		techniques and concepts to unpack, extract, de ques in future malwaresamples.	crypt, or t	ура	iss ne	W
al	iti-aliarysis techni	ques in future marwaresamples.				
Expected Co	ourse Outcomes:					
-		n of the course, student will be able to:				
	1	f malware, its capabilities, and how it is comba	ted		K	2
	sh detection and cl					
		conomic, and historical context in which malw	are occurs	5.	ŀ	K2
3 Analy	ze malicious in w	ndows programs.			ŀ	K4
		hodologies used to perform static and dynamic	analysis		H	K3
	known executable	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
		oncepts to unpack, extract, decrypt, or bypass n	ew anti-		ŀ	K3
	-	iture malware samples.		~		
KI - Reme	ember; <b>K2</b> - Unde	rstand; <b>K3 - App</b> ly; <b>K4 - Analyze</b> ; <b>K5 - Evalua</b>	$\mathbf{K6} = \mathbf{C}$	Crea	ite	
Unit:1		Malware Analysis Overview	38	12	hour	•6
Techniques malicious	- Types of Malwindows program	Malware – Goals of Malware Analysis- ware Analysis – General Rules for Malware ns:Windows API – Windows Registry – – Kernel vs User Mode- Native API.	<b>Analysis</b>	. A	nalyz	ing
Unit:2	0.0	Basic Analysis		1/	hour	
Basic Stat Obfuscated Analysis in Dirty Appro Process Exp Using Depe withRegsho	Malware – Portat Practice – PE F bach – Running M plorer: The Proces endency Walker,	Antivirus Scanning – Hashing – Finding Scanning – Hashing – Finding Scale Executable File Format – Linked Libraries and Sections. Basic Dynamic Art falware – Monitoring with Process Monitor – V ss Explorer Display, Using the Verify Option Analyzing Malicious Documents – Comparing k–PacketSniffingwithWireshark–UsingINetSin	and Funct nalysis: ( Viewing P , Compari g Registry	Pack ion Qual roce	ced a – Sta lity a ess w String	nd tic nd ith gs,
Unit:3		Advanced Analysis		10	hour	s
x86 Archit	ecture: Memory, i	nstructions, opcodes, operands, registers, funct	ions, stac			
		- Analyzing Functions – Using Graphing Optio	ons – Enha	ncii	ng	
Disassembly	y – Extending IDA	A with Plug-ins.				
IIm:4.1		Advanced Dynamic Analysis		1	2hou	
Unit:4		Advanced Dynamic Analysis Level Debuggers –Kernel vs User-Mode	Dobugai			
Debugger – OllyDbg Int Loading DI	- Exceptions – M terface – Memory LLs – Tracing – H	odifying Execution with a Debugger.OllyDbg MapViewing Threads and Stacks – Executing Exception Handling – Patching – Analyzing S ble Debugging. Using WinDbg – Microsoft Syr	g:Loading Code – B: hellcode -	Mareak	alwar point	re – ts –

Unit:5	Anti-Disassembly and Anti-Debugging	12hours
	nbly:Understanding Anti-Disassembly – Defeating Disassembly A	
	Techniques – Obscuring Flow Control – Thwarting Stack-Frame	
	Vindows Debugger Detection – Identifying Debugger Behaviour –	
00 0	nctionality – Debugger Vulnerabilities. Defeat Malware.	U
Unit:6	Contemporary Issues	2 hours
	ignment on any one of the following:	
1. Malware	AnalysisTools	
2. Malicious	in WindowsPrograms.	
	Total Lecture hours	62hours
Text Book	(s)	
1 Michael	Sikorski, Andrew Honig, "Practical Malware Analysis", No Stra	ch Press, 2012.
2 Michael	Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard "Ma	alware Analyst"s
Cookbo	ok and DVD: Tools and Techniques for Fighting Malicious Code	", Wiley Publishing
Inc, 201		
3 Chris E	agle, The IDA Pro Book", 2 <sup>nd</sup> Edition, No Strach Press, 2011.	
Reference	Books	
1 Eldad E	ilam, "Reversing: Secrets of Reverse Engineering", Wiley Publisl	hing Inc, 2005.
2 Michae	Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, "The Art	of Memory
Forensi	es: Detecting Malware and Threats in Windows, Linux, and Mac	Memory", Wiley,
2014.		
Related O	nline Contents [MOOC, SWAYAM, NPTEL, Websites etc.]	
	ww.cybrary.it/course/malware-analysis/[Intro to Malware Analys	is and Reverse
Engineer	6	
-	ww.elearnsecurity.com/course/malware_analysis_professional/ [Market Market Ma	Malware Analysis
Professio	onal]	
Web Link		
	ps://www.hackingtutorials.org/category/malware-analysis-tutoria	ls/
	ps://gbhackers.com/malware-analysis-cheat-sheet-and-tools-list/	
Course Des	signed By: Dr. S. Gavaskar and CSCC Labs	

Mappi	Mapping with Programme Outcomes										
COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	
CO1	М	L	L	L	L	L	L	S	L	М	
CO2	L	L	L	L	L	L	L	S	L	М	
CO3	S	S	S	М	S	М	М	S	S	S	
CO4	S	S	М	S	Μ	S	S	S	Μ	М	
CO5	М	М	М	S	М	S	S	S	Μ	М	

Course code	21CSESE03	INCIDENT RESPONSE	L	Т	Р	C
Core/Election	ive/Supportive	Elective	4			4
Pre-1	requisite	Forensics, Networks & Penetration Testing	Syllabus Version	202	21-2	022
Course O	bjectives:			•		
	objectives of this					
2. To u	understand Incide	ent Response Policy, Plan andProcedure. ent Handling, Coordination and InformationS I methods for Data Exfiltration Detection and	-	n.		
Expected	Course Outcom	nes:				
On the suc	ccessful completi	on of the course, student will be able to:				
1 Und	erstand the Incid	ent Response needs and structure.		]	K2	
2 Und	erstand the Incid	ent Handling techniques		k	K2	
3 Und	erstand the Coor	dination and Information Sharing in Incident	Response	K	K2	
4 Und	erstand and analy	ze the scenarios in Incidence Response		K	К2-К	4
		ne Incident Response issues.			КЗ-К	
<b>K1</b> - Rem	ember; <b>K2</b> - Unc	lerstand; K3 - Apply; K4 - Analyze; K5 - Ev	aluate; <b>K</b> 6	- C	reate	;
Unit:1		ntroduction to Incid <mark>ent Respon</mark> se			nour	'S
		e, Incident Response Policy, Plan, and Proce	dure Creat	ion,		
Incident Re	esponse Team Str	ucture, Incident Response Team Services.	10 m			
	1		-			
Unit:2		Incident Handling			hou	
-		Analysis, Containment, Eradication, and Re	covery, Po	st-In	cide	nt
Activity, In	cident Handling	Checklist.				
Unit:3	Coo	dination and Information Sharing		121	iour	•6
		Sharing Techniques, Granular Information S	haring	141	Ioui	3
Coordinat		Sharing Teeninques, Standard Information 5	naring.		10	
Unit:4	S	cenarios in Incidence Response		14	iour	'S
		DNS), Server Denial of Service (DoS), Co	mpromised		1	
Server, W Documents Host, Teleo	orm and Distri , Unknown Exf	buted Denial of Service (DDoS) Agent ltration, Unauthorized Access to Payroll R promise Anonymous Threat, Peer-to-Peer Fi	Infestatie ecords, Di	on, Isapp	Stol eari	en ng
II:4-5		noident Desponse Use Course	5 m	101	101	
Unit:5		ncident Response Use Cases	ing (IsT)		nour	
Data EXII	mation Detection	and Prevention. Mitigation of Internet of Th	nngs (101 <i>)</i>	inr	eats.	
Unit:6		Contemporary Issues		<b>2</b> ł	our	S
Issues in I	Dark Reading, Iss	sues in Cyber espionage. Problems with Logi	c Bomb.			
		Total Lecture hours		62h	ours	5
Text Book(s	·					
Handlir Publica	ng Guide", Nation tion,2012.	Iillar, TimGrance, Karen Scarfone, "Comput nal Institute of Standards and Technology Sp	ecial			t
		n Smith, "Applied Network Security Monitors", Syngress- Elsevier, 2014.	ring: Colle	ctior	۱,	

3	Don Murdoch, "Blue Team Handbook: Incident Response Edition : a Condensed Field							
	Guide for the Cyber Security Incident Responder", Create Space Independent Publishing,							
	2014							
Re	Reference Books : EBooks							
1	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf							
2	Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices							
	by Arun E Thomas							
3	Security Operations Center - Tools & Practices by Arun E Thomas							
	with the							
Re	Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]							

## Related Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]

	Course Title	Duration	Provider
1	Penetration Testing, Incident Response and Forensics	4 weeks	Coursera
	and the state		(IBM)
2	Cyber Security Capstone: Breach Response Case	4 weeks	Coursera
•	Studies		(IBM)
We	b link		
1. h	ttps://security.uc <mark>op.edu/</mark> files/documents/policies/incident-res	ponse-standard.pd	lf
2. h	ttps://www.cybersecuritycoalition.be/content/uploads/cyberse	ecurity-incident-m	anagement-
g	uide-EN.pdf		
Cour	se Designed by: Dr.M. Punithavalli and CSCC Labs	1000	

Map	Mapping with Programme Outcomes											
COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10		
CO1	L	М	М	OUL TE	М	М	L	S	М	S		
CO2	L	М	М	L	М	М	L	S	М	S		
CO3	L	L	L	L	М	М	М	S	М	S		
CO4	L	L	L	L	М	М	М	S	М	S		
CO5	М	М	S	S	М	S	S	М	S	S		

code	21CSESE04	THREAT INTELLIGENCE	L	Т	Р	0
Core/Elect	ive/Supportive	Elective	4			4
Pre-1	requisite	Information Security Assets, Attacks and Vulnerabilities	Syllabu s Version	202	1-20	22
Course (	Objectives:					
	objectives of thi					
1. To	understand Three	at Intelligence, Threat Intelligence types and	l LifeCycle	•		
		apply Threat detection and prevention.				
3. To	analyze and buil	d secure methods to preventthreats.				
	~ ~ ~					
<b>^</b>	l Course Outcor					
		ion of the course, student will be able to:		TZ	-	
		nreats, intelligence types.		K		
	-	s of a threat intelligence life cycle.		K2		
		ypes of threats and its features.	1	K		_
	· · ·	and evaluate the efficiency of secure method	ds to	K	2-K	5
	t and prevent three	ent the secure methods in real life scenarios.		V	3-K	6
	•	ate the effective detection and prevention n			. <u>3-k</u> 2, K	
		derstand; K3 - Apply; K4 - Analyze; K5 - E				
	<u>iember</u> , <b>K2</b> - On	derstand, KS - Appry, K4 - Anaryze, K5 - L		0 - CI	carc	/
Unit:1	I	ntroduction to Threat Intelligence	14	12h	our	s
		TI, Benefits and challenges of Threat Inform	nation Shar			-
	yber Threat Info			U,		
	•		76			
Unit:2		Thr <mark>eat Inte</mark> lligence Life Cycle		12h	our	s
Phases of	Life cycle, Dire	Threat Intelligence Life Cycle ction, Collection, Processing, Analysis, Diss	seminationa		our	s
	É Life cycle, Dire	ction, Collection, Processing, Analysis, Diss	seminationa		our	5
Phases of Feedback.		ction, Collection, Processing, Analysis, Diss	semination	and		The second se
Phases of Feedback. Unit:3		ction, Collection, Processing, Analysis, Diss Types of Threat Intelligence		and 12h	our	The second se
Phases of Feedback. <b>Unit:3</b> Strategic	, Threat Intelligen	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> .ce, tactical Threat Intelligence, operational		and 12h	our	The second se
Phases of Feedback. <b>Unit:3</b> Strategic		ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> .ce, tactical Threat Intelligence, operational		and 12h	our	The second se
Phases of Feedback. Unit:3 Strategic and techni	Threat Intelligen	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational ' gence.		and 12h Iligen	our: ce,	5
Phases of Feedback. Unit:3 Strategic and techni Unit:4	Threat Intelligen cal Threat Intelli App	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> .ce, tactical Threat Intelligence, operational ' gence. <b>Dications of Threat Intelligence</b>	Threat Inte	nd 12h Iligen 14h	our: ce, our:	<b>S</b>
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat Ir	Threat Intelligen cal Threat Intelligen App ntelligence for S	Ction, Collection, Processing, Analysis, Diss Types of Threat Intelligence ce, tactical Threat Intelligence, operational 'gence. Dications of Threat Intelligence Security Operations, Threat Intelligence for the formation of the fo	Threat Inte	12h lligen 14h Resp	our: ce, our: our:	s s e,
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat In Threat Inte	Threat Intelligen cal Threat Intelligen App ntelligence for S elligence for Vul	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> .ce, tactical Threat Intelligence, operational ' gence. <b>Dications of Threat Intelligence</b>	Threat Inte	12h 12h Iligen 14h Resp ty Le	ours ce, ours oons ader	s s .e,
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat Int Risk Analy	Threat Intelligen cal Threat Intelligen delligence for S elligence for Vul ysis, Threat Intell	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence	Threat Inte	12h 12h Iligen 14h Resp ty Le	ours ce, ours oons ader	s s .e,
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat In Threat In Risk Analy Third Part	Threat Intelligen cal Threat Intelligen al Threat Intelligence for S celligence for Vul ysis, Threat Intelligence Intelligence for Vul	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational ' gence. <b>Dications of Threat Intelligence</b> decurity Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence telligence for Digital Risk Protection.	Threat Inte	12h Iligen 14h Resp ty Le educin	ours ce, ours cons ader ng	s s s s,
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat In Threat Int Risk Analy Third Part Unit:5	Threat Intelligen cal Threat Intelligen cal Threat Intelligence for S elligence for Vul ysis, Threat Intelly y Risk, Threat In	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence telligence for Digital Risk Protection. <b>Threat Intelligence Use cases</b>	Threat Inte or Incident of or Securi gence for Re	12h 12h 11igen 14h Resp ty Le educin 10h	ours ce, ours oons ader ng	s s e, s,
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat Int Risk Analy Third Part Unit:5 Machine	Threat Intelligen cal Threat Intelligen cal Threat Intelligence for S elligence for Vul ysis, Threat Intellig y Risk, Threat In learning for bette	Ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational 'gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence for Fraud Prevention, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence telligence for Digital Risk Protection. <b>Chreat Intelligence Use cases</b> er Threat Intelligence, Threat Intelligence use	Threat Inte or Incident of or Securi gence for Re	12h 12h 11igen 14h Resp ty Le educin 10h	ours ce, ours oons ader ng	s s e, s,
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat Int Risk Analy Third Part Unit:5 Machine	Threat Intelligen cal Threat Intelligen cal Threat Intelligence for S elligence for Vul ysis, Threat Intellig y Risk, Threat In learning for bette	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence telligence for Digital Risk Protection. <b>Threat Intelligence Use cases</b>	Threat Inte or Incident of or Securi gence for Re	12h 12h 11igen 14h Resp ty Le educin 10h	ours ce, ours oons ader ng	s s e, s,
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat In Threat In Risk Analy Third Part Unit:5 Machine fraud, Con	Threat Intelligen cal Threat Intelligen cal Threat Intelligence for S elligence for Vul ysis, Threat Intellig y Risk, Threat In learning for bette	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence ligence for Digital Risk Protection. <b>Threat Intelligence Use cases</b> er Threat Intelligence, Threat Intelligence us Typo squatting and fraudulent domains.	Threat Inte or Incident of or Securi gence for Re	12h 12h Iligen 14h Resp ty Le educin 10h /ment	ours ce, oons ader ng ours	s s e, s s
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat Int Risk Analy Third Part Unit:5 Machine fraud, Con	Threat Intelligen cal Threat Intelligen cal Threat Intelligence for S elligence for Vul ysis, Threat Intelly y Risk, Threat In learning for bette npromised data, 7	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> .ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence ligence for Digital Risk Protection. <b>Threat Intelligence Use cases</b> er Threat Intelligence, Threat Intelligence us Typo squatting and fraudulent domains. <b>Contemporary Issues</b>	Threat Inte	12h 12h Illigen 14h Resp ty Le educin 10h yment	ours ce, ours oons ader ng	s s e, s s
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat Int Risk Analy Third Part Unit:5 Machine fraud, Con	Threat Intelligen cal Threat Intelligen cal Threat Intelligen telligence for Vul ysis, Threat Intelligence for Vul ysis, Threat Intelligence for Vul ysis, Threat Intelligence for Vul grisk, Threat Intelligence for better promised data, The solution of the solution of the solution promised data, The solution of the so	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence ligence for Digital Risk Protection. <b>Threat Intelligence Use cases</b> er Threat Intelligence, Threat Intelligence us Typo squatting and fraudulent domains.	Threat Inte	12h 12h Illigen 14h Resp ty Le educin 10h yment	ours ce, oons ader ng ours	s s e, s s
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat In Threat Int Risk Analy Third Part Unit:5 Machine fraud, Con Unit:6 Advantage	Threat Intelligen cal Threat Intelligen cal Threat Intelligen telligence for Vul ysis, Threat Intelligence for Vul ysis, Threat Intelligence for Vul ysis, Threat Intelligence for Vul grisk, Threat Intelligence for better promised data, The solution of the solution of the solution promised data, The solution of the so	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> .ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence ligence for Digital Risk Protection. <b>Threat Intelligence Use cases</b> er Threat Intelligence, Threat Intelligence us Typo squatting and fraudulent domains. <b>Contemporary Issues</b>	Threat Inte	12h 12h Illigen 14h Resp ty Le educin 10h yment	ours ce, oons ader ng ours	s s e, s s
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat In Threat Int Risk Analy Third Part Unit:5 Machine fraud, Con Unit:6 Advantage	Threat Intelligen cal Threat Intelligen cal Threat Intelligen telligence for Vul ysis, Threat Intelligence for Vul ysis, Threat Intelligence for Vul ysis, Threat Intelligence for Vul grisk, Threat Intelligence for better promised data, The solution of the solution of the solution promised data, The solution of the so	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> .ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence ligence for Digital Risk Protection. <b>Threat Intelligence Use cases</b> er Threat Intelligence, Threat Intelligence us Typo squatting and fraudulent domains. <b>Contemporary Issues</b>	Threat Inte	12h 12h 11igen 14h Resp ty Le educin 10h ment 2 d the	ours ce, oons ader ng ours	s s s rs
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat Int Risk Analy Third Part Unit:5 Machine fraud, Con Unit:6 Advantage	Threat Intelligen cal Threat Intelligen cal Threat Intelligence for Selligence for Vul ysis, Threat Intelly y Risk, Threat Intelly p Risk, Threat Intelly learning for better npromised data, 7	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence ligence for Digital Risk Protection. <b>Threat Intelligence Use cases</b> er Threat Intelligence, Threat Intelligence us Typo squatting and fraudulent domains. <b>Contemporary Issues</b> ing, Cyber Kill Chain, The role of private C	Threat Inte	12h 12h 11igen 14h Resp ty Le educin 10h ment 2 d the	ours ce, ours cons ader ng ours	s s s rs
Phases of Feedback. Unit:3 Strategic and techni Unit:4 Threat Int Risk Analy Third Part Unit:5 Machine fraud, Con Unit:6 Advantage Dark web.	Threat Intelligen cal Threat Intelligen cal Threat Intelligence for S elligence for Vul ysis, Threat Intelly y Risk, Threat In learning for bette npromised data, T es of Threat Hunt s)	ction, Collection, Processing, Analysis, Diss <b>Types of Threat Intelligence</b> ce, tactical Threat Intelligence, operational gence. <b>Dications of Threat Intelligence</b> Security Operations, Threat Intelligence for nerability Management, Threat Intelligence ligence for Fraud Prevention, Threat Intelligence ligence for Digital Risk Protection. <b>Threat Intelligence Use cases</b> er Threat Intelligence, Threat Intelligence us Typo squatting and fraudulent domains. <b>Contemporary Issues</b> ing, Cyber Kill Chain, The role of private C	Threat Inte	12h Illigen 14h Resp ty Le educin 10h /ment 2 d the 62	ours ce, oons ader ng ours hou	s s s s rs

2	Florian Skopik, "Collaborative Cyber Threat Intelligence: Detecting and Responding to						
	Advanced Cyber Attacks at the National Level", CRC Press, 2017						
3	Christopher Ahlberg, "The Threat Intelligence Handbook : A Practical Guidefor						
	Security Teams to Unlocking the Power of Intelligence", CyberEdge Group, 1997						
R	eference Books : EBooks						
1	https://paper.bobylive.com/Security/threat-intelligence-handbook-second-edition.pdf						
2	https://cyber-edge.com/wp-cont <mark>ent/uploads</mark> /2018/11/Recorded-Future-eBook.pdf						
3	https://books.google.co.in/books?id=cyE6DwAAQBAJ&printsec=frontcover&source=gb						
	s_ge_summary_r&ca <mark>d=0#v=onepage&amp;q&amp;f=false</mark>						
R	elated Online Contents [MOOC, SWAYAM, NPTEL, Websites etc.]						

	<b>Course Title</b>	Duration	Provider
1	Cyber Threat Intelligence	5 weeks	Coursera (IBM)
W	eb link		
	1. <u>https://www.fireeye.com/</u>		
	2. <u>https://www.ibm.com/in-en/security</u>		
Cou	urse Designed by: Dr.M. Punithavalliand CSCC Labs		
		1 3 1 1	

Mapp	Mapping with Programme Outcomes									
COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	L	М	М	М	cont <b>L</b> e	М	L	S	М	S
CO2	М	М	S	S	М	L	L	S	М	S
CO3	М	М	S	S	М	L	L	S	М	S
CO4	S	М	S	S	S	М	М	S	М	S
CO5	S	S	S	S	М	М	М	S	М	S

	21CSESE05	Cyber Law	L	Т	Р	C		
Core/Electiv	e/Supportive	Core	4	0	0	4		
Pre-re	equisite	IPC, IT ACT and Criminal ACTSyllabus Version202						
Course Obj	ectives:							
The main ob	jectives of this c	course are to:						
1. Unde	rstand the basic	s of Cyber Crime.						
		Law and Regulation of Cyberspace and Hu	ımanRights.					
3. Unde	rstand the Cybe	r Security Policy ofIndia.						
Expected Co	ourse Outcome	s:						
-		ion of the course, student will be able to:						
	tand Basics of C				K			
		al Law and Regulation of Cyberspace and I	Human Rights	5	K			
0	ssues of Interce	pting WiFi Transmissions			K K			
		ive versus Post-mortem"			K			
		derstand; K3 - Apply; K4 - Analyze; K5 - E	Evaluate; <b>K6</b> –	Cre				
Unit:1		Basics of Cyber <mark>crime</mark>			2 hou			
		Psychology: Introduction – Cyberbullying,						
Cyberstalki	ng – Revenge I	Pornography, Sexting, Sextortion and Rel	ated Offence	s - [	Fackli	ng		
Offensive	Online Commu	inications and Abuse. Why Cybercrime	Occurs: In	trodu	uction	_		
			Occurs. In	uou				
Rational C	hoice Theories:							
		Deterrence Theory and Routine Activit	y Theory -	Self	-Cont	rol		
Theory - G			y Theory -	Self	-Cont	rol		
		Deterrence Theory and Routine Activit	y Theory -	Self	-Cont	rol		
Theory - G Theories. Unit:2	eneral Strain Tl	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law	y Theory - ed Concepts -	Self Sut	-Cont ocultu 0 hou	rol ral		
Theory - G Theories. Unit:2 Introductio	eneral Strain Tl H bn: Perspectives	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge	y Theory - ed Concepts - s for Interna	Self Sub	-Cont ocultu 0 hou al La	rol ral <b>Irs</b> w:		
Theory - G Theories. Unit:2 Introduction Perspectives	eneral Strain Tl	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge rs - General Introduction to Public International	y Theory - ed Concepts - s for Interna ational Law -	Self Sub 1 ution Jur	-Cont ocultu 0 hou al La isdicti	rol ral <b>Irs</b> w: on		
Theory - G Theories. Unit:2 Introduction Perspectives	eneral Strain Tl	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge	y Theory - ed Concepts - s for Interna ational Law -	Self Sub 1 ution Jur	-Cont ocultu 0 hou al La isdicti	rol ral <b>Irs</b> w: on		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu	eneral Strain Tl bn: Perspectives s of Stakeholde attion of State	E Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge ers - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio	y Theory - ed Concepts - s for Interna ational Law - n - Attributi	Self Sub 1 ution Jur	-Cont ocultu 0 hou al La isdicti of St	rol ral <b>Irs</b> w: on ate		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil	eneral Strain Tl bn: Perspectives s of Stakeholdention of Statention ity. Regulation	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge rs - General Introduction to Public International	y Theory - ed Concepts - s for Interna ational Law - n - Attributi ral Backgrou	Self Sub 1 ution Jur	-Cont ocultu 0 hou al La isdicti of St	rol ral <b>Irs</b> w: on ate		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C	eneral Strain Tl bn: Perspectives s of Stakeholdention of Statention ity. Regulation	E Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate <b>Human Rights and International Law</b> s of Various Stakeholders and Challenge rrs - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Right	y Theory - ed Concepts - s for Interna ational Law - n - Attributi ral Backgrou	Self Sub 1 ntion Jur on nd -	Ont ocultu 0 hou al La isdicti of St Hum	rol ral w: on ate		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3	eneral Strain Tl bon: Perspectives s of Stakeholde ation of State ity. Regulation yberspace – Exc	E Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge rs - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Rights	y Theory - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection.	Self Sub 1 ntion Jur on nd -	Ont ocultu al La isdicti of St Hum	rol ral w: on ate an		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3 Cyber Inv	eneral Strain The method of Stakeholde ition of State ity. Regulation yberspace – Exconstruction estigative Roles	E Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge ors - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber	y Theory - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest	Self Sub 1 ntion Jur on nd - 1 igato	-Cont ocultu al La isdicti of St Hum 4 hou	rol ral w: on ate an <b>Irs</b>		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in Cy Unit:3 Cyber Inv Role of Lav	eneral Strain Tl bon: Perspectives s of Stakeholde ition of State ity. Regulation yberspace – Exc estigative Roles v Enforcement	E Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge rs - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Rights	y Theory - ed Concepts - ed Concepts - s for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden	Self Sub <u>1</u> Attion Jur on on - <u>1</u> iigato	-Cont ocultu 0 hou al La isdicti of St Hum -4 hou or - T espon	rol ral w: on ate an <b>Irs</b> 'he se:		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3 Cyber Inv Role of Law LiveForensi	eneral Strain Tl I Dri: Perspectives s of Stakeholde ation of State ity. Regulation yberspace – Exc estigative Roles v Enforcement of csandInvestigat	E Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge rrs - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber Officers - The Role of the Prosecuting Atto	y Theory - ed Concepts - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden oday'sLiveM	Self Sub 1 ation Jur on o nd - igato nt Ro etho	-Cont ocultu <b>0 hou</b> al La isdicti of St Hum - <u>4 hou</u> or - T espon ds.Le	rol ral w: on ate an the se: gal		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3 Cyber Inv Role of Law LiveForensi Issues of I	eneral Strain The method of Stakeholde ition of State ity. Regulation yberspace – Exc estigative Roles v Enforcement csandInvestigat ntercepting Wi	E Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge ers - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber Officers - The Role of the Prosecuting Atta ions-Post-mortem versusLiveForensics-T	y Theory - ed Concepts - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden oday'sLiveM nderstanding	Self Sub 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-Cont ocultu al La isdicti of St Hurr -4 hou or - T espon ds.Le Fi RE	rol ral w: on ate an <b>urs</b> 'he se: gal		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3 Cyber Inv Role of Lav LiveForensi Issues of I Scanning R	eneral Strain The method of Stakeholde ition of State ity. Regulation yberspace – Exc estigative Roles v Enforcement csandInvestigat ntercepting Wi	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge rs - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber Officers - The Role of the Prosecuting Atta ions-Post-mortem versusLiveForensics-T Fi Transmissions: WiFi Technology - U ing on WiFi - Fourth Amendment Expectation	y Theory - ed Concepts - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden oday'sLiveM nderstanding	Self Sub 1 ntion Jur on on on d - 1 nt Ro etho Will inW	-Cont ocultu <b>0 hou</b> al La isdicti of St Hum <b>4 hou</b> or - T espon ds.Le Fi RH /LAN	rol ral w: on ate an The se: gal s.		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in Cy Unit:3 Cyber Inv Role of Lav LiveForensi Issues of I Scanning R	eneral Strain Tl bn: Perspectives s of Stakeholde ition of State ity. Regulation yberspace – Exc estigative Roles v Enforcement csandInvestigat ntercepting Wi F - Eavesdroppi	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge rrs - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: General ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber Officers - The Role of the Prosecuting Atta ions-Post-mortem versusLiveForensics-T Fi Transmissions: WiFi Technology - U ing on WiFi - Fourth Amendment Expectation Cybercrime investigations	y Theory - ed Concepts - ed Concepts - s for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden 'oday'sLiveM nderstanding on of Privacy	Self Sub 1 ntion Jur on on on d - 1 igato nt Ro etho Will inW	-Cont ocultu <b>0 hou</b> al La isdicti of St Hum <b>4 hou</b> or - T espon ds.Leg Fi RF /LAN <b>2 hou</b>	rol ral w: on ate an The se: gal F - s.		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3 Cyber Inv Role of Lav LiveForensi Issues of I Scanning R Unit:4 Conducting	eneral Strain Tl minimum Ferspectives s of Stakeholde ition of State ity. Regulation yberspace – Exc estigative Roles v Enforcement csandInvestigat ntercepting Wi F - Eavesdroppi Cyber Investig	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge rrs - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber Officers - The Role of the Prosecuting Atta ions-Post-mortem versusLiveForensics-T Fi Transmissions: WiFi Technology - U ing on WiFi - Fourth Amendment Expectati Cybercrime investigations ations: Demystifying Computer/Cyber Cr	y Theory - ed Concepts - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden Oday'sLiveM nderstanding on of Privacy	Self Sub 1 attion Jur on Jur on on Jur igato trigato trigato Will in W	-Cont ocultu al La isdicti of St Hum -4 hou or - T espon ds.Le Fi RI /LAN -2 hou ding	rol ral w: on ate an The se: gal $\overline{z} = -$ s. IP		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3 Cyber Inv Role of Lav LiveForensi Issues of I Scanning R Unit:4 Conducting Addresses - '	eneral Strain The Image of State on: Perspectives s of Stakeholde ation of State ity. Regulation yberspace – Exc westigative Roles wenforcement csandInvestigat ntercepting Wi F - Eavesdroppi Cyber Investig The Explosion of	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge rrs - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: General ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber Officers - The Role of the Prosecuting Atta ions-Post-mortem versusLiveForensics-T Fi Transmissions: WiFi Technology - U ing on WiFi - Fourth Amendment Expectation Cybercrime investigations	y Theory - ed Concepts - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden 'oday'sLiveM nderstanding on of Privacy	Self Sub 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-Cont ocultu al La isdicti of St Hum 	rol ral w: on ate an The se: gal S. IP nal		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in Cy Unit:3 Cyber Inv Role of Lav LiveForensi Issues of I Scanning R Unit:4 Conducting Addresses - ' Communicat	eneral Strain Tl mini Perspectives s of Stakeholde ition of State ity. Regulation yberspace – Exc estigative Roles v Enforcement csandInvestigat ntercepting Wi F - Eavesdroppi Cyber Investig The Explosion of ion. Digital For	Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge ors - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber Officers - The Role of the Prosecuting Atto ions-Post-mortem versusLiveForensics-T Fi Transmissions: WiFi Technology - U ing on WiFi - Fourth Amendment Expectati Cybercrime investigations ations: Demystifying Computer/Cyber Cri of Networking - The Explosion of Wireless	y Theory - ed Concepts - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden 'oday'sLiveM nderstanding on of Privacy	Self Sub 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-Cont ocultu al La isdicti of St Hum 	rol ral w: on ate an The se: gal S. IP nal		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3 Cyber Inv Role of Lav LiveForensi Issues of I Scanning R Unit:4 Conducting Addresses - ' Communicat Phases of Dig	eneral Strain Tl mini Perspectives s of Stakeholde ition of State ity. Regulation yberspace – Exc estigative Roles v Enforcement csandInvestigat ntercepting Wi F - Eavesdroppi Cyber Investig The Explosion of ion. Digital For	E Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge ers - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber Officers - The Role of the Prosecuting Atto ions-Post-mortem versusLiveForensics-T Fi Transmissions: WiFi Technology - U ing on WiFi - Fourth Amendment Expectation Cybercrime investigations ations: Demystifying Computer/Cyber Cr of Networking - The Explosion of Wireless rensics and Analyzing Data: The Evolution - Examination – Analysis – Reporting.	y Theory - ed Concepts - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden 'oday'sLiveM nderstanding on of Privacy	Self Sub 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-Cont ocultu al La isdicti of St Hurr -4 hou or - T espon ds.Leg Fi RF /LAN -2 hou ading person rensic	rol ral w: on ate an the se: gal 7 - s. IP nal s -		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3 Cyber Inv Role of Lav LiveForensi Issues of I Scanning R Unit:4 Conducting Addresses - ' Communicat Phases of Dig	eneral Strain The second state of Stakeholde of Stakeholde of State of State of State of State of State of Stakeholde of State of Stakeholde of State of Stakeholde of State of Stakeholde of State of State of Stakeholde of Stakehol	<ul> <li>Deterrence Theory and Routine Activity heory - Social Learning Theory and Relate</li> <li>Human Rights and International Law</li> <li>s of Various Stakeholders and Challenge</li> <li>ars - General Introduction to Public International Responsibility in Cyberspace: Jurisdiction</li> <li>of Cyberspace and Human Rights: Generations - Territorial Scope of Human Right</li> <li>Cybercrime Roles</li> <li>s - Understanding Your Role as a Cyber</li> <li>Officers - The Role of the Prosecuting Attaines</li> <li>s - Understanding Your Role as a Cyber</li> <li>Officers - The Role of the Prosecuting Attaines</li> <li>Fi Transmissions: WiFi Technology - U</li> <li>ung on WiFi - Fourth Amendment Expectation</li> <li>Cybercrime investigations</li> <li>ations: Demystifying Computer/Cyber Criptor</li> <li>of Networking - The Explosion of Wireless</li> <li>rensics and Analyzing Data: The Evolution - Examination – Analysis – Reporting.</li> </ul>	y Theory - ed Concepts - ed Concepts - es for Interna ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden oday'sLiveM nderstanding on of Privacy	Self Sub 1 ation Jur on Jur on on d - 1 igato tetho Will inW 1 rstan nter r For 1	-Cont ocultu al La isdicti of St Hum 	rol ral w: on ate an the se: gal 3 - s. IP nal s - urs		
Theory - G Theories. Unit:2 Introduction Perspectives and Attribu Responsibil Rights in C Unit:3 Cyber Inv Role of Lav LiveForensi Issues of I Scanning R Unit:4 Conducting Addresses - ' Communicat Phases of Dig Unit:5 Cyber Sec Introduction	eneral Strain The solution of State solution of State solution of State stigative Roles were been been been been been been been b	E Deterrence Theory and Routine Activit heory - Social Learning Theory and Relate Human Rights and International Law s of Various Stakeholders and Challenge ers - General Introduction to Public Interna Responsibility in Cyberspace: Jurisdictio of Cyberspace and Human Rights: Gener ceptions - Territorial Scope of Human Right Cybercrime Roles s - Understanding Your Role as a Cyber Officers - The Role of the Prosecuting Atto ions-Post-mortem versusLiveForensics-T Fi Transmissions: WiFi Technology - U ing on WiFi - Fourth Amendment Expectation Cybercrime investigations ations: Demystifying Computer/Cyber Cr of Networking - The Explosion of Wireless rensics and Analyzing Data: The Evolution - Examination – Analysis – Reporting.	y Theory - ed Concepts - ed Concepts - es for Interna- ational Law - n - Attributi ral Backgrou s Protection. Crime Invest orney. Inciden Yoday'sLiveM nderstanding on of Privacy time - Under Networks - I of Computer	Self Sub 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-Cont ocultu al La isdicti of St Hum 	rol ral w: on ate an <b>urs</b> he se: gal Ts is. IP nal s - <b>urs</b> ine:		

	-	- tools Used for Cyber Crime – Other Cyber Crime Methods – C	Connection between					
	unit:6	nd Cyber Crime. Cyber Crime and Punishment. Contemporary Issues	2 hours					
		ive versus Post-mortem	2 11041 5					
Cub	e Brudy.L							
		Total Lecture hours	62 hours					
F	Reference							
1	National	Cyber Crime Reference Handbook, AICTE, National Cyber Safe	ety and Security					
		ls, Ministry of Social Justice and Empowerment, MSME, Govt of	•					
2		riminology, Series Editor, Anthony J. Masys, Humanitarian Assis						
	•	nd Security, University of South Florida, Tampa, USA, Springer (						
3	Public Ir	iternational Law of Cyberspace - Law, Governance and Technolog	bgy Series 32,					
		litors, Pompeu Casanovas, Giovanni Sartor, Springer(2017)						
4	Cyber C	rime Investigations, Anthony Reyes, Syngress Publishing, Inc (20	007).					
F	Related O	nline Contents [MOOC, SWAYAM, NPTEL, Websites etc.]						
1		nlinecourses.swayam2.ac.in/cec20_cs09/preview_						
2	_	ww.coursera.org/lecture/cyber-conflicts/introduction-to-cybercri	me-and-					
		ental-issues-xndSq						
3		ww.bu.edu/online/programs/certificate-programs/cybercrime-inv	vestigation-					
	cybersec							
4								
5	https:/	//www.udemy.com/course/ifci-expert-cybercrime-investigators-co	ourse/					
V	Veb Link							
1.	https://c	<u>ybercrime.gov.in/</u>						
2.								
3.		ybercrime.gov.in/						
C	Course De	signed By: MrS.Palanisamy						

Mappi	Mapping with Programme Outcomes									
COs	PO1	PO2	PO3	PO4	PO5	PO6	<b>PO7</b>	PO8	PO9	PO1 0
CO1	M	S	М	S	М	М	М	S	М	S
CO2	S	L	S	S	S	М	М	S	S	M
CO3	S	S	М	S	М	М	S	L	S	S
CO4	M	S	S	S	S	S	S	S	S	L
CO5	S	S	S	S	S	S	S	S	S	М

Course code		21CSESE06	ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING	L	Т	Р	C				
<b>Core/Elective/Supportive</b>		ve/Supportive	Elective	4		4					
	Dro r	equisite	Basics of Mathematical Probabilities and	nd Syllabus <sub>20</sub> 2			1-2022				
	rre-r	equisite	Computer Programming	Vers	ion	2021	1-2022				
Cour	se Ob	jectives:									
		• 1	ems, both technical and philosophical, in the o	levelo	pme	nt of					
		ialintelligence									
			cepts of Machine learning algorithms of differ	rent pr	obab	ilistic	:,rE				
Expe		Course Outcome									
CO1	sol	ving and learning	•			K1					
CO2		nderstand the pro plicable	blems where artificial intelligence techniques	are		K2	ļ.				
CO3	1 1		of machine learning			K2					
<b>CO</b> 4			oretical concepts of probabilistic and linear			<b>T</b> 7 4					
CO4		thods	1 1			K4	•				
CO5	D	istinguish Superv	vised, Unsupervised and semi supervised learn	ing		K4,	K3,K5				
K1	- Rer	nember; <b>K2</b> - Un	derstand; K3 - Apply; K4 - Analyze; K5 - Ev	aluate	; K6	– Cre	ate				
Un	it:1	Artificial In	telligence		-	12—h	nours				
Intro	oducti	on to Artificial Ir	ntelligence – Intelligent Agents – Problem sol	ving –	Solv	ving					
			earch in complex environments – Adversarial				ies –				
Con	strain	ts Satisfaction Pr	oblems	1							
			A DIE DEA	1							
	it:2		, reasoning and planning				nours				
			-Order Logic – Inference in First –Order								
			ed Pla <mark>nning –</mark> Uncertain knowledge and rea								
		ty – Probabilistic	Reasoning – Probabilistic Programming – M	ulti Ag	gent i	Decis	ion				
Mak	ting	100	Constant and and	- 8		88	14				
				-		1					
	it:3	Machine Lear		100			hours				
			tions – Overview – applications - Types of ma								
			ing Examples of Machine Learning -Applica				lodels				
			sis Function Models - The Bias-Variance Dec	ompos	sitior	1-					
Bay	esian	Linear Regressio	n - Bayesian Model Comparison								
			A Barrier all Pr	1 and a state							
	it:4	Models for Cl	THE STATE OF THE S				nours				
			r Models for Classification - Discriminant Fu								
			babilistic Discriminative Models - Bayesian	0		0					
			ation Trees- Regression Trees - Pruning. Ne								
			s - Error Back propagation - Regularization -								
	Bayesian Neural Networks - Kernel Methods - Dual Representations - Radial Basis Function										
	Networks. Support Vector Machines - Ensemble methods- Bagging Boosting – Evaluation Methods										
B00	sung	- Evaluation Met	11008								
TT	.i+.5	Clustoring				12—ł	NOU PC				
	it:5	Clustering	lustering- K-means - EM - Mixtures of Gauss	iona			nours				
	-	U U	del selection for latent variable models - high				0000				
U U			lity - Dimensionality Reduction - Factor anal			-	aces -				
			babilistic PCA- Independent components anal	-		ipai					
	Pone	<u>11. 7 mai y 515 - 1 10</u>	such such a set independent components and	9010							

	Unit:	6 Contemporary Issues		2 hours					
		al Considerations in Machine Learning Applicati	ons – Ethics and	Challenges of AI and					
	ML as	disruptive technology Use cases – Webinars							
			ecture hours	62—hours					
	ext Boo								
1									
2		vin P. Murphy, "Machine Learning: A Probabilis							
3		emAlpaydin, "Introduction to Machine Learning	g 3(Adaptive Con	nputation and					
	Mac								
		arning Series)", Third Edition, MIT Press, 2014							
4		m M Mitchell, "Machine Learning", First Edition							
5		art Russell and Peter Norvig, "Artificial Intellige	ence: A Modern A	Approach", Fourth					
		on, 2020.							
		e Books							
1		nesKlaas, "Machine Learning for Finance", ISB	- (MC)(0)						
_		iseppe Bonaccors <mark>o, "Machine Learning Algorith</mark>	ms", Second Edi	tion, ISBN:					
2		31789347999, 2018 [Packt]							
3	Ste	phen Marsland, "Machine Learning –An Algorit	hmic Perspective	", CRC Press, 2009					
4	Ha Spri	stie, Tibshirani, Friedman, "The Elements of Standard Revenues of S	tistical Learning	, Second Edition,					
5	Yu	xi Liu, "Pyth <mark>on Mac</mark> hine Learning By Example"	, 2017 [Packt]	· /					
6		in Paul Mueller, Luca Massaron, "Machine Lear Edition, Wiley Publisher, ISBN: 978812656305		nd R) For Dummies",					
7		Dinesh Kumar ManaranjanPradhan,,"Mach lisher: Wiley, ISBN: 9788126579907, 2019	nine Learning	using Python". )					
	Onlir	ne Course:	1.37	1					
S	S.No	Course Title	Duration	Provider – Free					
	1.	AI for Everyone	4 Weeks	Coursera					
	2.	AI for Everyone: Master the Basics	4 Weeks	edX					
	3.	Introduction to Artificial Intelligence	16 Weeks	Udacity					
	4.	Machine Learning : Regression	6 Weeks	Coursera					
	5.	Introduction to Machine Learning	12 Weeks	Swayam – NPTEL					
	6	Deep Learning Specialization	4 Courses	Coursera					

## Web Link - Video:

1. https://www.packtpub.com/data/hands-on-machine-learning-with-scikit-learn-and-tensorflow-2-0-video

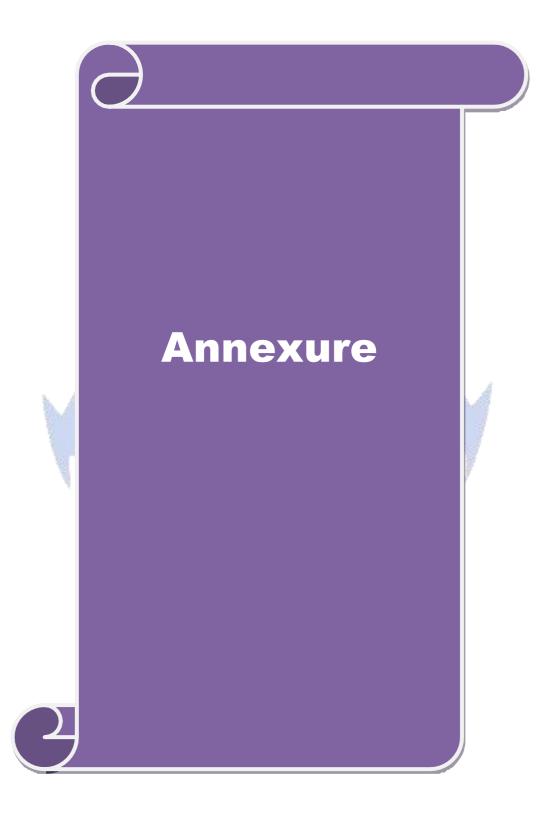
2. https://www.packtpub.com/data/machine-learning-projects-with-tensorflow-2-0-

video3.https://www.packtpub.com/application-development/complete-machine-learning-course-python-video

Mapp	ing with F	Programm	e Outcon	nes						
COs	<b>PO1</b>	PO2	PO3	PO4	PO5	PO6	<b>PO7</b>	<b>PO8</b>	PO9	PO10
CO1	М	S	М	S	L	L	М	L	S	L
CO2	М	S	L	S	М	М	L	L	S	S
CO3	S	S	L	L	L	L	L	L	L	L
<b>CO4</b>	S	S	S	S	L	L	М	М	М	L
CO5	S	S	S	L	L	L	L	L	L	L

\*S-Strong; M-Medium; L-Low

Students have to undergo One Job Oriented Course and one Value added course every year.



# **M.Sc. Cyber Security**

## Syllabus With effect from 2021-22

# **Program Code :**



DEPARTMENT OF COMPUTER APPLICATIONS Bharathiar University (A State University, Accredited with "A" Grade by NAAC and 13<sup>th</sup> Rank among Indian Universities by MHRD-NIRF) Coimbatore 641 046, INDIA

## BHARATHIAR UNIVERSITY, COIMBATORE-641 046 DEPARTMENT OF COMPUTER APPLICATIONS

## M.Sc. CYBER SECURITY 2021-2022 – (CBCS) University Dept. in collaboration with CSCC Labs (Effective from the academic Year 2021-2022)

## 1. Eligibility forAdmission

A pass in any Bachelors degree of minimum 3 years duration with Mathematics or Statistics as any one of the subjects at Graduate level.

## 2. Duration

The programme shall be offered on a full-time basis for two years. The students will undergo the programme in Bharathiar University campus for the first three semesters and will undertake project work in the fourthsemester.

## 3. Regulations

The general Regulations of the Bharathiar University Choice Based Credit System Programme are applicable to these programmes.

## 4. The Medium of Instruction and Examinations

The medium of instruction and Examinations shall be in English.

## 5. Submission of Record Notebooks for Practical Examinations & Project Viva-Voce.

Candidates taking the Practical Examinations should submit bonafide Record Note Books prescribed for the Examinations. Otherwise the candidates will not be permitted to take the Practical Examinations. Candidates taking the practice School / Project & Viva -Voce Examination should submit Project Report prescribed for the Examinations. Otherwise the candidates will not be permitted to take up the Project & Viva-voceExamination.

Students carry out Case Studies /Mini-projects and finishing school / major project and the schedule for review meetings are as givenbelow:

	First Review	Second Review
Case Studies / Mini Projects	Thursday of first week in June	Thursday of first week in August
Practice School / MajorProject	Friday of first week of February	Friday of first week of April

#### Table: Schedule for Review Meetings

## 6. Ranking

A candidate who qualifies for the PG Degree Course passing all the Examinations in the first attempt, within the minimum period prescribed for the Course of Study from the date of admission to the Course and secures 1<sup>st</sup> or 2<sup>nd</sup> Class shall be eligible for ranking and such ranking will be confined to 10% of the total number of candidates qualified in that particular subject to a maximum of 10ranks.

## 7. Revision of Regulations and Curriculum

The above Regulation and Scheme of Examinations will be in vogue without any change for a minimum period of three years from the date of approval of the Regulations. The University may revise/amend/ change the Regulations and Scheme of Examinations, if foundnecessary.



## BHARATHIAR UNIVERSITY : : COIMBATORE 641046 DEPARTMENT OF COMPUTER APPLICATIONS

## MISSION

- To impart practical knowledge and professional skills in the area of computer applications to students to make them industryready.
- To contribute to the advancement of knowledge in the field of Computer Applications through research.
- To involve the students in societal contributions to make them aware of the society and itsneeds.

