Roll No..... Total No. of Pages: 06

END TERM EXAMINATION EIGHTH SEMESTER 2015-16 HUL-2401 - Cyber Security

	HUL-240	of - Capel Security	
Time allowed: 3 Hrs. General Instructions:			Max. Marks: 100
1. All questions are compuls	ory		
2. Each question carry one n	nark		
3. There is no negative mark	king		
1. In computer security, mea	ans that computer syste	m assets can be modified only b	y authorized parities.
A) Confidentiality	B) Integrity	C) Availability	D) Authenticity
2. In computer security, mea	ans that the information	n in a computer system only be a	accessible for reading by
A) Confidentiality	B) Integrity	C) Availability D) A	Authenticity
3. Which of the following is	independent malicious	program that need not any host	program?
A) Trap doors	B) Trojan Horse	e C) Virus	D) Worm
4. The Is code that re user ID of by unlikely seque		equence of input or is triggered	by being run from a certain
A) Logic Bomb 5. Theis code em are met.	B) Virus bedded in some legitima	C) Trojan Horse ate program that is set to "explo	D) Trap doors ode" when certain conditions
A) Logic Bomb 6. Which of the following m	B) Trap doors alicious program do not	C) Virus replicate automatically?	D) Trojan Horse
A) Trojan Horse 7 programs can be accomplish directly.	B) Virus e used to accomplish fun	C) Worm actions indirectly that an unauth	D) Zombie orized user could not
A) Zombie 8. Ais a program th the virus program, which ca		C) Worm grams by modifying them, the morograms.	D) Logic Bomb odification includes a copy of
•	B) Zombie pes NOT use a 'Cryptogra	C) Virus aphically Technique' to protect o	D) Trap doors data?
A) the use of digital signatures	B) data encryption	C) the use of stored encrypted password file:	D) using asymmetric keys at 'sender' and 'receiver' nodes
10. Which of the following o	rimes is done using a co	omputer as the instrument ?	
A) Computer Manipulation	B) Money Laundering	C) Data Alteration	D) Theft of services
		d on a computer system which	usually are located between O
and keyboard hardware to r		C/ C - C: '' '	D) A = - '
A) Keystroke12. They used readymade so	B) PC key logger oftware or application to	C) Software Key Logger b hack a computer.	D) Anonymizer
A) Hacker 13. In which year Information	B) Cracker on Technology Act was in	C) Script kiddies mplemented in India.	D) Phreakers

A)2013 14mail is also kno	B)2000 own as junk mail	C)2015	D)2003
A)Spoof 15 is a science of	B)Spam changing information into un	C)Fake intelligible form.	D)Fraud
A) Cryptography 16 is a fraud in	B) Steganography ivolving another person's iden		D) None of them
	B) Internet Time Theft ering raw data just before it is	The state of the s	D) Salami
A) Data Diddling 18. Which of the following is		C) Salami Attack	D) None of them
A) Greed 19. Which of the following t	B) Revenge erms best describes data that	• •	D) All of them
A) Text 20. First Cybercrime was rec	B) Cipher Text corded in	C) Plain text	D) Cryptography
A) 1820 21. 'Cyber' is a prefix derive	B) 1880 ed from:	C) 1940	D) 2004
	B) cybercell on compute	C) cybermatic er in 1982.	D) cybernetic
A) Apple 23. Any information being s	B) Microsoft ubject to human action or not	, 0	D) IBM computer.
A) Digital Evidence 24Uses Compu	B) Analog Evidence uter Forensics.	C) Physical Evidence	D) Logical Evidence
A) Corporations 25.Which of the following is	B) Insurance Companies the reason for Computer Fore	C) Criminal Prosecutors ensic:	D) All of them
A) Forgery 26. Computer/Cyber Crime	B) Virus is a Technique.	C) Fraud	D) All of them
A) Social 27. Recovering Deleted, En	B) Corporate acrypted and Damaged data is	C) Socio-Technical known as:	D) General
A) Cyber Security 28. Hashing algorithm pro	B) Computer Forensic tects which of the following ch	C) Physical Security paracteristic of the Cryptograp	D) None of them hic.
A) Availability 29. Transposition stream cip	B) Integrity oher uses which of the followir	C) Confidentiality ng technology:	D) Authenticity
A) Replace the character	B) Rearrange the letters	C) Substitute the character	D) None of them
30. Keyword searching ser	vice provided by:		
A) Computer Crime 31 .In Block Cipher plain cor	B) Cyber security nation of the control of the cont	C) Cyber criminals f the following block:	D) Computer forensics
A) 16 Bytes 32. Asymmetric Encryption	B) 26 Bytes a algorithm protects	C) 6 Bytes	D) All of them

A) Confidentiality	B) Integrity	C) Availability D) All of them				
33 is a kind of malware whose presence is typically hidden from the user.						
A) Spyware 34. When someone takes o	B) Logic Bomb ontrol of your website conside		D) Annonymizer			
A) Salami 35 mail is one that	B) Web Jacking t originate from one source bu	C) Spoofing ut actually has been sent from	D) Data Diddling another source.			
A) Spam	B) Fake	C) Spoof	D) Fraud			
36. Computer program that	lies dormant and triggered or	n a event on a particular day is	::			
A) Virus 37. CGA stand for	B) Worm	C) Logic Bomb	D) Trojan Horse			
granteed Access	B) Cryptographically generated address describes crime that is not rep	C) Cryptographically granteed Address corted to the police and that re	D) None of them emains unknown to			
A) Dark figure of crime	B) Light figure of crime	C) Cyber stalking	D) Crime typology			
39. Which of the following operating across national b		dertaken and supported by or	ganized criminal groups			
A) Malware	B) Transnational organized crime	C) Computer crime	D) Corporate crime			
40. Which of the following	describes malicious computer	programs such as viruses, wo	rms, and Trojan horses?			
A) Arson	B) Software Piracy	C) Malware	D) Larceny			
	unsolicited commercial bulk of a commercial product or so	email whose primary purpose ervice?	is the commercial			
A) Cyber terrorism	B) Terrorism	C) Spam	D) Malware			
42 is to protect dat	ta and passwords.					
A) Encryption	B) Authentication	C) Authorization	D) Non-repudiation			
43. SSID stands for	_					
A) Service Set ID	B) Service Set Identifier	C) System Service Identifier	D) None of the above			
44. The idea behind this atta first sight.	ck is to deduct a small amoun	t of money which would go co	empletely unnoticed in a			
A) Salami	B) Data Diddling	C) Web Jacking	D) Spoofing			
45. WEP stands for A) Wireless Equivalent	B) Wired Equivalent	C) Wireless Equivalent	D) None of them			
Privacy	Protocol	Protocol	D ₁ None of them			
•		s from one location to anothe	r using a public network			
A) Physical Public Network	B) Virtual Public Network	C) Physical Private Network	D) Virtual Private Network			

_	is/are methods of providin ical coding?	g secure communication b	etween two entities through the
A) Private key encryption	B) Public key encryption	C) Digital Signature encryption	D) All of the above
48. Which term best describ	es the type of attack that n		outers are communicating with
		ceiving data with a compute	_
· · · =	B) Man in Middle	C) Middle Man	D)None of them
49. A software defect is con			
A) Risk	•	C) Vulnerability	•
50. In this technique attacker signal strength.	er often launches an attack	on wireless network by crea	ating a new network with strong
A) Sniffing	B) Man in the Middle	C) DoS	D) Spoofing
51. What has become moreA) Natural Disasters52. What can a firewall prot	B) Data integrity and data security	increased use of computers C) Hardware Malfunction	s, the internet and WWW. ons D) Malicious deletions
32. What can a mewan prot	ect against:		
A) Viruses	B) fire		o) unauthenticated interactive ogins from the "outside" world
53. Which of the following n	nethods can effectively be	used to prevent logical brea	ich of security?
A) Operating system and other system software		C) Network design	D) computer architectural design
54 is the crim	_	engineering over telephon	_
			·
A) Smishing	B) Vishing	C) Phishing	D) Mishing
55 is an art of	detecting messages that are	e hidden in images, audio/v	rideo files.
A) Steganography	B) Cryptanalysis	C) Cryptography	D) Steganalysis
56. An attempt to make a co		ole to its intended users is c	alled
A) Botnet process	B) DoS attack	•	•
57 is the crim			vice
A) Smishing	B) Vishing	C) Mishing	D) Phishing
		Media Access Control addr	ess of a network Interface card
to a different one			
A) MAC Filtering	B) MAC Spoofing	C) IP Filtering	D) IP Spoofing
59. The attacker usually inst			activities such as:
A) Collecting MAC address	B) Detection of SSID	C) Collecting frame to crack WEP	D) All of them
60. This must be used to pro	tect from a SQL injection a	ttack	
A) Modify error report	B) Input Validation	C) Isolate servers	D) All of them
61. In this attack a query is s	ent to the database to che	ck if a user has valid name a	and password.
Brute Force attack	B) SQL injection attack	C) Password Guessing	D) Dictionary attack
62. In this technique hundre	eds or thousands of zombie	computers are used to floo	d a device with requests.
A) Buffer Overflow	B) DdoS	C) Man in Middle	D) DoS
63. This type of attack involved	es inquiring the network to	o discover host(s) to confirm	n information
A) Active reconnaissance	B) Active attack	C) Rattling the doorkno	bbs D) All of them
64. Purpose of a proxy serve	er is		
A) Keep System behind	B) Speed up access to a	C) Both A and B	D) None of them
curtain	resource		
	es all possible permutation	n-combinations of letters, n	umbers and special characters to
crack the password.	D) Distinguish 1	C) 11/4 - 1-1	D) Daiolann tall 1
A) Brute force attack66. The program files as wel	B) Dictionary attack I as boot sector is infected	C) Hybrid attack with activation of this type	D) Rainbow table attack of virus attack.

A) Program virus	B) Multipartite virus	C) Boot sector virus	D) Stealth virus
67. Which of the following a	ccurately reflects the purpose	of stegnography?	
A) Steganography	B) Steganography hides	C) Steganography exposes	D) Steganography
scrambles a message so	the existence of the data.	hidden data	encrypts cleartext data
that it cannot be viewed			
68 scannin	g is to understand the existing	weakness in the system.	
A) Port	B) Vulnerability	C) Network	D) System
69. Program that is designed	d to take advantage of vulnera	bility in an application or an o	perating system to enter an
application is known as			
A) Zombie	B) Worm	C) Trojan Horse	D) Virus
70. In this technique attacke	er insert a new node between	two existing nodes.	
A) Spoofing	B) Sniffing	C) Man in the Middle	D) DoS
71. Which of the following a	ttack is likely to result in Ident	tity theft?	
	B) Denial of Service attack		D) Virus infection
72. Virus is a computer		,	•
A) File	B) Database	C) Program	D) Network
	a security flaw or other proble	· -	•
A) Repair	B) Patch	C) Exploit	D) Hot Fix
	cookies could not be retained		,
	B) Session cookies	C) Stored cookies	D) None of them
·	performing one activity but a		•
advertised and malicious ac	-	outum, domestioned elect	or perrorming sour and
A) Virus	B) Zombie	C) Trojan Horse	D) Worm
76. Public Key Cryptography	·	o,o,a	2,
A) Symmetric Key		C) Asymetric key	D) None of the above
Cryptography	Cryptography	Cryptography	b) None of the above
77. Threats are categorized		ci yptograpiiy	
A) Passive or active	- \	C) Masquerade	D) Others
	to measure and analyze human	· ·	•
A) Footprinting	B) JBOD	C) Biometric	D) Anthropomorphism
	this command is used to retri		
A) Get	B) Post	C) Select	D) Rerieve
	etween Data Integrity and Dat	·	D) Nerieve
A) Limiting physical access	B) Encryption; Audit trails	C) Consistent, accurate	D) Distributing work to
to computer systems;	b) Encryption, Addit trails	and reliable data;	preserve integrity;
assigning passwords to		protection of data from	installing system
users.		unauthorized access.	passwords
81. In this phishing attack Ph	nishers identify the victim in a	dvance:	
A) Dragnet	B) Lobsterpot	C) Rod and reel	D) Gilnet
82. How are viruses spread?	1		
A) Through Firewalls	B) Downloading infected	C) Garbled information	D) Install anti-virus
	programs and files from		
	internet.		
83. If someone steal the sou	irce code of a game and sold it	t, is considered as violation of	
A) Patent	B) Tradesecret	C) Trademark	D) Copyright
84. Main purpose of a sniffe	r in a wireless network is to		
A) Detect SSID	B) Collect MAC	C) Collect frame to crack WEP	D) All of them
85. Gaining unauthorized ac	cess to a computer system wo		of computer crime?
A) Hacking	B) Destruction of data &	C) Theft of Services	D) Data Theft
=			

Software

96 technique involve	es copying information of a de	hit/ credit card to create a du	nlicate card
	· · · =		
A) Traiangulation	B) Traditional	C) Modren	D) None of them
87. Wireless network can be	·	C/ D: 11: CCID	D) All (1)
	B) Disbaling Mac filtering	=	D) All of them
	ocking the access of a specific		
A) IP Blocking	B) IP Clocking	C) Industry Espionage	•
89 can be used as I	P address Multiplexer to enab		omputers on the internet
A) FTP Server	B) Proxy Server	C) Web Server	D) None of these
90. Which among given is a	Bluetooth hacking tool:		
A) Bluejacking	B) Car-Whispering	C) Bluebugging	D) All of them
91. What is the maximum h	eader size of an IP packet?		
A) 32 Bytes	B) 30 Bytes	C) 64 Bytes	D) 62 Bytes
92 attack is	a computer threat which atte	mpts to exploit computer app	olication vulnerability that is
unknown to anybody in the	world.		
A) Data Diddling	B) Vulnerability	C) Zero day	D) None of the above
93. Dumpster diving is an ex	kample of		
A) Phishing	B) Fraud	C) Social Engineering	D) Cyber Stalking
94. A software update to fix	a security flaw or other prob	lem is known as	
A) Repair	B) Hot Fix	C) Patch	D) Exploit
95. Counterfeit websites are	e used by to extrac	ct personal information.	
A) Foistware	B) Phreakers	C) Heedless guests	D) Stalkers
96. is used by att	ackers to find the open port ir	· =	,
A) Vulnerability Scanner			D) All of them
	ole mails from zombie comput	ers are known as	,
A) Spoofer	B) Spies Kiddies	C) Spammer	D) Stalker
98. Which among these is u	sed to track missing laptop(s).		
A) Motion Sensor	B) Labels	C) Alarms	D) All of them
99. In the realm of 'cyber at	·	•	,
•	B) Damaging Downtime of	C) Digital Data Output	D) None of them
of System	System	Spoit	,
•	er uses public cloud resources	•	nown as:
	B) Global cloud		

[Total No. of Pages:04]



Roll No:

End Term Exam

Semester-VIII

Date: Department:	Time: 180 minutes
Title of the Course: Cyber Security	Max. Marks: 100
Course Code: HUL 2401	
Q1 Sam send a message Tim and Joe using same	Q13 A destructive employee of a company installed a script in the
encryption key, at the receiving side Tim and Joe decrypt	server to take revenge from his employer and this is going to be
the message with the key used by Sam to encrypt the	executed after one week of the installation date is an example of:
message is an example of .	(a) Worm (b) Logic Bomb
(a) Symmetric encryption (b) Hashing	(c) Virus (d) Trojan Horse
(c) Asymmetric encryption (d) None of the above	Q14 "Do no evil" is the motto of
Q2 is a person who is ethically opposed to the	(a) Microsoft (b Google
abuse of computer systems.	(c) Yahoo (d) Intel
(a) White hat hacker (b) Red hat hacker	Q15 Which term best describes the type of attack that makes it
(c) Green hat hacker (d) Black hat hacker	possible to deny the service of a server using multiple computers
Q3 Which among these is a feature of Hashing	from different geographical locations?
(a) Confidentiality (b) Availibility	(a) Buffer Over flow (b) DoS
(c) Authenticity (d) None of these	(c) Man in Middle (d) None of these
Q4 the first phase to commit a crime and is treated	Q16 Which term best describes the type of attack that makes it
as passive attack	seem like two computers are communicating with each other,
(a) Scanning (b) Scrutinizing	when actually they are sending and receiving data with a
(c) Reconnaissance (d) None of them	computer between them?
Q5 Which statement about virus attack is true	
A. Boot sector virus infects the storage media	(a) Spoofing (b) Middle Man
B. Program virus is a hybrid virus	(c) Bucket Brigade (d) Replay
C. Stealth virus mask itself so detection is not easy	Q17 A is a program that secretly takes over
D. Multipartite virus target .exe files	another Internet-attached computer and then uses that
(a) Both A and B (b) Both A and C	computer to launch attacks.
(c) Both A and D (d) None of them	(a) Worm (b) Zombie
Q6 In the right setting a thief will steal your information by	(c) Virus (d) Trap doors
sampling watching what you type.	Q18 This type of attack involves gathering information about
(a) Snagging (b) Spying	individual about his her knowledge, for example which the IN and
(c) Social Engineering (d) Shoulder surfing	OUT time of an employee.
Q7 is the criminal practice of using social	(a) Passive attack (b) Active attack
engineering over telephone.	(c) Forgery attack (d) None of these
(a) Phishing (b) Mishing	Q19 Difference between Data Integrity and Data Security is
(c) Vishing (d) Smishing	Q15 Bireferice Section Butto integrity and Butto Security is
Q8 attack is a computer threat which attempts to	(a) Limiting physical access to computer systems; assigning
exploit computer application vulnerability that are unknown to	passwords to users.
anybody in the world.	(b) Consistent, accurate and reliable data; protection of data
(a) Zerod day (b) Vulnerability	from unauthorized access.
(c) Data Diddling (d) Salami	(c) Encryption; Audit trails
Q9 Which among given is a Bluetooth hacking tool?	(d) Distributing work to preserve integrity; installing system
(a) Bluejacking (b) Blue bugging	passwords
(c) Car Whispering (d) All of them	Q20 In a computer security, means that computer
Q10 In asymmetric cryptographic algorithm when Tom wants to	system assets can be modified only by authorized parties
send a message to Alisha he will decrypt it with	(a) Confidentiality (b) Integrity
(a) His Public Key (b) Public key of Alisha	(c) Availability (d) Authenticity
(c) His Private Key (d) Private key of Alisha	Q21 It is a type of program do not replicate automatically?
Q11 Another name of Public Key Cryptography	(a) Worm (b) Zombie
(a)Symmetric Key Cryptography	(c) Trojan Horse (d) Logic Bomb
(b) Private key Cryptography	Q22 Which of the following is independent malicious program
(c) Asymetric key Cryptography	that need not any host program?
(d) None of the above	(a) Trap doors (b) Trojan Horse
Q12 are software programs installed on a computer	(c) Virus (d) Worm
system which usually are located between OS and keyboard	Q23 also known as a "trading name that a business
hardware to record every key stroke	trader use under commercial purposes.
(a) Key Stroker (b) Key Logger	(a) Trade Secret (b) Trade Name
(c) Software Key logger (d) Annonymizers	(c) Patent (d) Copy Right

Q24 Doodle me Diddle fraud held in	1996 in India was a	Q38 is a generic term which	ch refers to all the legal and
type of cyber crime		regulate aspects of Internet and th	ne World Wide Web
(a) Salami (b) Credi		(a) Cyber Law	(b) Cyber Dyne
(c) Data Diddling (d) None		(c) Cyber Cafe	(d) Electronic Law
Q25 The purpose of a DoS attack is/are		Q39 What is the difference bet	ween Data Integrity and Data
(a) Flood a network with tr	affic, thereby preventing	Security?	
legitimate network traffic (b) Disrupt connection between to	NO systems		to computer systems; assigning
(c) Prevent a particular individual		passwords to users	unlinkle data, muntantiam of data
(d) All of them	to access the service(s).		reliable data; protection of data
Q26 Which of the following is issued or	nline for use over the	from unauthorized access.	
Internet and is stored in an electronic of		(c) Encryption; Audit trails	rve integrity; installing system
computer memory?		passwords	ive integrity, mistaining system
•	(b) Business Card	Q40 Attacker uses this server to o	connect with a network which is
	(d) E-Card	block through the firewall of the o	
Q27 Gaining unauthorized access to a	computer system would fall	_	TP Server
under which category of computer crin	ne?		lone of these
(a) Hacking		Q41 We can categorize threats as:	
(b) Theft of Service		(a) Passive attack (b) A	ctive attack
(c) Destruction of data & Software	2	(c) Both a and b (d) N	lone of them
(d) Data Theft		Q42 Symbol of a reputed firm is	S
Q28 One day while working on your s		(a) Patent (b) (
from an organization asking that		(c) Trademark (d) A	
information within 12 hours, or your best thing to do is	account win be closed, the	Q43 are the symbols us	ed by busineses to identify their
(a) Reply to the email asking them	why this information is	goods and services.	
required.	willy this information is	(a) Trade Mark	(b) Trade Secret
(b) Reply to the email with the infe	ormation asked for	(c) Designs	(d) None of them
(c) report the email to the actual of		Q44 is a preparation tov	
delete the email.	0	(a) Passive attack (c) Reconnaissance	(b) Active attack(d) None of them
(d) None of these		Q45 Whenever, by words either sp	` <i>'</i>
Q29 A is a document tha	t grant the holder exclusive	by signs or by visible representation	
right on an invention for fixed number	of years.	imputaion concerning any person	
		or having reason to believe that su	
(a) Copy Right	(b) Patent	reputation of such person is said:	,,
(c) Trade Mark	(d) Trade Secret		(b) Phishing
		(a)Cyber Stalking (c) Social Engineering	(d) Cyberdefamation
Q30 Which of these companies is not a	leader in Cloud	Q46 cipher replaces of	
Computing?	(1-) A	another character to create	
(a) Google	(b) Amazon (d) Blackboard		•
(c) Microsoft Q31is the simple process of inte		(a) Substitution	(b) Transposition
is broadcasted on unsecured network.	reepting wheless data that	(c) either (a) or (b)	(d) neither (a) or (b)
(a) Spoofing (b) Sniffi	ng	Q47 Information Technology Act I	
(c) Spamming (d) None	_	year in India	
Q32 Which of the following is a cyber of		(a) 2000	(b) 2004
(a) Hacking (b) Worm		(c) 2008	(d) 2012
(c) Virus Attack (d) None		Q48 A cookie that was not created	` '
Q33 This attack involves altering raw d		to access it is called a	·
processing and then changing it back a	fter the processing is	(a) First-party cookie	(b) Second-party cookie
completed:		(c) Third-party cookie	(d) Fourth-party cookie
(a) Data Tampering (b) Data I	Diddling		
(c) Salami Attack (d) None		Q49 A hacker who claims to be mo	otivated by improving security
Q34 is a type of virus which	n effect/ infects the storage	by uncovering vulnerabilities is cal	led.
media on which OS is stored.		(a) Black hat attacker	(b)White hat attacker
(a)Boot Sector Virus (b) Progra		(c)Cowboy attacker	• •
(c) Multipartite Virus (d) Stealt		Q50 This mechanism is used to	protect private networks
Q35 Network administrator must	do to protect a	from outside attack is	
wireless network.	(1) 5: 11: 20:5	(a) Firewall	(b) Antivirus
	(b) Disabling SSID	(c) Digital signature	(d) Formatting
	(d) All of them	Q51 can be used as II	
Q36 It is a technique breaking into pho	one or other communication	to connect to number of com	
systems. (a) Hacking (b) Cracki	ing		TP Server
(c) Phreaking (d) War d	_		lone of these
Q37 is a tool installed on you	_	Q52 Which term best describes the	
presence of a key logger	IIIpara. to detect the	uses a large pregenerated date every possible password?	ia set of hasiles from hearty
(a) Keylogger	(b) Anti Keylogger	(a) Brute Force Attack	(b) Dictionary Attack
(c) Software Keylogger	(d) Hardware Keylogger	(c) Rainbow Table Attack	(d) Host File Attack

Q53	Hackers often gain entry to a net	work by pretending to be at		(c) A login name and password	(d) A fake identity	
a legitimate computer shows an example of		Q69 Poorly designed social networking sites are especially				
	(a) Spoofing	(b) Forging		vulnerable to	(Is) COL intention attack	
OF 4	(c) IP Spoofing	(d) ID Theft		(a) Buffer overflow attack	(b) SQL injection attack	
	Multiple ping packets are sen			(c) Non- Persistent cross-site scripting(d) Persistent cross-site scripting	_	
	which results into more traffic		070	A SQL injection attack may be use		
	handle, in this type of denial of		۵, ۵	(a) Change number of coloumns		
	(a) Flood attack (c) SYN attack	(b) Ping of death attack (d) Smurf attack		(b) Read a row in a table		
055	It is a way of generating significar	• •		(c) Change coloumn name in a ta	ble	
455	on a victim network.	it compares necessors traine		(d) None of them		
	(a) Flood attack	(b) Ping of death attack	Q71	. The most effective remedy for SC	-	
	(c) Teardrop attack	(d) Smurf attack		(a) To filter HTML form input at t		
Q56	When the control of a web sit	e is taken by an attacker		(b) To employ stored procedures		
	is considered as			(c) To employ prepared SQL state		
	(a) Data Diddling	(b) Salami	ovni	(d) To perform input validation o ression	ii the server via regular	
	(c) Web theft	(d) Web Jacking		! Tasks performed by firewall inclu	de	
	This is installed between coputer	and Keyboard to generate	Q, 2		et Integrity Checking	
	the log of keys pressed by user.			(c) IP address spoofing (d) All		
	(a) PC Key logger	(b) Software key logger	Q73	The role of a payment gateway is		
	(c) Hardware key logger	(d) None of them		(a) A proxy to the merchant		
Q58	This process involves changing co			(b) A proxy to the bankcard netw	rork	
	depending upon a user's IP addre			(c) A financial service provider		
	(a) IP Base Clocking (c) Industry Espionage	(b) IP Base Blocking (d) None of them		(d) A government regulator		
O59	Which among given is/are challer	• •	Q74	The motivation of an ethical hack	er is	
QJJ	(a) Employee wasted time or			(a) Financial gain		
	(b) Controlling Access to Wel			(b) The thrill of hacking		
		Application		(c) To desire to identify vulnerabi	ilities so they can be patched	
	(c) Bandwidth Wastage		beto	ore they are publicaly exposed		
	(d) All of them		075	(d) A religious/political/ideologic		
	This techniques is used on a wire	ess network to scan the		Q75 Which of the follwoing is/are necessary feature(s) of a DDoS attack		
	ork passively.	(h) Species	atta			
	(a) Scanning	(b) Spoofing (d) All of them		(a) Use of a TCP SYN packets		
	(c) Sniffing This in built feature of web brows			(b) Use of a spoofed IP address(c) Use of multiple attackers geor	raranhically dispressed	
QUI	malicious sites by:	sers to warm about		(d) Use of malformed IP packets	grapmeany dispressed	
	(a) Anti-phishing filters in IE	and Firefox	076	An attack originating and/or atte	mpted within the security	
	(b) Web of Trust	and therex		meter of an organization is		
	(c) Clearing history of brows	ar.		(a) Active	(b) Inside	
	(d) Addlock Plus			(c) Passive	(d) Outside	
063		omputing allows	Q77	The attacker usually installs the s	niffers on the wireless	
	is a social media c	, -	netv	work and conduct activity such as:		
peo	ple to connect and share in			(a) Detection of SSID	(b) Collecting MAC address	
	(a) Facebook	(b) My Space		(c) Collecting fram to creack WEF		
	(c) Linkedin	(d) Twitter	Q78	A Digital certificate is used to bin		
Q63	is not a cloud sphere			(a) A person's public key to his pr	-	
	(a) Joint Sphere (c) Recipient Sphere	(b) User Sphere (d) Client Sphere		(b) A person's public key to his id		
	Secret key cryptography is synoyr	• •		(c) A person's private key to his id(d) A person's signature to his pri		
	(a) Symmetric Key Cryptography	nous with	070	Which of the following attacks is,		
	(b) Asymmetric key cryptography		Q/9	identity theft?	rare likely to result in	
	(c) Private key cryptography			(a) Phishing attack	(b) Denial of Service attack	
	(d) Quantum Cryptography			(c) Virus Infection	(d) All	
	To encypt a message from Aman	to Alka using public key	080	In which of the following does so		
	cryptography, the following is ne		400	capture and manipulate packets		
		(b) Aman's public key		your network?	, , , , , , , , , , , , , , , , , , ,	
	(c) Alka's private key	(d) Alka's public key		(a) DoS	(b) Backdoor	
Q66	Which of the following protocols	is used in accessing web		(c) Man in Middle	(d) Spoofing	
	mail?		Q81	is a "technique to in	- · · · · · -	
	(a) SMTP	(b) HTTP		the information or perform some		
	(c) POP3	(d) IMAP		(a) Social Engineering	(b) Phishing	
	The phrase describe			(c) Cyber stalking	(d) None	
	horse attack applets, and attack s	·	Q82	! Intellectual Property Rights (IPR)		
	(a) Malware	(b) Spam		information and ideas that are of		
	(c) Phishing	(d) Virus		(a) Ethical value	(b) Moral Value	
	A counter- measure to eavesdro	oping on the communication		(c) Social value	(d) Commercial value	
	s the use of (a) A cryptography checksum	(b) Encryption	Q83	A hacker that changes or forges in		
	(a) A ciyptograpily checksulli	(b) LIICI YPUUII		resource, is engaging in	•	

(a) Sniffing	(b) Denial of Service
(c) Terrorism	(d) Data Diddling
Q84 It involves harassing or three	atening behavior that an
individual will conduct repeate	dly for following a person,
visiting a person's home and/or I	ousiness place
(a) Phishing	(b) Social Engineering
(c) Cyber Stalking	(d) None
Q85 Security risks from social enginee	• •
(a) Malware distribution	_
• •	(b) Cyber bullying
(c) Privacy concern	(d) All
Q86 Threats are categorized as:	
(a) Passive or active	(b) Traffic
(c) Masquerade	(d) Others
Q87 How are viruses spread?	
(a) Through Firewalls (b) Dow	nloading infected programs
and files from internet.	9
(c) Garbled information. (d) Insta	Il anti-virus
O88 DDoS stand for	in anti viras.
	- A A 1.
(a) Distributed Denial of Service a	аттаск
(b) Digital Data Output Spoit	
(c) Damaging Downtime of Syste	
(d) Distributed Destruction of Sys	stem
Q89 is not a kind of cyber a	ttack.
(a) Cber Stalking	(b) Micro sites
(c) Firewall attack	(d) E-Mail
Q90 The latest WLAN standard is:	(a) E ivian
•	(h) 002 11 -
(a) 802.11g	(b) 802.11n
(c) 802.12g	(d) 802.12n
Q91 The following is used when the so	ource code for a piece of
software is unavailable	
(a) Blackbox testing	(b) Whitebox testing
(c) Regrssion testing	(d) Unit testing
Q92 Which of the following is/are true	` '
malware:	0 01 1411040 1011110 01
	file or program
(a) A worm attaches itself to a	
(b) A Trojan is stand-alone prog	
(c) A virus does not necessarily	replicate
(d) All of the above	
Q93 cryptography technique i	s used for ATM cards
(a) Symmetric	(b)Assymetric
(c) Hashing	(d) None
Q94 cipher takes one character	
another.	and replaces it min
	(h) Cinglo
(a) Stream	(b) Single
(c) Substitution	(d) Hash
Q95 The purpose of digital signatue is	
(a) Verify Sender (b)Prove	e Integrity of message
(c) Prevent sender from disowing	g the message
(d) All	
Q96 is the science of tran	nsforming information into a
secure form so that unauthorized use	rs cannot access it.
(a) Steganography	(b) Cryptography
(c) Neither a nor b	(d) Both a and b
Q97 A victim unknowingly downloads	a Trojan norse virus is a
type of crime.	
(a) Type 1 Cyber crime	(b) Type 2 Cyber crime
(c) Type 3 Cyber crime	(d) Type 4 Cyber crime
Q98 Survival mantra for netizens is an	e:
(a) Keep genuine software	
(b) keep browsers updated with	n security patches
(c) Keep an effective Antivirus	
(d) All of them	
Q99 is a technique of cha	anging an assigned Modia
Access Control address of a network I	interrace card to a different
one () IR 6	(1) 15 511
(a) IP Spoofing	(b) IP Filtering

(c) MAC Spoofing

(d) MAC Filtering

Q100 Which among following(s) can be patented.

(b) Machine

(a) Process (c) Composition of matter

(d) All of the above

Rol	l No				Tota	l No. of Pages: 04
		END TERM E	XAMINA	ATION		
		FIFTH SEMESTER	DECEM	BER 2015		
		CAL3313 – CY	BER SEC	CURITY		
Tim	e allowed: 3 Hrs.				Max	. Marks: 100
Gen	eral Instructions :					
1. A	ll questions are compulsory					
	ach question carry one mark					
3. 1	here is no negative marking					
Q1	are used in denial of	of service attacks typically		(c) Distribut	ed systems design	
	nst targeted websites.	of service attacks, typically		(d) Network		
идин	(a) Worm	(b) Zombie	014	` '	firewall protect agair	nst?
	(c) Virus	(d) Trojan Horse	-,- :	(a) viruses		
Q2	is a form of virus expli			. ,	nticated interactive I	ogins from the "outside"
	from detection by antivirus.			world		_
	(a) Stealth Virus	(b) Polmorphic Virus		(c) fire	(d) connecting to	and from the "outside"
	(c) Parasitic Virus	(d) Macro Virus			world	
Q3	A is a program that s		Q15			ity of a computer system or
	Internet-attached computer and	then uses the computer to			•	erruption ii) Interception iii)
	launch attacks.				n iv) creation v) abric	ation
	(a) Worm	(b)Zombie		(a) i, ii, iii an		
	(c)Virus	(d) Trap doors		(b) ii, iii, iv a	•	
Q4	In computer security, m			(c) i, ii, iii an	•	
	assets can be modified by the aut	-		(d)All of the		
	(a) Confidentiality	(b) Integrity	Q16		·	nt because of the incre
0.5	(c) Availability	(d) Authenticity			computers, the inter	
Q5	Which of the following malicious	program does not replicate		(a) Natural [(b)Hardware Malfunctions
	automatically?	4122	047			ity (d)Malicious deletions
	(a) Trojan	(b) Virus	Q1/			someone who gains illegal
06	(c) Worm	(d) none of these			computer system?	(b) 1-1
Qб	A is a program that ca			(a) Hacker		(b) Identity theft
	modifying them, the modification		010	(c) Intruder		(d) Cyber-terrorist
	program, which can go on to infe		Q18		_	thical issues facing the use of
	(a) Worm	(b) Virus			in business today?	(b) Software piracy
07	(c) Zombie IPSec is designed to provide the s	(d)Trap doors		(a) E-mail Pr	ual property	(d) All of the above
Q/	(a) Transport layer	(b) Network Layer	∩10			send secure messages from
	(c) Application Layer	(d) Session Layer	QIJ		_	oublic network such as the
Ω 8	An attempt to make a computer			Internet?	i to another using a p	Subile Hetwork Such as the
QU	intended users is called	resource dilavallable to its			Public Network	(b) Virtual Public Network
	(a) DoS attack	(b) Virus attack			Private Network	(d) Virtual Private Network
	(c) Botnet process	(d) worms attack	020			methods of providing secure
Q9	Pretty good privacy (PGP) is used	` '	~		_	entities through the use of
	(a) Browser Security	(b) Email Security		mathematic		and an angle and and a
	(c) FTP Security	(d) None of these			ignature encryption	(b) Public key encryption
Q10	When a DNS server accepts and u	• •			ey encryption	(d) All of the above
•	from a host that has no authority		Q21		maximum header siz	` '
	then it is called	,		(a) 32 bytes		(b) 64 bytes
	(a)DNS Lookup	(b) DNS Hijacking		(c) 30 bytes		(d) 62 bytes
	(c) DNS Spoofing	(d) None of these	Q22	Which of the	e following is/are Pro	otocols of Application?
Q11	WPA2 is used for security in			(a) FTP		(b) DNS
	(a) ethernet	(b) Bluetooth		(c) Telnet		(d) All of the above
	(c) wifi	(d) None of these	Q23	I want to red	quest secure web pag	ges using https://. What port
Q12	What characteristic make Interne	et so attractive?		will I need t	o open on my firewa	ll to allow these SSL-
	(a) the 'secure' surroundings with	-			ackets to flow?	
	(b) the ability to provide an open,			(a) 161		(b) 53
	(c) it eliminates the need for firev			(c) 6000		(d) 443
	(d) You don't require a fast comp		Q24		lia was amended in	***
Q13	Which of the following methods of	can effectively be used to		(a) 2000		(b) 2004

(c) 2008

(d) 2010

prevent logical breach of security?

(b) computer architectural design

(a) Operating system and other system software

Q25	Intellectual property rights and _	are two of		(a) Dos	(b) DDoS
	the most important developing a	reas of law.		(c) Man in the middle	(d) Buffer Overflow
	(a) Cyber Law	(b) copyright infringment	Q42	2 This must be used to protect f	rom a SQL injection attack
	(c) patent law	(d) trademark infrignment		(a) Input validation	(b) Modify error report
	Commercial use domain names w			(c) Isolate servers	• •
	following suffix in their website a	ddress.	Q43	3 not involves in securin	g a wireless network
	(a) .net	(b) .gov		(a) Disable remote login	
	(c) .com	(d) .org		(b)Disable WPA/WEP encryption	on
Q27	If Social engineering is used to cra	ack the password, it comes		(c) Disable SSID broadcast	
	under the category of			(d)Enable MaC address filterin	_
	(a) Online Attack	(b) Offline attack	Q44	4 is a kind of malwar	e whose presence is typically
	(c) Non-electronic SQL injection attack involves	(d) None of these		hidden from the user.	
Q28	SQL injection attack involves	command to retrieve		(a) Spyware	(b)Logic Bumb
	information from a web page/we			(c) Key Logger	(d) Annonymizer
	(a) GET	(b) POST	Q45	5 Which among these is not a th	
	(c) SELECT	(d) DELETE			(b) Stalking
	In this type of password cr			(c) Privacy Concern	• •
	substitutes numbers and symbols	=	Q46	6 is an art of detect	ing messages that are hidden
		(b) Hybrid attack		in images, audio/video files.	
	(c) Bruce force attack	(d) Rainbow attack		(a) Steganalysis	(b) Steganography
	The latest standard of WLAN is			(c) Cryptography	(, , , , , , , , , , , , , , , , , , ,
	(a) 802.11g	(b) 802.11n	Q47	7 This process involves chan	
	(c) 802.12g	(d) 802.12n			IP address and geographica
	In this technique attacker often la			location.	
	wireless network by creating a ne	ew network with strong		(a) IP base blocking	(b)IP base clocking
	signal strength.				(d)None of these
	(a) Sniffing	(b) Spoofing	Q48	8 A mail is one	
	(c) Man in the middle	(d) Dos		but actually has been sent from	
Q32	SSID stand for			(a) Spam	(b) Spoof
	(a) System Service Identifier	(b) Service Set ID		(c) Fake	(d) Fraud
	(c) Service Set Identifier	(d) None of the above	Q49	9 An accountant of a company c	
Q33	WEP stand for			computation of the salary of the	
	(a) Wireless Equivalent Protocol				he data to its original form, this
	(b) Wired Equivalent Protocol			shows the example of a	
	(c) Wireless Equivalent Privacy			(a) Salami attack	(b) Forgery attack
	(d) Wired Equivalent Privacy			(c) Social Engineering attack	
	cookies remains in the	e system until intentionally	Q50	O scanning is	to understand the existing
	removed by user			weakness in the system	
	(a) System	(b) Session		(a) Port	(b) Network
	(c) Persistent	(d) Transient		(c) Vulnerability	(d) System
Q35		tained after the browser is	Q52	1 When someone take control o	-
	closed			(a) Salami	(b) Data Didding
	(a)Persistent Cookies	(b) Stored Cookies		(c) Web Jacking	(d) Spoofing
	(c) Transient Cookies	(d) None of them	Q52	2 Which term best describes the	
Q36	This social media tool allows po	eople to connect and share		seem like two computers are o	_
	information.				sending and receiving data with
	(a) Facebook	(b)Linkedin		a computer between them?	
	(c) MySpace	(d) Twitter		(a) Spoofing	(b) Middle Man
Q37	Which among given is not a kind			(c) Man in the middle attack	(d) Replay
	(a) JointSphere	(b) UserSphere	Q53	3 Dumpster diving is an example	
	(c) ClinetSphere	(d) Recipient Sphere		(a) Social Engineering	(b) Phishing
Q38	Anti-phishing tools cannot detect			(c) Fraud	(d) Cyber Staking
	(a) Website Forgery	(b)Phone Phishing	Q54	4 Which among given is a Blueto	
000	(c) Mail Phishing	(d)Flash Phishing		(a)Bluejacking	(b) Bluebugging
Q39	The SSID of Wireless Access F	oint can be upto		(c) Car-whispering	(d) All of them
	characters.	(1)00	Q55	5 CGA stands for	
	(a) 16	(b)20		(a) Cryptographically generate	
O * *	(c) 24	(d)32		(b) Cryptographically granteed	
Q40	Purpose of a proxy server is	•		(c) Cryptographically granteed	Address
	(a) Keep System behing curtain		0-1	(d) None is correct	lle.
	(b) Speed up access to the resour	rce	Q56	6 Cousnterfeit websites are used	byto extract
	(c) Both A & B			personal information.	
044	(d) None of these	aanda af aciiilat		(a) Foistware	(b) Heedless guests
	In this technique hundreds or the			(c) Phreakers	(d) All of them
	computers are used to flood a de	vice with requests.			

Q57	is a tool which extract	the data from the phone of a		(c) Unicast	(d) None of the above
-,-	person even his/her mobile phor		074	Cryptographic hash function ta	
	(a) Bluejack	(b) Bluesnaffer		and returns	,
	(c) Bluediving	(d) Bluebugger		(a) fized size bit string	(b) variable size bit string
058	Hashing algorithm can pro			(c) bit string	(d) None of these
QJU	information.		075	Which one of the following is a	• •
	(a) Confidentiality	(b) Integrity	Q/3	to secure HTTP connection?	a cryptograpine protocor useu
		,			a protocol (CCTD)
	(c) Availability	(d) Authencity		(a) stream control transmission	
050	to orbital consult and inculation	Literaturality		(b) transport layer security (TS	
Q59	In which year IT act implemented			(c) explicit congestion notificat	
	(a)1998	(b) 2000		(d) resource reservation proto	
	(c) 2004	(d) 2008	Q76	What is the number one conce	
Q60	Asymmetric Encryption algorithm	n protects		(a) Too expensive	(b) Security concerns
	(a) Confidentiality	(b) Integrity		(c) Too many platforms	(d) Accessibility
	(c) Availability	(d) All of them	Q77	' Which is not a major cloud cor	nputing platform?
Q61	This type of virus when execute	d infects program files along		(a) Google 101	(b) IBM Deep blue
	with boot record.			(c) MS Azure	(d) Amazon EC 2
	(a) Boot Sector virus	(b) Program virus	Q78	"Cloud" in cloud computing, re	presents what?
	(c) Multipartite virus	(d) Stealth virus		(a) Wireless	(b) harddrives
062	The attacker usually installs the	• •		(c) People	(d) Internet
	network and conduct activities si		079	is the feature of cl	
		(b) Collecting MAC address	α, 3	service to change in size or vo	
	(c) collecting frame to crack WEP				duffie in order to ffieet a user s
063	-			needs.	(I=) \ (I; = + : = + : = : = : = : = : = : = : = :
Q63	A small hardware device or a p	_		(a) Scalability	(b) Virtualization
	keystroke a user types on the co	imputer's keyboard is known		(c) Security	(d) Cost-savings
	as:		Q80	The attackers a network of con	-
	(a)Proxy Server	(b) Anonymizer		(a) Internet	(b) Botnet
	(c) Key Logger	(d) Key Capture		(c) Telnet	(d) D-net
Q64	IPSec is designed to provide secu	rity at	Q81	The DoS attack is which the	e attacker establishes a large
	(a) Transport layer	(b)Network layer		number of half-open or fully	open TCP connections at the
	(c) Application layer	(d) Session layer		target host	
Q65	WPA2 is used for security in			(a) Vulnerability attack	(b) Bandwidth Flooding
	(a) ethernet	(b) bluetooth		(c) Connection Flooding	(d) All of the above
	(c) wi-fi	(d) None of these	Q82	Sniffers can be deployed in	
Q66	PGP encrypts data by using a blo	• •		(a) Wired environment	(b) Wi-fi
	(a) international data encryption	-		(c)Ethernet LAN	(d) All of the above
	(b) private data encryption algori	_	083	A botnet is	(4) / 0 0 450 10
	(c) intrenet data encryption algorithms (c)		QUU	(a) a computer virus that replic	cates and spreads itself from
	(d) none mentioned			computer to computer via e	
067	In wireless ad-hoc network			traffic.	e-man and other miternet
Q07		(h) a coope we just in way at			
	(a) access point is not required			(b) software that gives you adr	ninistrator rights to a
0.00	(c) nodes are not required	(d) access point is hidden		computer or network.	6.1
Q68	A piece of icon or image on a wel	o page associated with		(c) an exact copy or snapshot o	of the contents of an electronic
	another webpage is called			medium.	
	(a) url	(b) hyperlink		(d) a collection of computers the	
	(c) plugin	(d) None			automatically by themselves.
Q69	A web cookie is a small piece of o	data	Q84	Which of the following refers t	o the forging of the return
	(a) sent from a website and store	ed in user's web browser		address on an e-mail so that th	ne e-mail message appears to
	while a user is browsing a we	bsite		come from someone other tha	in the actual sender?
	(b) sent from user and stored in t	the server while a user is		(a) Spoofing	(b) Redacting
	browsing a website			(c) Spamming	(d) Pharming
	(c) sent from root server to all se	rvers	Q85	SQL injection is an attack in wh	
	(d) sent from client to server			into strings that are later passe	
070	Which of the following is not the	funtion of network layer?		(a)malicious	(b) reduntant
α, σ	(a) routing	(b) inter networking		(c) clean	(d) Non-reduntant
	(c) congestion control	(d) error checking	006	Point out the correct statemer	
071		(d) error checking	Qou		
Q/I	In cryptography, what is ciper?	nuntion and description		(a) Parameterized data cannot	be manipulated by a skilled
	(a) algorithm for performing enc	ryption and decryption		and determined attacker	COL etatamas et elle 111
	(b) encrypted message	/ N **		(b) Procedure that constructs S	
	(c) both a and b	(d) None of the above		reviewed for injection vuln	
Q72	The header length of IPv6 datagr			(c) The primary form of SQL inj	ection consists of indirect
	(a) 10 bytes	(b) 25 bytes		insertion of code	
	(c) 30 bytes	(d) 40 bytes		(d) None of the above is correct	ct
Q73	IPv6 does not use type of	f address			

(a) Broadcast

(b) Multicast

087	time based SQL injection attack.
(a) Quick detection	(b) Initial Explication
(c) Blind SQL inject	
	ed on a per-click model is called
_	engine advertising
(b) Feedback	(c) Source advertising
(d) Search Engine (
_	-date is most successful among
(a)American consu	
(c) Spanish consum	
	ng is IEEE fiber cable standard? (b) 100BASE-CX
(a)100BASE- FX (c) 10GBASE-LR	(d) 100BASE-EX
	ens when a buffer is overflowed?
	ce that comes after the buffer holds the
	I as keeping the data that it contained
before	i as keeping the data that it contained
	e memory space that comes after the
buffer is overw	
	in the computer gets too big and
explodes	of the many and the said at anti-office
	of the memory chip and start a fire.
Q92 A DNS Client is call	
(a)DNS Updator	(b) DNS resolver
(c) DNS handler Q93 Network layer fire	(d) None of the above
•	
(a) frame filter	(b) packet filter
(c) both a and b	(d) None of the above onally encompassed abuses and misuses
	or computers connected to the Internet,
	d concomitant losses.
(a)Digital crime	(b) Cyber crime
(c) Computer relat	crime (d) None of the above
Q95 Which of the follow	ng crimes is done using a computer as
the instrument?	
(a)Computer Mani	` ,
(c) Data alteration	(d) Theft of services
	ng techniques is most effective in
preventing compu (a)Backups	(b) Digital forensic analysis
(c) Using a farewal	(d) None of the above
Q97 What is a Hacktivis	• •
(a)Politically motiv	ed hacker
(b) Denial of service	attacker
(c)A proponent of	
	g in an intentional act involving a
·	ch the person may have gained at the
victim expense	runtanalusis saftuvara?
Q98 What is purpose of (a)Breaking encryp	
(b) Taking advanta	
	roying function in a computer
(d) Delievering atta	
Q99 Which of the follow	ng is not a similarity between real-world
stalking and cyber	
(a)Most victims are	
	ictim are near to each other
(d) Stalkers are ger the victim	rally motivated by the desire to control
	f kids have been bullied while online?
(a) 42%	(b) 11%
(c) 67%	(d) 2%

Roll No	Total No. of Pages: 07
---------	------------------------

END TERM EXAMINATION FIFTH SEMESTER 2015-16

CAL3313 – CYBER SECURITY Time: 03 Hrs. Max. Marks: 100 **General Instructions:** 1. All questions are compulsory 2. Each question carry one mark 3. There is no negative marking Anti-phishing tools cannot detect such kinds of phishing sites. 1) Website forgery (ii) Phone phishing (iii) Mail phishing (iv) Flash phishing In this type of attack attacker establishes a connection between a victim and the server to which victim is 2) connected to extract the information. Man in the middle attack Bucket-brigade attack (i) (ii) (iii) Janus attack (iv) All of them This type of attack involves all possible permutation-combinations of letters, numbers and special 3) characters to crack the password. (i) Dictionary attack (ii) Hybrid attack Brute force attack Rainbow table attack (iii) (iv) 4) All the program files as well as boot sector is infected with activation of this type of virus attack (i) Boot sector virus (ii) Multipartite virus (iii) Stealth virus (iv) Program virus Purpose of a proxy server is 5) Keep System behind curtain (ii) Speed up access to a resource (iii) Both A and B (iv) None of them This type of attack involves inquiring the network to discover host(s) to confirm information 6) Active attack (ii) Rattling the doorknobs (i) (iii) Active reconnaissance (iv) All of them 7) Hashing algorithm can protect the of information. Confidentiality (ii) Integrity (i) (iii) Availability (iv) Authenticity 8) This ensures that the information is correct and no unauthorized person or malicious software has altered that data. Confidentiality (i) (ii) Integrity Availability (iv) Authenticity Asymmetric Encryption algorithm protects 9) (i) Confidentiality (ii) Integrity (iii) Availability (iv) All of them 10) In which year Information Technology Act was implemented in India (i) 1998 (ii) 2000 (iii) 2004 (iv) 2008 11) In this technique hundreds or thousands of zombie computers are used to flood a device with requests. (ii) DDoS Man in Middle **Buffer Overflow** (iii) (iv) 12) attack occurs when a process attempts to store data in random access memory (RAM) beyond the boundaries of a fixed-length storage buffer. (i) DoS DDoS

(iv) Buffer Overflow

(iii)

Man in Middle

In this attack a query is sent to the database to check if a user has valid name and password. (ii) Password Guessing (ii) SQL injection attack (iii) Dictionary attack (iv) Brute Force attack (i) Input Validation (ii) Modify error report (iii) Isolate servers (iv) All of them (iii) Isolate servers (iv) All of them (iii) Isolate servers (iv) All of them (iii) Vulnerability Scanner (iv) All of them (iii) Port Scanner (iv) All of them (iii) Port Scanner (iv) All of them (iv) Vulnerability Scanner (iv) All of them (iv) Port Scanner (iv) Stalkers (iv) Port Scanner (iv) Stalkers (iv) Port Scanner (iv) Stalkers (iv) Public Cloud (iv) Virtual cloud (iv) Vulnerability Scanner (iv) Stalkers (iv) Global cloud (iv) Virtual cloud (iv) Bluebouth Scanner (iv) Bluebugger (iv) Bluebugger (iv) Bluebagger (iv) Bluebugger (iv) Bluebugger (iv) Bluedak (iv) Bluebugger (iv) Bluebugger (iv) Detection of SSID (iv) Bluebugger (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detection of SSID (iv) Detect	13)	In	this type of attack attacker halt the wir		oint, s	o that victim cannot get access of it.
In this attack a query is sent to the database to check if a user has valid name and password. (i) Password Guessing (ii) SQL injection attack (iii) Dictionary attack (iv) Brute Force attack (iii) Dictionary attack (iv) Brute Force attack (iii) Input Validation (iii) Modify error report (iii) Isolate servers (iv) All of them		(i)	Man in middle attack	(ii)	DoS a	attack
(ii) Password Guessing (ii) SQL injection attack (iii) Injut Validation (iii) Modify error report (iii) Injut Validation (iii) Modify error report (iii) Isolate servers (iv) All of them (iii) Isolate servers (iv) All of them (iii) Vulnerability Scanner (iii) Newtow's Scanner (iii) Newtow's Scanner (iii) Port Scanner (iv) All of them (iv) All of them (iv) Port Scanner (iv) All of them (iv) All of them (iv) Port Scanner (iv) All of them (iv) All of them (iv) Port Scanner (iv) All of them (iv) Port Scanner (iv) All of them (iv) All of them (iv) Port Scanner (iv) All of them (iv) All of them (iv) Port Scanner (iv) All of them (iv) Stalkers 18) When a service provider uses public cloud resources to create a private cloud is known as: (iv) Public cloud (iv) Virtual cloud (iv) Virtual cloud (iv) Virtual cloud (iv) Virtual cloud (iv) Public cloud (iv) All of them (iv) Bluebooth Jacking (iv) Bluebooth Scanner (iv) Bluebooth Scanne		(iii)	DDoS attack	(iv)	Wire	less attack.
This must be used to protect from a SQL injection attack (i)	14)	In	this attack a query is sent to the databa	ase to check if	a user	has valid name and password.
This must be used to protect from a SQL injection attack (i) Input Validation (ii) Modify error report (iii) Isolate servers (iv) All of them 16)		(i)	Password Guessing	(ii)	SQL i	njection attack
(i) Input Validation (ii) Modify error report (iii) Isolate servers (iv) All of them is used by attackers to find the open port in a network (ii) Vulnerability Scanner (iii) Network Scanner (iii) Port Scanner (iii) Phreakers (iv) Stalkers 18) When a service provider uses public cloud resources to create a private cloud is known as: (i) Public cloud (ii) Private cloud (iii) Global cloud (ii) Private cloud (iii) Global cloud (ii) Private cloud (iii) Global cloud (iii) Private cloud (iii) Global cloud (iii) Plussers (iv) Stalkers 19) This GUI based utility is used to find Bluetooth enabled devices (iii) Bluetooth Jacking (iii) Bluedoth Jacking (iv) BlueSmiff (iv) BlueSmiff (iv) Bluedoth Jacking (iv) BlueSmiff (iv) Bluedoth Jacking (iv) BlueSmiff (iv) Bluedoth Global Cloud (iv) BlueSmiff (iv) Bluedoth Global Cloud (iv) BlueSmiff (iv) Bluedoth Global Cloud (iv) BlueSmiff (iv) BlueSmiff (iv) Bluedoth Global Cloud (iv) BlueSmiff (iv) Bluedoth Global Cloud (iv) BlueSmiff (iv) BlueDmigger (iv) Blue		(iii)	Dictionary attack	(iv)	Brute	e Force attack
Solate servers Sola	15)	Th	is must be used to protect from a SQL i	njection attac	:k	
16		(i)	Input Validation	(ii)	Modi	ify error report
(i) Vulnerability Scanner (iv) All of them (iv) All of them (iii) Port Scanner (iv) All of them (iii) Phreakers (iii) Phreakers (iii) Phreakers (iv) Stalkers (iv) Stalkers (iv) Phreakers (iv) Stalkers (iv) Stalkers (iv) Stalkers (iv) Phreakers (iv) Stalkers (iv) Stalkers (iv) Phreakers (iv) Stalkers (iv) Stalkers (iv) Phreakers (iv) Stalkers (iv) Stalkers (iv) Phublic cloud (iv) Virtual cloud (iv) Virtual cloud (iv) Virtual cloud (iv) Ortrad standard (iv) Stalkers (iv) Bluetooth Jacking (iv) Bluetooth Jacking (iv) Bluetooth Jacking (iv) Bluetooth Jacking (iv) Bluesniff (iv) Bluebugger (iv) Bluesniff (iv) Bluebugger (iv) Bluesniff (iv) Bluebugger		(iii)	Isolate servers	(iv)	All of	them
(iii) Port Scanner (iv) All of them (ii) Foist ware (ii) Heedless guests (iii) Phreakers (iv) Stalkers (ii) Phreakers (iv) Stalkers (ii) Public cloud (ii) Private cloud is known as: (i) Public cloud (iii) Private cloud is known as: (ii) Public cloud (iii) Private cloud (iii) Global cloud (iv) Virtual cloud 19) This GUI based utility is used to find Bluetooth enabled devices (i) Bluetooth Jacking (ii) Bluetooth scanner (iii) Bluebugger (iv) BlueSniff (iii) Bluejack (ii) Bluesnarfer (iii) Bluejack (ii) Bluesnarfer (iii) Bluejack (iii) Bluesnarfer (iii) Blueidving (iv) Bluebugger 20) The attacker usually installs the sniffers on the wireless network and conduct activities such as: (i) Detection of SSID (ii) Collecting MAC address (iii) Collecting frame to crack WEP (iv) All of them 22) not involves in securing a wireless network (i) Disable remote login (ii) Disable WPA/WEP encryption (iii) Disable SSID Broadcast (iv) Enable Mac address filtering (ii) Spyware (ii) Logic Bumb (ii) Key Logger (i) Joint Sphere (ii) User Sphere (ii) Joint Sphere (ii) User Sphere (ii) Joint Sphere (ii) User Sphere (iii) Clinet Sphere (iv) Twitter Which among given is not a kind of cloud sphere? (i) Joint Sphere (ii) User Sphere (iii) MySpace (iv) Twitter Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) Dos Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (ii) Man in Middle (iii) Dos CCGA stands for (i) Cryptographically granteed Address (iv) None of them 28) Involves gathering information about individual about a target without his/her knowledge (ii) Passive Attack (iii) Forgery Attack (iv) Cyberstalking	16)		is used by attackers to find the	open port in a	a netw	ork
Counterfeit websites are used by to extract personal information. (i) Foist ware (ii) Heedless guests		(i)	Vulnerability Scanner	(ii) N	etwork	c Scanner
(i) Foist ware (ii) Heedless guests (iii) Phreakers (iv) Stalkers (iii) Phreakers (iv) Stalkers (i) Public cloud (ii) Private cloud is known as: (i) Public cloud (ii) Private cloud (iii) Global cloud (iv) Virtual cloud (iii) Global cloud (iv) Virtual cloud 19 This GUI based utility is used to find Bluetooth enabled devices (iv) Bluetooth Jacking (iv) Bluetooth scanner (iv) BlueBugger (iv) BlueSniff 20 is a tool which extract the data from the phone of a person even his/her mobile phone is switched off (i) Bluejack (ii) Bluesnarfer (iii) Bluediving (iv) Bluebugger 21 The attacker usually installs the sniffers on the wireless network and conduct activities such as: (i) Detection of SSID (ii) Collecting MAC address (iii) Collecting frame to crack WEP (iv) All of them 22 not involves in securing a wireless network (ii) Disable SSID Broadcast (iv) Enable Mac address filtering (iii) Spyware (ii) Logic Bumb (iii) Spyware (ii) Logic Bumb (iii) Spyware (ii) Logic Bumb (iii) Key Logger (iv) Annonymizer 24 Which among given is not a kind of cloud sphere? (i) Joint Sphere (ii) User Sphere (ii) Joint Sphere (ii) User Sphere (iii) MySpace (iv) Twitter 25 is a professional networking tool used to connect with community of top executives. (i) Facebook (ii) Linkedin (iii) NySpace (iv) Twitter 26 Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) Cryptographically generated address (iv) None of them 27 involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (iii) Forgery Attack (iv) Cyberstalking		•	•	, ,		
(iii) Phreakers (iv) Stalkers When a service provider uses public cloud resources to create a private cloud is known as: (i) Public cloud (ii) Private cloud (iii) Global cloud (iv) Virtual cloud This GUI based utility is used to find Bluetooth enabled devices (i) Bluetooth Jacking (ii) Bluetooth scanner (iii) BlueBugger (iv) BlueSniff	17)	Co	ounterfeit websites are used by	to extract	persor	nal information.
When a service provider uses public cloud (ii) Private cloud (ii) Public cloud (ii) Private cloud (iii) Global cloud (iv) Virtual cloud Public cloud (iv) Bluebouth scanner (iv) Bluebouth scanner (iv) Bluebugger (iv) Bluebniff Public cloud which extract the data from the phone of a person even his/her mobile phone is switched off (i) Bluejack (ii) Bluesnarfer (ii) Bluediving (iv) Bluebugger		(i)	Foist ware			=
(i) Public cloud (ii) Private cloud (iii) Private cloud (iii) Global cloud (iv) Virtual cloud (iv) Bluetooth Jacking (ii) Bluetooth Jacking (ii) Bluetooth scanner (iii) Bluebugger (iv) BlueSniff (iii) Bluebugger (iv) Bluebugger as person even his/her mobile phone is switched off (ii) Bluejack (iii) Bluebugger (iv) Bluebu		-				
This GUI based utility is used to find Bluetooth enabled devices (i) Bluetooth Jacking (ii) Bluetooth scanner (iii) Bluebugger (iv) BlueShiff	18)					
This GUI based utility is used to find Bluetooth enabled devices (i) Bluetooth Jacking (ii) Bluetooth scanner (iii) Bluebugger (iv) BlueShiff is a tool which extract the data from the phone of a person even his/her mobile phone is switched off (i) Bluejack (ii) Bluebugger (iii) Bluediving (iv) Bluebugger 21) The attacker usually installs the sniffers on the wireless network and conduct activities such as: (i) Detection of SSID (ii) Collecting MAC address (iii) Collecting frame to crack WEP (iv) All of them 22) not involves in securing a wireless network (ii) Disable SSID Broadcast (iv) Enable Mac address filtering 23) is a kind of malware whose presence is typically hidden from the user. (i) Spyware (ii) Logic Bumb (iii) Key Logger (iv) Annonymizer 24) Which among given is not a kind of cloud sphere? (i) Joint Sphere (ii) User Sphere (iii) Clinet Sphere (iv) Recipient Sphere 25) is a professional networking tool used to connect with community of top executives. (ii) Facebook (iii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS CGA stands for (iv) Cryptographically generated address (iv) None of them 27) CGA stands for (iv) Cryptographically granteed Access (iv) None of them (ivolves) passive Attack (iv) Passive Attack (iv) Cyberstalking						
(ii) Bluetooth Jacking (iii) Bluetooth scanner (iii) BlueBugger (iv) BlueSniff is a tool which extract the data from the phone of a person even his/her mobile phone is switched off iii Bluediving (iv) Bluebugger						
(iii) BlueBugger (iv) BlueSniff is a tool which extract the data from the phone of a person even his/her mobile phone is switched off	19)		•			
Sa tool which extract the data from the phone of a person even his/her mobile phone is switched off (i) Bluejack (ii) Bluebugger (iii) Bluediving (iv) Bluebugger (iv) Bluediving (iv) Bluediving (iv) Bluebugger (iv) Bluediving (iv) Bluebugger (iv) Bluediving (iv) Bluebugger (iv) Bluebugger (iv) Bluediving (iv) Bluebugger (iv) Bluebugge						
switched off (i) Bluejack (ii) Bluesnarfer (ii) Bluediving (iv) Bluebugger 21) The attacker usually installs the sniffers on the wireless network and conduct activities such as: (i) Detection of SSID (ii) Collecting MAC address (iii) Collecting frame to crack WEP (iv) All of them 22) not involves in securing a wireless network (i) Disable remote login (ii) Disable WPA/WEP encryption (iii) Disable SSID Broadcast (iv) Enable Mac address filtering 23) is a kind of malware whose presence is typically hidden from the user. (i) Spyware (ii) Logic Bumb (iii) Key Logger (iv) Annonymizer 24) Which among given is not a kind of cloud sphere? (i) Joint Sphere (iv) Recipient Sphere (ii) Clinet Sphere (iv) Recipient Sphere 25) is a professional networking tool used to connect with community of top executives. (ii) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (ii) Cryptographically generated address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking		(iii				
(ii) Bluejack (iii) Bluebugger The attacker usually installs the sniffers on the wireless network and conduct activities such as: (i) Detection of SSID (ii) Collecting MAC address (iii) Collecting frame to crack WEP (iv) All of them 22) not involves in securing a wireless network (ii) Disable remote login (ii) Disable WPA/WEP encryption (iii) Disable SSID Broadcast (iv) Enable Mac address filtering 23) is a kind of malware whose presence is typically hidden from the user. (i) Spyware (ii) Logic Bumb (iii) Ney Logger (iv) Annonymizer 24) Which among given is not a kind of cloud sphere? (ii) Joint Sphere (ii) User Sphere (iii) User Sphere (iii) Clinet Sphere (iv) Recipient Sphere 25) is a professional networking tool used to connect with community of top executives. (ii) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iv) Doos 27) CGA stands for (i) Cryptographically generated address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (ii) Passive Attack (iii) Active Attack (iv) Cyberstalking	20)	_		from the pho	ne of a	person even his/her mobile phone is
The attacker usually installs the sniffers on the wireless network and conduct activities such as: (i)				/::\ D	1	f
The attacker usually installs the sniffers on the wireless network and conduct activities such as: (i) Detection of SSID (ii) Collecting MAC address (iii) Collecting frame to crack WEP (iv) All of them 22) not involves in securing a wireless network (ii) Disable remote login (ii) Disable WPA/WEP encryption (iii) Disable SSID Broadcast (iv) Enable Mac address filtering 23) is a kind of malware whose presence is typically hidden from the user. (i) Spyware (ii) Logic Bumb (iii) Key Logger (iv) Annonymizer 24) Which among given is not a kind of cloud sphere? (ii) Joint Sphere (iv) Recipient Sphere (iii) Clinet Sphere (iv) Recipient Sphere 25) is a professional networking tool used to connect with community of top executives. (i) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking						
(i) Detection of SSID (ii) Collecting MAC address (iii) Collecting frame to crack WEP (iv) All of them 22) not involves in securing a wireless network	21\	-	-			
(iii) Collecting frame to crack WEP (iv) All of them 22) not involves in securing a wireless network (i) Disable remote login (ii) Disable WPA/WEP encryption (iii) Disable SSID Broadcast (iv) Enable Mac address filtering 23) is a kind of malware whose presence is typically hidden from the user. (i) Spyware (ii) Logic Bumb (iii) Key Logger (iv) Annonymizer 24) Which among given is not a kind of cloud sphere? (i) Joint Sphere (ii) User Sphere (iii) Clinet Sphere (iv) Recipient Sphere 25) is a professional networking tool used to connect with community of top executives. (i) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking	21)		-			
22) not involves in securing a wireless network (i) Disable remote login (ii) Disable WPA/WEP encryption (iii) Disable SSID Broadcast (iv) Enable Mac address filtering 23) is a kind of malware whose presence is typically hidden from the user. (i) Spyware (ii) Logic Bumb (iii) Key Logger (iv) Annonymizer 24) Which among given is not a kind of cloud sphere? (ii) Joint Sphere (iv) Recipient Sphere (iii) Clinet Sphere (iv) Recipient Sphere (iv) Facebook (iv) Linkedin (iv) Twitter 25) is a professional networking tool used to connect with community of top executives. (i) Facebook (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (iv) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (iv) Cyberstalking						
(i) Disable remote login (ii) Disable WPA/WEP encryption (iii) Disable SSID Broadcast (iv) Enable Mac address filtering 23)	221	(111)			(IV)	All or them
(iii) Disable SSID Broadcast (iv) Enable Mac address filtering 23) is a kind of malware whose presence is typically hidden from the user. (i) Spyware (ii) Logic Bumb (iii) Key Logger (iv) Annonymizer 24) Which among given is not a kind of cloud sphere? (i) Joint Sphere (ii) User Sphere (iii) Clinet Sphere (iv) Recipient Sphere 25) is a professional networking tool used to connect with community of top executives. (i) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking	22)	/:\ 		network	/::\	Disable MDA MATD anomination
23			_			
(ii) Spyware (iii) Logic Bumb (iii) Key Logger (iv) Annonymizer 24) Which among given is not a kind of cloud sphere? (i) Joint Sphere (ii) User Sphere (iii) Clinet Sphere (iv) Recipient Sphere 25) is a professional networking tool used to connect with community of top executives. (i) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking	221	(111)				_
(iii) Key Logger (iv) Annonymizer 24) Which among given is not a kind of cloud sphere? (i) Joint Sphere (ii) User Sphere (iii) Clinet Sphere (iv) Recipient Sphere 25)	23)	/:\ 		esence is typi		
24) Which among given is not a kind of cloud sphere? (i) Joint Sphere (ii) User Sphere (iii) Clinet Sphere (iv) Recipient Sphere 25) is a professional networking tool used to connect with community of top executives. (i) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDOS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Address (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Forgery Attack (iv) Cyberstalking						_
(i) Joint Sphere (iii) User Sphere (iii) Clinet Sphere (iv) Recipient Sphere 25) is a professional networking tool used to connect with community of top executives. (i) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking	24\				(IV)	Annonymizer
(iii) Clinet Sphere (iv) Recipient Sphere is a professional networking tool used to connect with community of top executives. (i) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking	24)			spnere?	···\	
25) is a professional networking tool used to connect with community of top executives. (i) Facebook (ii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking					` '	
(i) Facebook (iii) Linkedin (iii) MySpace (iv) Twitter 26) Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking	25)	(111)				
(iii) MySpace (iv) Twitter Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (iii) Active Attack (iv) Cyberstalking	25)	/:\		usea to conne		•
Which term best describes the type of attack that makes it possible to deny the service of a server using a computer? (i) Man in Middle (ii) DoS (iv) DDoS CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Address (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (iii) Forgery Attack (iv) Cyberstalking						
computer? (i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Address (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (iii) Forgery Attack (iv) Cyberstalking	26)					
(i) Man in Middle (ii) Buffer Over Flow (iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking	26)		• •	tack that mak	es it po	ossible to deny the service of a server using a
(iii) DoS (iv) DDoS 27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking					/::\	Duffer Over Flavo
27) CGA stands for (i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking						
(i) Cryptographically generated address (ii) Cryptographically granteed Access (iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking					(IV)	DDoS
(iii) Cryptographically granteed Address (iv) None of them 28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking	27)					
28) involves gathering information about individual about a target without his/her knowledge (i) Passive Attack (iii) Forgery Attack (iv) Cyberstalking		(1)	Cryptographically generated address		(11)	Cryptographically granteed Access
(i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking		(iii)	Cryptographically granteed Address		(iv	None of them
(i) Passive Attack (ii) Active Attack (iii) Forgery Attack (iv) Cyberstalking	28)	_	involves gathering information	on about indiv	idual a	about a target without his/her knowledge
(iii) Forgery Attack (iv) Cyberstalking	•	(i)				
			Forgery Attack		(iv)	Cyberstalking
	29)	` A	mail is also known as junk ma	il	. ,	

	(i)	Spoof			(ii)	Sp	am	
	(iii)	Fake			(iv)	Fr	aud	
30)	Pe	eople who send multi	ple mails from zoml	oie com	puters are k	cnowr	n as	
	(i)	Spoofer			(ii)	S	pies Kiddies	
	(iii)	Spammer			(iv)	_	Stalker	
31)	Tł	nis social media tool a	llows people to con	nect an	d share info	ormati	ion.	
,	(i)	Facebook			(ii)		inkedin	
	(iii)	MySpace			(iv)		witter	
32)		hich among these is i	not a threat from so	cial Me		•		
,	(i)	Malware Distribu			(ii)	St	talking	
	(iii)	Privacy Concern			(iv)		ll of them	
33)		e can use these built	in and add-on featu	ıres in v	, ,	•		us sites by:
,	(i)		ers in IE and Firefox		Web of			,
	(iii)	Clearing history o		(iv)				
34)	` '		que of changing an				ontrol address of a	network Interface
,	ca	ard to a different one		Ū				
	(i)	IP Spoofing		(ii)	MAC Spo	oofing	g	
	(iii)	IP Filtering		(iv)	=		=	
35)	lt	refers to a scenario w	herein an attacker	on host	A inserts A	betw	een all communicat	ions between host
	Χ	and Y.						
	(i)	Middle man		(ii)	Denial o	of Serv	vice	
	(iii)	Distributed Denia	of Service	(iv)	Bucket-k	brigad	le attack	
36)		is the crir	minal practice of usi	ing socia	al engineerir	ng usi	ng SMS service	
	(i)	Phishing		(ii)	Vishing			
	(iii)	Mishing		(iv)	Smishing			
37)	W	hich among given is a	Bluetooth hacking	tool				
	(i)	Bluejacking		(ii)	Bluebuggir	ng		
	(iii)	Car-Whispering		(iv)	All of them	n		
38)		can be used	l as IP address Mult	iplexer t	to enable to	conn	ect to number of co	omputers on the
	in	ternet						
	(i)	Web Server		(ii)	FTP Server	r		
	(iii)	Proxy Sever		(iv)	None of th	ne abo	ove	
39)		are softwar	e programs installe	d on a c	omputer sys	stem	which usually are lo	cated between OS
	ar	nd keyboard hardwar	e to record every ke	y stroke	<u>)</u> .			
	(i)	Keystroker		(ii)	PC Keylogg	ger		
	(iii)	Software Keylogger		(iv)	Anonymize	er		
40)	Α	computer program th	nat lies dormant and	d trigger	ed on a eve	ent on	a particular day is	
	(i)	Virus		(ii)	Logic Bom	ıb		
		Worm		(iv)	Trojan Ho			
41)		are used in d	enial of service atta	icks, typ	ically agains	st targ	geted websites.	
	(i) W	/orm		(ii)	Zombie			
	(iii) Vi			(iv)	Trojan Ho			
42)	<u> </u>		rus explicitly design				ection by antivirus.	
		alth Virus			Imorphic Vi	rus		
42\		rasitic Virus			acro Virus			
43)		is a program t		over ar	iotner inter	rnet-a	ittached computer	and then uses the
	(i) Wo	uter to launch attacks	•	(ii)Zor	nhia			
	(iii)Vir				ap doors			
441		us nputer security,	means that comp			asset	s can be modified	I by the authorized
	partie			Jaco Sys	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	45500	s can be mounted	S, the authorized

	(i) Confidentiality	(ii) Inte	egrity
	(iii) Availability	(iv) Au	thenticity
45)	Which of the following malicious program does		
	(i) Trojan	(ii) Viru	us .
	(iii) Worm	(iv) no	ne of these
46)	Ais a program that can infect other pr	ograms l	modifying them, the modification includes a
	copy of the virus program, which can go o	n to infe	ct other programs.
	(i) Worm	(ii) Viru	JS
	(iii) Zombie	(iv)Tra	p doors
47)	IPSec is designed to provide the security at the	!	
	(i) Transport layer		work Layer
	(iii) Application Layer		ssion Layer
48)	An attempt to make a computer resource unav		
	(i) DoS attack		us attack
	(ii) Botnet process	(iv) wo	rms attack
49)	Pretty good privacy (PGP) is used in	<u>-</u>	
	(i) Browser Security		ail Security
50 \	(iii) FTP Security	. ,	ne of these
50)		intormat	ion from a host that has no authority giving that
	information, then it is called (i) DNS Lookup	(;;) DNI	5 Hijacking
	(iii) DNS Spoofing		ne of these
51)	It is an eavesdropping on a wireless network to		
31,	(i) Sniffing	(ii)	Spoofing
	(iii) Scanning	(iv)	Blocking
52)	WEP stand for	(10)	Diocking
32)	(i) Wireless equivalence Protocol	(ii)	Wired equivalence Protocol
	(iii) Wireless equivalence Privacy	(iv)	Wired equivalence Privacy
53)			in the office, however they required regular access to
55)	data while on move	ttie tiirie	in the office, nowever they required regular access to
	(i) Tethered Workers	(ii)	Road Warrior
	(iii) Nomad	(iv)	Roaming Users
54)	• •		e hidden in images, audio/video files.
,	(i) Steganalysis	(ii)	Steganography
	(iii) Cryptography	(iv)	Cryptanalysis
55)	In this type of DoS attack there is/are not		
,	(i) DDoS	(ii)	HDoS
	(iii) PDoS	(iv)	
56)	• •		tack that uses a large pregenerated data set of hashes
,	from nearly every possible password?		5 1 5
	(i) Brute Force Attack	(ii)	Dictionary Attack
	(iii) Rainbow Table Attack	(iv)	
57)	This refers to harass an individual or group		
,	(i) Social Engineering	(ii	_
	(iii) Fraud	(iv	·
58)	Dumpster diving is an example of	`	, ,
,	(i) Social Engineering	(ii) Phishing
	(iii) Fraud	(i)	
59)	• •	•	ttempts to exploit computer application vulnerability
/	that are unknown to anybody in the world		, - p p p p
	(i) Zero day	(ii) Vulnerability
	-	•	·

	(iii)	Data Diddl	ing	(iv)	None of the above	
60)	_		is the criminal practice	of using social er	ngineering over tele	phone system
	(i)	Phishing		(ii)	Vishing	
	(iii)	Mishing		(iv)	Smishing	
61)	WPA2	2 is used for s	security in			
	(i) eth	nernet		(ii) Bl	uetooth	
	(iii) w	ifi		(iv) N	one of these	
62)			tic make Internet so attr			
			roundings within which	•	d	
			rovide an open, easy-to-	use network		
			ne need for firewalls			
C2 \			uire a fast computer to u			
63)			owing methods can effect			
			m and other system sof		ii) computer archite	ectural design
<i>C</i> 1\			stems design	(iv) Network design	
04)	(i) viru		II protect against?			
			ed interactive logins fror	n the "outside" v	vorld	
	(iii) fir		ta interactive logins iroi	Title outside i	voria	
			and from the "outside"	world		
65)			ts on the security of a co		or network are	
•			n ii)Interception iii) mo			
	(i) i, ii	, iii and iv on	ly			
	(ii) ii,	iii, iv and v o	nly			
		ii, iii and v or				
		of the above				
66)			e more important becau	se of the increas	ed use of computer	s, the internet and
	WW\				/::\	
		tural Disaste			(ii)Hardware Malfur	
67)	לם (ווו)		and data security a computer on a netwo		iv)Malicious deletio	
07)		uters on that	•	ik willeli acts as	an intermediary for	connections with other
	(i)	Web	t network	(ii)	FTP	
	(iii)	Mail		(iv)	Proxy	
68)	(''')		type of deception desig	, ,	=	ion credit card details
00,	n n		count data or other info	-	r personal illiorinati	ion, creare cara actums,
	(i)	Phishing			Social Engineerin	g
	(iii)	Spamm		(iv)	Hacking	5
69)		· · · · · · · · · · · · · · · · · · ·	/ireless Access Point can	, ,	_ characters.	
,	(i)	16		. <u></u>	_ 	
	(iii)	24		(iv)	32	
70)		QL injection	attack involves			from a web page/web site.
	(i)	GET			POST	· -
	(iii)	SELECT		(iv)	DELETE	
71)	Ir	n this technic	que attacker often launc	hes an attack on	wireless network b	y creating a new network with
	S	trong signal s	strength.			
	(i)	Sniffing		(ii)	Spoofing	
	(iii)	Man in	the Middle	(iv)	DoS	
72)	A	A software uլ	pdate to fix a security fla	w or other prob	lem is known as	
	(i)	Repair		(ii)	Patch	
	(iii)	Hot Fix		(iv) Exploit	
73)	А	program that	at hides its true intent a	nd then reveal it	self when activated	is known

	(i)	Trojan Horse	(ii)	Virus
	(iii)	Worm	(iv)	Zombie
74)		software defect is considered as	` ,	
,	(i)	Asset	(ii)	Threat
		Vulnerability	(iv)	Risk
75)		hich term best describes the type of attack that r		
, 5,		ith each other, when actually they are sending an		
	(i)	Spoofing	(ii)	Middle Man
	(iii)	Man in Middle	(iv)	
76\	(111)			Replay
76)	/:\ 	scanning is to understand the state		
	(i)	Port	(ii)	Network
	(iii)	Vulnerability	(iv)	System
77)		of the following describes someone who gains il		
	(i) Hac			Identity theft
	(iii) Int			Cyber-terrorist
78)		of the following are the ethical issues facing the		
		ail Privacy		Software piracy
		ellectual property		All of the above
79)		of the following is used to send secure messages	from	one location to another using a public network
		s the Internet?		
		sical Public Network		Virtual Public Network
		ysical Private Network		Virtual Private Network
80)	Which		cure c	communication between two entities through the
	use of	G		
		tal Signature encryption		Public key encryption
		vate key encryption	(iv)	All of the above
81)	What	is the maximum header size of an IP packet?		
	(i) 32 k			64 bytes
	(iii) 30		(iv)	62 bytes
82)		of the following is/are Protocols of Application?		
	(i) FTP			DNS
	(iii) Te			All of the above
83)			at por	t will I need to open on my firewall to allow these
		ncrypted packets to flow?		
	(i) 161		(ii) !	
	(iii) 60		(iv)	443
84)		lress consists of bits.		
	(i) 32			128
	(iii) 64		٠,	256
85)		ectual property rights and are	two of	f the most important developing areas of
	law.			
		er Law		copyright infringment
		tent law		trademark infrignment
86)	Comm	ercial use domain names will normally use the	foll	owing suffix in their website address.
	(i) .net		(ii) .	.gov
	(iii) .cc			.org
87)	It is a to	echnique breaking into phone or other communic	cation	systems.
	(i)	Hacking	(ii)) Cracking
	(iii)	Phreaking	(iv	v) War dialler

88) This process involves changing contents of a website depending upon a user's IP address and geographical location.

	(i)	IP base bloc	cking		(ii)	IP base clocking
	(iii)	Industry Esp	pionage		(iv)	None of them
89)	W	hich term be	est describes the type of passv	word a	ttack that	uses a large pre-generated data set of
	ha	shes from n	early every possible password	Ι?		
	(i)	Brute Force	e Attack		(ii)	Dictionary Attack
	(iii)	Rainbow Ta	ible Attack		(iv)	Host File Attack
90)	W	hat is the ma	aximum header size of an IP p	acket?	•	
	(i)	32 bytes			(ii) 64	bytes
	(ii	i) 30 bytes			(iv) 62	bytes
91)		Co	okies are also known as Store	d cook	ies.	
	(i)	Session		(ii)	Persiste	
	(iii)	Transient		(iv)	Web bas	sed
92)		invo	olves altering raw data just bef	fore it i	is process	sed by computer.
	(i)	Forgery att	tack	(ii)	Data D	Diddling attack
	(iii)	Salami atta	ack	(iv)	None	of the above
93)		scar	nning is to understand the exis	sting w	eakness i	n the system
	(i)	Port		(ii)	Netwo	ork
	(iii)	Vulnerabili	· ·	(iv)	Syster	
94)			ie breaking into phone or othe			
	(i)	Hacking		(ii)	Cracki	_
	(iii)	Phreaking		(iv)	War d	
95)			nd this attack is to deduct a sm	nall am	ount of n	noney which would go completely unnoticed in
a firs	t sight			···	5 . 5.	Luc
	(i)	Salami		(ii)	Data Dic	_
0.5)	(iii)	Web Jackin	=	(iv)	Spoofing	
96)			ne take control of your website			1.10
	(i)	Salami		(ii)	Data Did	_
07)	(iii)	Web Jackin	-	(iv)	Spoofing	_
97)			est describes the type of attac	k that	makes it j	possible to deny the service of a server using a
comp	outer?		ا حال م	/::\	Dff a.r. O	Non Flaur
	(i)	Man in Mid	idie	(ii)		over Flow
00)	(iii)	DoS	sishing mathad involves the w	(iv)	DDoS	mails bearing falsified cornerate identification
98)			iisning method involves the us		Rod and	mails bearing falsified corporate identification.
	(i)	Dragnet		(ii)	Gilnet	reei
00)	(iii)	Lobsterpot	phiching attack browser of a	(iv)		d to radiract him /har to a fake wah site
99)	ın					d to redirect him/her to a fake web site.
		(i)	Dragnet	(ii)		nd reel
100\		(iii)	Lobsterpot	(iv)	Gilnet	
100)		ID stand for		/:: \	Comit	o Sot ID
	(i) (;;;)	System Ser Service Set	rvice Identifier	(ii)		e Set ID
	(iii)	sei vice set	. identinei	(iv)	none	of the above



End Term Exam

	Semeste	er	
Roll No:			[Total No. of Pages:04]
Date:			Time: 90 minutes
Department:			
Title of the Course: Cyber S	Security		Max. Marks: 100
Course Code: HUL 2401			
Q1 Which of the following	ng uses two keys to encrypt a	Q13 This computer program lie	es dormant and triggered on a
message?		event on a particular day is:	
(a) Symmetric encryption	Algorithms	(a) Worm	(b) Logic Bomb
(b) Hashing Algorithm	-	(c) Virus	(d) Trojan Horse
(c) Asymmetric encryptio	n Algorithm	Q14 "Do no evil" is the motto o	
(d) None of the above		(a) Microsoft	(b Google
	shers identify the victim in advance:	(c) Yahoo	(d) Intel
(a) Dragnet	(b) Lobsterpot		es the type of attack that makes it
(c) Rod and reel	(d) Gilnet	from different geographical loca	a server using multiple computers
Q3 Which among these is a f	<u> </u>	(a) Buffer Over flow	(b) DoS
	(b) Availibility	(c) Man in Middle	(d) None of these
(c) Authenticity	(d) None of these	` '	the type of attack that makes it
recovery of the server	there is/are not any chance of the	seem like two computers are co	
(a) HdoS	(b)DDoS	·	_
(c) SdoS	(d) PDoS	when actually they are sending	and receiving data with a
Q5 Which statement about vi	` '	computer between them?	
	ects the storage media	(a) Spoofing	(b) Middle Man
B. Program virus is a hy		(c) Bucket Brigade	
	self so detection is not easy	Q17 Ais a prograr	
 D. Multipartite virus ta 	rget .exe files	another Internet-attached co	
(a) Both A and B	(b) Both A and C		-
(c) Both A and D	(d) None of them	computer to launch attacks.	
Q6 An attempt to make a cor	mputer resource unavailable to its	(a) Worm (c) Virus	(b) Zombie (d) Trap doors
intended users is called.		Q18 This type of attack involves	. , .
(a) Virus attack	(b) Worm attack	* *	dge, for example which the IN and
(c) Botnett Process	(d) Denial of Service	OUT time of an employee.	age, for example which the hy and
	criminal practice of using social	(a) Passive attack	(b) Active attack
engineering over telephone.		(c) Forgery attack	(d) None of these
(a) Phishing	(b) Mishing		ta Integrity and Data Security is
(c) Vishing	(d) Smishing		,
Q8 attack is a cor	nputer threat which attempts to rulnerability that are unknown to	(a) Limiting physical acces	ss to computer systems; assigning
anybody in the world.	differentiate and distribution to	passwords to users.	
(a) Zerod day	(b) Vulnerability	(b) Consistent, accurate a	nd reliable data; protection of data
(c) Data Diddling	(d) Salami	from unauthorized access.	
Q9 Which among given is a B	• •	(c) Encryption; Audit trails	
(a) Bluejacking	(b) Blue bugging	(d) Distributing work to p	preserve integrity; installing system
(c) Car Whispering	(d) All of them	passwords	
Q10 In asymmetric cryptograp	hic algorithm when Tom wants to		means that computer
send a message to Alisha	he will decrypt it with	system assets can be modified of	• •
	b) Public key of Alisha	(a) Confidentiality	(b) Integrity
(c) His Private Key ((c) Availability	(d) Authenticity
Q11 Another name of Public K		Q21 It is a type of program do r (a) Worm	(b) Zombie
(a)Symmetric Key Cryptog		(c) Trojan Horse	(d) Logic Bomb
(b) Private key Cryptogra	-	Q22 Which of the following is in	· · · -
(c) Asymetric key Cryptog	тарпу	that need not any host program	
(d) None of the above			o) Trojan Horse
	re programs installed on a computer	The state of the s	I) Worm
	ocated between OS and keyboard		a "trading name that a business
hardware to record every key		trader use under commercial pu	_
(a) Key Stroker ((c) Software Key logger	b) Key Logger (d) Annonymizers	(a) Trade Secret (b) Trade Name
(c) software key logger	(u) Annonymizers	(c) Datont	I) Cony Bight

(c) Patent

(d) Copy Right

Q24 Doodle me Diddle fraud h	neld in 1996 in India was a	Q38 is a generic term wh	ich refers to all the legal and
type of cyber crime		regulate aspects of Internet and t	
(a) Salami (b	Credit Card	(a) Cyber Law	(b) Cyber Dyne
(c) Data Diddling (d	None of them	(c) Cyber Cafe	(d) Electronic Law
Q25 The purpose of a DoS attac			nd science of detecting messages
	vith traffic, thereby preventing		ages, audio/video files using
legitimate network traffic		steganography	
(b) Disrupt connection bety		(a) Cryptography	(b) Steganography
	ividual to access the service(s).	(c) Cryptanalysis	
(d) All of them			connect with a network which is
Q26 Which of the following is is		block through the firewall of the	_
	tronic device such as a chip card or		FTP Server
computer memory?		(c) Proxy Server (d)	
(a) Hard Cash	(b) Business Card	Q41 We can categorize threats as	
(c) E-Cash	(d) E-Card	(a) Passive attack (b) (c) Both a and b (d)	Active attack
	ss to a computer system would fall		
under which category of compu	ter crime?	Q42 Which among these is pu	ırpose of hacking
(a) Hacking		(a) Greed	(b) Revenge
(b) Theft of Service		(c) Desire to access forbidde	n information (d) All
(c) Destruction of data & So	oftware	Q43 are the symbols u	sed by busineses to identify their
(d) Data Theft		goods and services.	
	your system you receive an email	(a) Trade Mark	(b) Trade Secret
from an organization asking	that you verify your account	(c) Designs	(d) None of them
information within 12 hours, o	r your account will be closed, the	Q44 is a preparation to	wards preattack.
best thing to do is		(a) Passive attack	(b) Active attack
(a) Reply to the email askin	g them why this information is	(c) Reconnaissance	(d) None of them
required.		Q45 Whenever, by words either s	spoken or intended to be read, or
(b) Reply to the email with	the information asked for	by signs or by visible representati	ions, makes or publishes any
(c) report the email to the	actual organization and then	imputaion concerning any persor	
delete the email.		or having reason to believe that s	such imputation will harm, the
(d) None of these		reputation of such person is said:	
Q29 A is a docume	ent that grant the holder exclusive	(a)Cyber Stalking	(b) Phishing
right on an invention for fixed r	number of years.	(c) Social Engineering	
		Q46 cipher replaces	
(a) Copy Right	(b) Patent	another character to crea	
(c) Trade Mark	(d) Trade Secret	another character to crea	te cipiler text.
		(a) Substitution	(b) Transposition
Q30 Which of these companies	is not a leader in Cloud		
Computing?		(c) either (a) or (b)	
(a) Google	(b) Amazon	Q47 Information Technology Act	ITA was amended in
(c) Microsoft	(d) Blackboard	year in India	(1.) 2004
	of intercepting wireless data that	(a) 2000	(b) 2004
is broadcasted on unsecured ne	twork.	(c) 2008	(d) 2012
(a) Spoofing (b) Sniffing	Q48 A cookie that was not create	ed by the Web site that attempts
(c) Spamming (d	None of them	to access it is called a	
Q32 Which of the following is a	cyber crime?	(a) First-party cookie	(b) Second-party cookie
(a) Hacking (b	Worm Attack	(c) Third-party cookie	(d) Fourth-party cookie
(c) Virus Attack (d	None of these		
Q33 This attack involves altering	g raw data just before final	Q49 A hacker who claims to be m	notivated by improving security
processing and then changing it	back after the processing is	by uncovering vulnerabilities is ca	alled.
completed:		(a) Black hat attacker	(b)White hat attacker
(a) Data Tampering (b) Data Diddling	(c)Cowboy attacker	(d) Resource attacker
) None of these	Q50 This mechanism is used to	protect private networks
	s which effect/ infects the storage	from outside attack is	
media on which OS is stored.	,	(a) Firewall	(b) Antivirus
(a)Boot Sector Virus (b) Program Virus	(c) Digital signature	
` ') Stealth Virus	Q51 can be used as	
	must do to protect a	to connect to number of cor	
wireless network.	must us to protect u		FTP Server
(a) MAC address filtering	(b) Disabling SSID	. ,	
	(d) All of them		None of these
(c) Disbaling Mac filtering	• •	Q52 Which term best describes the	
	nto phone or other communication		ata set of hashes from nearly
systems. (a) Hacking (b)	\ Cracking	every possible password?	(h) Dictionary Attack
	Cracking	(a) Brute Force Attack	(b) Dictionary Attack
) War dialling	(c) Rainbow Table Attack	
	on your computer to detect the	Q53 This technology is used to de	
presence of a key logger	(b) Anti Kaylaggar	body uniqueness for authenticati	
(a) Keylogger	(b) Anti Keylogger	(a) Footprinting	(b) Biometric
(c) Software Keylogger	(d) Hardware Keylogger	(c) JBOD	(d) Anthropomorphism

	Multiple ping packets are send which results into more traffic		Q69 Poorly designed social networking vulnerable to		
	handle, in this type of denial o		(a) Buffer overflow attack (c) Non- Persistent cross-site scrip	(b) SQL injection attack	
	(a) Flood attack (c) SYN attack	(b) Ping of death attack (d) Smurf attack	(d) Persistent cross-site scripting a	=	
	It is a way of generating significan	` '	Q70 A SQL injection attack may be use		
	on a victim network.	•	(a) Change number of coloumns in	n a table	
	(a) Flood attack	(b) Ping of death attack	(b) Read a row in a table(c) Change coloumn name in a table	ماد	
	(c) Teardrop attack	(d) Smurf attack	(d) None of them	ЛС	
	When the control of a web site is considered as	e is taken by an attacker	Q71 The most effective remedy for SQ	L injection attacks is	
	(a) Data Diddling	(b) Salami	(a) To filter HTML form input at th		
	(c) Web theft	(d) Web Jacking	(b) To employ stored procedures		
	This is installed between coputer a		(c) To employ prepared SQL state(d) To perform input validation or		
	the log of keys pressed by user.		expression	i tile server via regular	
	(a) PC Key logger	(b) Software key logger	Q72 Tasks performed by firewall include	de	
	(c) Hardware key logger	(d) None of them		et Integrity Checking	
	This process involves changing co depending upon a user's IP address		(c) IP address spoofing (d) All		
		(b) IP Base Blocking	Q73 The role of a payment gateway is		
	(c) Industry Espionage	(d) None of them	(a) A proxy to the merchant	- wl.	
	Which among given is/are challen	ge(s) for any organization	(b) A proxy to the bankcard netwo(c) A financial service provider	ork	
	(a) Employee wasted time on	internet	(d) A government regulator		
	(b) Controlling Access to Web	Application	Q74 The motivation of an ethical hacke	er is	
	(c) Bandwidth Wastage		(a) Financial gain		
	(d) All of them		(b) The thrill of hacking		
	This techniques is used on a wirele	ess network to scan the	(c) To desire to identify vulnerabil	ities so they can be patched	
	vork passively. (a) Scanning	(b) Spoofing	before they are publicaly exposed (d) A religious/political/ideological	al cause	
	(c) Sniffing	(d) All of them	Q75 Which of the follwoing is/are necessary		
	This in built feature of web brows	• •	attack		
	malicious sites by:		(a) Use of a TCP SYN packets		
	(a) Anti-phishing filters in IE a	ind Firefox	(b) Use of a spoofed IP address		
	(b) Web of Trust		(c) Use of multiple attackers georg	graphically dispressed	
	(c) Clearing history of browse	er	(d) Use of malformed IP packets	antad within the cocurity	
	(d) Addlock Plus		Q76 An attack originating and/or atter perimeter of an organization is		
	is a social media co	_	(a) Active	(b) Inside	
peo	ple to connect and share inf		(c) Passive	(d) Outside	
	(a) Facebook	(b) My Space	Q77 The attacker usually installs the sr	niffers on the wireless	
Q63	(c) Linkedin is not a cloud sphere.	(d) Twitter	network and conduct activity such as:	//-> C-II+: NAAC -	
QUS	(a) Joint Sphere	(b) User Sphere	(a) Detection of SSID (c) Collecting fram to creack WEP	(b) Collecting MAC address	
	(c) Recipient Sphere	(d) Client Sphere	Q78 A Digital certificate is used to bind		
Q64	Secret key cryptography is synoyn		(a) A person's public key to his pri		
	(a) Symmetric Key Cryptography		(b) A person's public key to his identity		
	(b) Asymmetric key cryptography		(c) A person's private key to his id		
	(c) Private key cryptography (d) Quantum Cryptography		(d) A person's signature to his priv		
	To encypt a message from Aman t	o Alka using public key	Q79 Which of the following attacks is/sidentity theft?	are likely to result in	
	cryptography, the following is nee		(a) Phishing attack	(b) Denial of Service attack	
	(a) Aman's private key	(b) Aman's public key	(c) Virus Infection	(d) All	
		(d) Alka's public key	Q80 In which of the following does sor	meone use an application to	
Q66	Which of the following protocols is	s used in accessing web	capture and manipulate packets a	as they are passing through	
	mail? (a) SMTP	(b) HTTP	your network?	(1) 5 1 1	
	(c) POP3	(d) IMAP	(a) DoS (c) Man in Middle	(b) Backdoor(d) Spoofing	
	The buffer overflow attack is cause	` '	Q81 is a "technique to inf		
•	(a) A vulnerability in the design of		the information or perform some		
	(b) A Vulnerability in the implem	nentation of a networking	(a) Social Engineering	(b) Phishing	
	protocol		(c) Cyber stalking	(d) None	
	(c) A vulnerability in human beh	aviour	Q82 In this technique user tries to get		
	(d) A vulnerability in softwareA counter- measure to eavesdrop	ping on the communication	personal data- such as credit card account data and other information		
	s the use of	E o on the communication	provide it under false pretenses.	on by convicting the user to	
	(a) A cryptography checksum	(b) Encryption	(a) Phishing	(b) Data Diddling	
	(c) A login name and password	(d) A fake identity	(c) Salami	(d) DoS	

Q83 In this netizens to the website designed and developed by		
him, by altering the browser address bar through java script		
commands.	(h) Mala Fannani	
(a) Flash Phishing	(b) Web Forgery	
(c) Phone Phishing	(d) Social Phishing	
Q84 It involves harassing or threa individual will conduct repeated		
visiting a person's home and/or b		
(a) Phishing	(b) Social Engineering	
(c) Cyber Stalking	(d) None	
Q85 Security risks from social enginee	• •	
(a) Malware distribution	(b) Cyber bullying	
(c) Privacy concern	(d) All	
Q86 Threats are categorized as:	(u) All	
(a) Passive or active	(b) Traffic	
(c) Masquerade	(d) Others	
Q87 How are viruses spread?	(a) Stricts	
The state of the s	nloading infected programs	
and files from internet.	modalily infected programs	
(c) Garbled information. (d) Instal	ll anti-virus	
Q88 DDoS stand for		
(a) Distributed Denial of Service a	nttack	
(b) Digital Data Output Spoit	ictack	
(c) Damaging Downtime of Syster	m	
(d) Distributed Destruction of Sys		
Q89 is not a kind of cyber at		
(a) Cber Stalking	(b) Micro sites	
(c) Firewall attack	(d) E-Mail	
Q90 The latest WLAN standard is:	(4) =	
(a) 802.11g	(b) 802.11n	
(c) 802.12g	(d) 802.12n	
Q91 The following is used when the so	• •	
software is unavailable	р	
(a) Blackbox testing	(b) Whitebox testing	
(c) Regrssion testing	(d) Unit testing	
Q92 Which of the following is/are true	. ,	
malware:		
(a) A worm attaches itself to a f	ile or program	
(b) A Trojan is stand-alone prog		
(c) A virus does not necessarily		
(d) All of the above		
Q93 cryptography technique is	s used for ATM cards	
(a) Symmetric	(b)Assymetric	
(c) Hashing	(d) None	
Q94 cipher takes one character	• •	
another.		
(a) Stream	(b) Single	
(c) Substitution	(d) Hash	
Q95 The purpose of digital signatue is,	/are	
(a) Verify Sender (b)Prove		
(c) Prevent sender from disowing		
(d) All	,	
Q96 is the science of tran	sforming information into a	
secure form so that unauthorized user		
(a) Steganography	(b) Cryptography	
(c) Neither a nor b	(d) Both a and b	
Q97 A victim unknowingly downloads	• •	
type of crime.		
(a) Type 1 Cyber crime	(b) Type 2 Cyber crime	
(c) Type 3 Cyber crime	(d) Type 4 Cyber crime	
Q98 Survival mantra for netizens is are		
(a) Keep genuine software		
(b) keep browsers updated with	security patches	
(c) Keep an effective Antivirus a		
(d) All of them	a apaates	
Q99 is a technique of cha	nging an assigned Media	
Access Control address of a network Ir		
one		

(b) IP Filtering

(a) IP Spoofing

(c) MAC Spoofing (d) MAC Filtering Q100 This is used by attacker to automatically dialls a phone number looking for a computer on the other end.

(a) Dialler (c) Self dialler (b) Auto dialler

(d) War dialler



End Term Exam

Semester - VII

Roll	No:			[Total No. of Pages:04]
Dat				Time: 90 minutes
Department: Title of the Course: Cyber Security			Max. Marks: 100	
	e of the course. Cyber Sec irse Code: HUL 2401	urity		IVIAX. IVIAI KS. 100
Cou	1136 COUE. 110L 2401			
Q1	D DoS stand for		Q13 Which of the followi	ng is not a method to preserve the
	(a) Dual Disk Operaing System	m	security and Integrit	y of Information?
	(b) Denial of Services		(a) An Antivirus Sof	tware (b) Firewall
	(c) Distributed Denial of Se	rvices	(c) Phishing	(d) Disk Encryption
	(d) None of these			n this technique attacker insert a new
Q2	Which among these is a m	nail protocol	node 'X' between two exist	
	(a) SMTP	(b) IMAP	(a) Spoofing	(b Sniffing
	(c) POP	(d) All of them	(c) Man in Middle	(d) DoS
Q3	Which among these is a feat	ure of Hashing	Q15 Which term best desc	cribes the type of attack that makes it
	(a) Transposition	(b) Availibility	possible to deny the service	e of a server using multiple computers
	(c) either (a) or (b)	(d) Neither (a) nor (b)	from different geographical	locations?
Q4	Which of the following acc	curately reflects the purpose of	(a) Buffer Over flow	(b) DoS
steg	anography?		(c) Man in Middle	(d) None of these
	(a) Steganography scrambles	a message so that it cannot be	Q16 A program advertised a	as performing one activity but actually
view	ved		doing something else, or pe	erforming both the advertised and
	(b) Steganography hides the		malicious activities	
	(c) Steganography exposes h			
	(d) Steganography encrypts	cleartext data.	(a) Trojan Horse	(b) Virus
Q5	We don't want our packets	s to get lost in transit. Which	(c) Worm	(d) Logic Bomb
OSI	layer is responsible for ord	lered delivery of packets?	Q17 A is a progr	am that secretly takes over
	(a) Network	(b) DatalLink	another Internet-attache	ed computer and then uses that
	(c) Transport	(d) Physical	computer to launch attac	cks.
		he type of attack that makes it	(a) Trap door	(b) Trojan Horse
	m like two computers are com	=	(c) Worm	(d) Logic Bomb
	en actually they are sending a	nd receiving data with a	Q18 Another name of Publi	c Key Cryptography
com	puter between them		(a)Symmetric Key Cryp	otography
	(a) Phishing	(b) Social Engineering	(b) Private key Cryptog	graphy
	(c) Fraud	(d) Cyber Stalking	(c) Asymetric key Crypt	tography
Q7		ninal practice of using social	(d) None of the above	
engi	ineering over telephone.	(b) Miching	Q19 Difference between	Data Integrity and Data Security is
	(a) Phishing	(b) Mishing		
Q8	(c) Vishing	(d) Smishing Iter threat which attempts to	(a) Limiting physical a	access to computer systems; assigning
	-	erability that are unknown to	passwords to users.	
	body in the world.	crabinty that are unknown to	(b) Consistent, accurat	te and reliable data; protection of data
u,.	(a) Zero day	(b) Vulnerability	from unauthorized access.	
	(c) Data Diddling	(d) Salami	(c) Encryption; Audit to	
Q9	Which among given is a Blue	• •	• • • •	to preserve integrity; installing system
	(a) Bluejacking	(b) Blue bugging	passwords	
	(c) Car Whispering	(d) All of them		embedded in some legitimate program
Q10		algorithm when Tom wants to		en certain conditions are met
	send a message to Alisha he		(a) Confidentiality	(b) Integrity
	(a) His Public Key (b)	Public key of Alisha	(c) Availability	(d) Authenticity do not replicate automatically?
		Private key of Alisha	(a) Worm	(b) Zombie
Q11	. This type of attack involves g	athering information about	(c) Trojan Horse	(d) Logic Bomb
	_	ge, for example which the IN and	· · · · ·	is independent malicious program
OUT	Ttime of an employee.		that need not any host prog	· · · · · · · · · · · · · · · · · · ·
	(a) Passive attack	(b) Active attack	(a) Trap doors	(b) Trojan Horse
	(c) Forgery attack	(d) None of these	(c) Virus	(d) Worm
		programs installed on a computer	` ,	ates copies during replication that are
		ed between OS and keyboard		have distinctly different bit patterns.
hard	dware to record every key stro		(a) Boot Sector Virus	(b) Polymorphic Virus
	(a) Key Stroker	(b) Key Logger	(c) Parasitic Virus	(d) Micro Virus
	(c) Software Key logger	(d) Annonymizers		

Q24 Doodle me Diddle fraud held in 1	996 in India was a	Q38 is a generic term	which refers to all the legal and
type of cyber crime		regulate aspects of Internet ar	nd the World Wide Web
(a) Salami (b) Credit ((a) Cyber Law	(b) Cyber Dyne
(c) Data Diddling (d) None of	f them	(c) Cyber Cafe	(d) Electroni Law
Q25 The purpose of a DoS attack is/are:	· · · · · · · · · · · · · · · · · · ·		detects messages that are hidden in
(a) Flood a network with tra-	ffic, thereby preventing	images, audio/video files	
legitimate network traffic			(b) Steganography
(b) Disrupt connection between two	-	(c) Cryptanalysis	
(c) Prevent a particular individual to	access the service(s).		used by attackers to connect with
(d) All of them	ing for use quarthe		igh the firewall of the organization
Q26 Which of the following is issued only		institution.	(b) FTD Comion
Internet and is stored in an electronic de	evice such as a chip card of	` '	(b) FTP Server
computer memory?	h) Business Card		(d) None of these
	b) Business Card	Q41 Threats can be categorize	
	d) E-Card		(b) Active attack
Q27 Gaining unauthorized access to a co			(d) None of them
under which category of computer crime	= :	Q42 For a hacker the purpos	
(a) Hacking		(a) Greed	(b) Revenge
(b) Theft of Service(c) Destruction of data & Software			dden information (d) All
• •			ls used by busineses to identify thei
(d) Data Theft	*	goods and services.	// \ = \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
Q28 On day while working on your sys		(a) Trade Mark	(b) Trade Secret
from an organization asking that y		(c) Designs	(d) None of them
information within 12 hours, or your actions in the second	ccount will be closed, the	Q44 is a preparation	
best thing to do is			(b) Active attack
(a) Reply to the email asking them v	why this information is	(c) Reconnaissance	
required.			er spoken or intended to be read, o
(b) Reply to the email with the infor			tations, makes or publishes any
(c) report the email to the actual or	ganization and then		son intending to harm, or knowing
delete the email.		_	at such imputation will harm, the
(d) None of these	and the selection and the selection	reputation of such person is sa	
Q29 A is a document that g			(b) Phishing
right on an invention for fixed number o	or years.		(d) Cyberdefamation
(a) Carry Biolet	h) Datast	Q46 cipher replac	
. , , , ,	b) Patent	another character to cr	eate cipher text.
(c) Trade Mark	d) Trade Secret		
030 An attained to make a commutan mass		(a) Substitution	(b) Transposition
Q30 An attempt to make a computer res	source unavailable to its	(c) either (a) or (b)	(d) neither (a) or (b)
intended users is called (a) Denial of Service attack ((la) Minus attack	Q47 In India Information Tech	nology Act ITA was amended in
	(b) Virus attack	year.	
• •	d) Botnet Process	(a) 2000	(b) 2004
Q31is the simple process of interc	epting wireless data that	(c) 2008	(d) 2012
is broadcasted on unsecured network.	_	` '	eated by the Web site that attempts
(a) Spoofing (b) Sniffing	•	to access it is called a	eated by the Web site that attempts
(c) Spamming (d) None of			(h) Second party cookie
Q32 Which of the following is a cyber cri		(a) First-party cookie	(b) Second-party cookie
(a) Hacking (b) Worm A		(c) Third-party cookie	(d) Fourth-party cookie
(c) Virus Attack (d) None of		040 A backer who claims to b	a mativated by improving cocurity
Q33 This attack involves altering raw dat			e motivated by improving security
processing and then changing it back after	er the processing is	by uncovering vulnerabilities i	
completed:	al all the co	(a) Black hat attacker	(b) White hat attacker
(a) Data Tampering (b) Data Di	_	(c)Cowboy attacker	(d) Resource attacker
(c) Salami Attack (d) None of			I to protect private networks
Q34 is a type of virus which e	effect/ infects the storage	from outside attack is	
media on which OS is stored.		(a) Firewall	(b) Antivirus
(a)Boot Sector Virus (b) Program		(c) Digital signature	• • • •
(c) Multipartite Virus (d) Stealth		Q51 can be used	as IP address Multiplexer to enable
Q35 Network administrator must d	o to protect a	to connect to number of	computers on the internet.
wireless network.		(a) Web Server	(b) FTP Server
	b) Disabling SSID		(d) None of these
	d) All of them		es the type of password attack that
Q36 It is a technique breaking into phon	e or other communication	uses a large pregenerate	d data set of hashes from nearly
systems.		every possible password?	
(a) Hacking (b) Cracking	g	(a) Brute Force Attack	(b) Dictionary Attack
(c) Phreaking (d) War dia	alling	(c) Rainbow Table Attack	(d) Host File Attack
Q37 Ethical responsibilities of IT prof	essionals include	Q53 This technology is used to	determine and analyze human
	b) Minimizing cost	body uniqueness for authention	cation purpose.
	d) Minimizing testing	(a) Footprinting	(b) Biometric
,, <u> </u>	, 0	(c) JBOD	(d) Anthropomorphism

	In this type of DoS attack attac ping packets through ping com	nmand which result into	Q69 Poo	both (a) and (b) are correct orly designed social networking nerable to	sites are especially
	more traffic than the victim ca (a) Flood attack (c) SYN attack	n handle. (b) Ping of death attack (d) Smurf attack	(a)	Buffer overflow attack Non- Persistent cross-site scrip	(b) SQL injection attack
	It is a way of generating significan			Persistent cross-site scripting a	_
QJJ	on a victim network.	t computer network traine	Q70 A S	QL injection attack may be use	d to
	(a) Flood attack	(b) Ping of death attack	(a)	Change number of coloumns in	n a table
	(c) Teardrop attack	(d) Smurf attack	٠,	Read a row in a table	
	When the control of a web site	• •		Change coloumn name in a tak	ole
	is considered as			None of them	
	(a) Data Diddling	(b) Salami		e most effective remedy for SQ	-
	(c) Web theft	(d) Web Jacking		To filter HTML form input at th	
	This is installed between coputer a			To employ stored procedures	
	the log of keys pressed by user.	,		To employ prepared SQL state	
	(a) PC Key logger	(b) Software key logger		To perform input validation or	i the server via regular
		(d) None of them	expressi		J_
Q58	Consider the following represen	ntation and fill appropriate		ks performed by firewall include Access Control (b) Packet	
	keyword in the blank space conce	rning 'Trojan Horse'		IP address spoofing (d) All	t Integrity Checking
	Unlike Viruses ,they areprogr	rams		e role of a payment gateway is	
	(a) stand-alone	(b) variable		A proxy to the merchant	
	(c) harmless	(d) destructive		A proxy to the bankcard netwo	ork
Q59	Which among given is/are challen	ge(s) for any organization		A financial service provider	51 K
	(a) Employee wasted time on	internet		A government regulator	
	(b) Controlling Access to Web	Application		nich is the most interesting face	tor that motivates a hacker
	(c) Bandwidth Wastage			Financial gain	,
	(d) All of them			The thrill of hacking	
	In wireless network to scan the ne	etwork passively		To desire to identify vulnerabil	ities so they can be patched
	h technique(s) is used.	, ,		hey are publicaly exposed	
	(a) Scanning	(b) Spoofing	(d)	A religious/political/ideologica	l cause
	(c) Sniffing	(d) All of them	Q75 SM		
Q61	This in built feature of web brows	ers to warn about	(a)	DDoS	
	malicious sites by:		(b)	Trapdoor	
	(a) Anti-phishing filters in IE a	ind Firefox	(c)	antivirus	
	(b) Web of Trust		(d)	None of these	
	(c) Clearing history of browse	er		attack originating and/or atter	
	(d) Addlock Plus			er of an organization is	type of attack.
	is a social media co	omnuting allows	. ,	Active	(b) Inside
	ple to connect and share inf	-		Passive	(d) Outside
•	•			attacker usually installs the sr	liffers on the wireless
	(a) Facebook	(b) My Space (d) Twitter		and conduct activity such as:	//\
063	(c) Linkedin	· /		Detection of SSID	(b) Collecting MAC address
Q63	is not a cloud sphere. (a) Joint Sphere	(b) User Sphere		Collecting frame to crack WEP	
	(c) Recipient Sphere	(d) Client Sphere		Digital certificate is used to bind	
	Secret key cryptography is synoym			A person's public key to his pri	
QUT	(a) Symmetric Key Cryptography	iods with		A person's public key to his ide A person's private key to his id	-
	(b) Asymmetric key cryptography			A person's signature to his private key to his id	-
	(c) Private key cryptography			ich of the following attacks is/	
	(d) Quantum Cryptography			ntity theft?	are intery to result in
	To encypt a message from Aman t	to Alka using public key		Phishing attack	(b) Denial of Service attack
	cryptography, the following is nee			Virus Infection	(d) All
	(a) Aman's private key	(b) Aman's public key			neone use an application to
				vnich of the following does sor	
	(c) Alka's private key	(d) Alka's public key			
	(c) Alka's private key Which of the following protocols i	(d) Alka's public key s used in accessing web	cap	oture and manipulate packets a	
			сар уо	oture and manipulate packets a ur network?	s they are passing through
	Which of the following protocols i		сар уоч (a)	oture and manipulate packets a	s they are passing through (b) Backdoor
	Which of the following protocols i mail?	s used in accessing web	сар уоч (a)	oture and manipulate packets a ur network? DoS Man in Middle	s they are passing through
Q67	Which of the following protocols i mail? (a) SMTP (c) POP3 The buffer overflow attack is caus	s used in accessing web (b) HTTP (d) IMAP ed by	car you (a) (c) Q81	oture and manipulate packets a ur network? DoS Man in Middle	s they are passing through (b) Backdoor (d) Spoofing luence" people to obtain
	Which of the following protocols i mail? (a) SMTP (c) POP3 The buffer overflow attack is caus (a) A vulnerability in the design of	s used in accessing web (b) HTTP (d) IMAP ed by of a networking protocol	cap you (a) (c) Q81 the	oture and manipulate packets a ur network? DoS Man in Middle is a "technique to inf	s they are passing through (b) Backdoor (d) Spoofing luence" people to obtain
	Which of the following protocols i mail? (a) SMTP (c) POP3 The buffer overflow attack is caus (a) A vulnerability in the design of the company of the compa	s used in accessing web (b) HTTP (d) IMAP ed by of a networking protocol	cap you (a) (c) Q81 the (a) (c)	oture and manipulate packets a ur network? DoS Man in Middle is a "technique to inf e information or perform some Social Engineering Cyber stalking	(b) Backdoor (d) Spoofing luence" people to obtain action. (b) Phishing (d) None
	Which of the following protocols i mail? (a) SMTP (c) POP3 The buffer overflow attack is caus (a) A vulnerability in the design of the company of the protocol	s used in accessing web (b) HTTP (d) IMAP ed by of a networking protocol nentation of a networking	cap you (a) (c) Q81 the (a) (c) Q82 In t	oture and manipulate packets a ur network? DoS Man in Middle is a "technique to inf e information or perform some Social Engineering Cyber stalking his technique user tries to get	(b) Backdoor (d) Spoofing luence" people to obtain action. (b) Phishing (d) None the user disclose valuable
	Which of the following protocols i mail? (a) SMTP (c) POP3 The buffer overflow attack is caus: (a) A vulnerability in the design of the desig	s used in accessing web (b) HTTP (d) IMAP ed by of a networking protocol nentation of a networking	cap you (a) (c) Q81 the (a) (c) Q82 In t	oture and manipulate packets a ur network? DoS Man in Middle is a "technique to inf e information or perform some Social Engineering Cyber stalking his technique user tries to get	(b) Backdoor (d) Spoofing luence" people to obtain action. (b) Phishing (d) None the user disclose valuable numbers, password,
	Which of the following protocols i mail? (a) SMTP (c) POP3 The buffer overflow attack is caus (a) A vulnerability in the design of the design	s used in accessing web (b) HTTP (d) IMAP ed by of a networking protocol nentation of a networking aviour	cap you (a) (c) Q81	oture and manipulate packets a ur network? DoS Man in Middle is a "technique to information or perform some Social Engineering Cyber stalking his technique user tries to get resonal data- such as credit card count data and other information	(b) Backdoor (d) Spoofing luence" people to obtain action. (b) Phishing (d) None the user disclose valuable numbers, password,
	Which of the following protocols i mail? (a) SMTP (c) POP3 The buffer overflow attack is caus (a) A vulnerability in the design of the design	s used in accessing web (b) HTTP (d) IMAP ed by of a networking protocol nentation of a networking aviour	cap you (a) (c) Q81 the (a) (c) Q82 In t per acc	oture and manipulate packets a ur network? DOS Man in Middle is a "technique to information or perform some Social Engineering Cyber stalking his technique user tries to get rsonal data- such as credit card count data and other informationide it under false pretenses.	(b) Backdoor (d) Spoofing luence" people to obtain action. (b) Phishing (d) None the user disclose valuable numbers, password, on by convicting the user to
	Which of the following protocols i mail? (a) SMTP (c) POP3 The buffer overflow attack is caus (a) A vulnerability in the design of the company of the compa	s used in accessing web (b) HTTP (d) IMAP ed by of a networking protocol nentation of a networking aviour rding 'Virus'	cap you (a) (c) Q81	oture and manipulate packets a ur network? DOS Man in Middle is a "technique to information or perform some Social Engineering Cyber stalking his technique user tries to get resonal data- such as credit card count data and other informationide it under false pretenses. Phishing	(b) Backdoor (d) Spoofing luence" people to obtain action. (b) Phishing (d) None the user disclose valuable numbers, password, on by convicting the user to (b) Data Diddling
	Which of the following protocols i mail? (a) SMTP (c) POP3 The buffer overflow attack is caus (a) A vulnerability in the design of the design	s used in accessing web (b) HTTP (d) IMAP ed by of a networking protocol nentation of a networking aviour rding 'Virus'	cap you (a) (c) Q81	oture and manipulate packets a ur network? DOS Man in Middle is a "technique to information or perform some Social Engineering Cyber stalking his technique user tries to get rsonal data- such as credit card count data and other informationide it under false pretenses.	(b) Backdoor (d) Spoofing luence" people to obtain action. (b) Phishing (d) None the user disclose valuable numbers, password, on by convicting the user to

	(a) Social Engineering	(b) Phishing
	(c) Fraud	(d) Cyber Stalking
084	It involves harassing or threa	. , ,
Ψο.	individual will conduct repeated	_
	visiting a person's home and/or be	
	(a) Phishing	
	` '	(b) Social Engineering
	(c) Cyber Stalking	(d) None
Q85	Security risks from social engineer	_
	(a) Malware distribution	(b) Cyber bullying
	(c) Privacy concern	(d) All
Q86	Threats are categorized as:	
	(a) Passive or active	(b) Traffic
	(c) Masquerade	(d) Others
Q87	How are viruses spread?	. ,
	(a) Through Firewalls (b) Down	loading infected programs
	and files from internet.	iodding imeeted programs
	(c) Garbled information. (d) Install	anti-virus
000		
Ų88	A challenge relating to Cyber-	crimes is the conection
	of	
	(a) Electronic Evidence	
	(b) Paper Evidence	
	(c) Mechanical Evidence	
	(d) Hardware Evidence.	
Q89	is not a kind of cyber att	tack.
	(a) Cber Stalking	(b) Micro sites
	(c) Firewall attack	(d) E-Mail
nan	The latest WLAN standard is:	(a) E Ivian
Q90		/h) 902 11n
	(a) 802.11g	(b) 802.11n
004	(c) 802.12g	(d) 802.12n
Q91	The following is used when the so	urce code for a piece of
	software is unavailable	
	(a) Blackbox testing	(b) Whitebox testing
	(c) Regrssion testing	(d) Unit testing
Q92	Which of the following is/are true	of various forms of
mal	ware:	
	(a) A worm attaches itself to a fil	le or program
	(b) A Trojan is stand-alone progr	
	(c) A virus does not necessarily r	
	(d) All of the above	cpiloate
Q93	• •	used for ATM sards
Q93		
	(a) Symmetric	(b)Assymetric
	(c) Hashing	(d) None
	cipher takes one character	and replaces it with
anot	her.	
	(a) Stream	(b) Single
	(c) Substitution	(d) Hash
Q95	The purpose of digital signatue is/	are
	(a) Verify Sender (b)Prove	Integrity of message
	(c) Prevent sender from disowing	the message
	(d) All	G
Q96	is the science of trans	forming information into a
-	re form so that unauthorized users	_
3000	(a) Steganography	(b) Cryptography
	(c) Neither a nor b	
007	• •	(d) Both a and b
Q97	A victim unknowingly downloads a	a Trojan norse virus is a
	type of crime.	
	(a) Type 1 Cyber crime	(b) Type 2 Cyber crime
	 ,.	(b) Type 2 Cyber crime (d) Type 4 Cyber crime
Q98	(a) Type 1 Cyber crime	(d) Type 4 Cyber crime
Q98	(a) Type 1 Cyber crime (c) Type 3 Cyber crime	(d) Type 4 Cyber crime
Q98	(a) Type 1 Cyber crime (c) Type 3 Cyber crime Survival mantra for netizens is are	(d) Type 4 Cyber crime
Q98	(a) Type 1 Cyber crime (c) Type 3 Cyber crime Survival mantra for netizens is are (a) Keep genuine software (b) keep browsers updated with	(d) Type 4 Cyber crime : security patches
Q98	(a) Type 1 Cyber crime (c) Type 3 Cyber crime Survival mantra for netizens is are (a) Keep genuine software (b) keep browsers updated with (c) Keep an effective Antivirus an	(d) Type 4 Cyber crime : security patches
	(a) Type 1 Cyber crime (c) Type 3 Cyber crime Survival mantra for netizens is are (a) Keep genuine software (b) keep browsers updated with (c) Keep an effective Antivirus an (d) All of them	(d) Type 4 Cyber crime : security patches nd updates
	(a) Type 1 Cyber crime (c) Type 3 Cyber crime Survival mantra for netizens is are (a) Keep genuine software (b) keep browsers updated with (c) Keep an effective Antivirus ar (d) All of them This process involves changing cor	(d) Type 4 Cyber crime : security patches nd updates ntents of a website
	(a) Type 1 Cyber crime (c) Type 3 Cyber crime Survival mantra for netizens is are (a) Keep genuine software (b) keep browsers updated with (c) Keep an effective Antivirus ar (d) All of them This process involves changing cordepending upon a user's IP address	(d) Type 4 Cyber crime : security patches nd updates ntents of a website ss and geographical location
	(a) Type 1 Cyber crime (c) Type 3 Cyber crime Survival mantra for netizens is are (a) Keep genuine software (b) keep browsers updated with (c) Keep an effective Antivirus ar (d) All of them This process involves changing cordepending upon a user's IP addres (a) IP Base Clocking	(d) Type 4 Cyber crime : security patches nd updates ntents of a website ss and geographical location (b) IP Base Blocking
Q99	(a) Type 1 Cyber crime (c) Type 3 Cyber crime Survival mantra for netizens is are (a) Keep genuine software (b) keep browsers updated with (c) Keep an effective Antivirus ar (d) All of them This process involves changing cordepending upon a user's IP address	(d) Type 4 Cyber crime : security patches nd updates ntents of a website ss and geographical location (b) IP Base Blocking (d) None of them

looking for a computer on the other end.

(a) Dialler

(c) Self dialler

(b) Auto dialler

(d) War dialler