Estd. 1962
NAAC 'A' Grade

SHIVAJI UNIVERISTY, KOLHAPUR-416 004. MAHARASHTRA
PHONE : EPABX-2609000 **website- www.unishivaji.ac.in**
FAX 0091-0231-2691533 & 0091-0231-2692333 – BOS - 2609094
शिवाजी विद्यापीठ, कोल्हापूर – 416004.
दुरध्वनी (ईपीएबीएक्स) २६०९००० (अभ्यास मंडळे विभाग— २६०९०९४)
फॅक्स : ००९१-०२३१-२६९१५३३ व २६९२३३३.e-mail:bos@unishivaji.ac.in

SU/BOS/Science & Tech./ No 0822 Date:- 17 MAR 2020

To,

Head of the Department, All Science Departments, Shivaji University, Kolhapur.	The Principle, All Affiliated Science (M.Sc.) Colleges/Institutes Shivaji University, Kolhapur.

Subject: Regarding Syllabus, Qusetion Bank of SEC-I (Skill Enhancement Course) Non CGPA Paper-I M. Sc. Part I Sem-II under Faculty of Science and Technology.

Sir/Madam,

With reference to the subject mentioned above, I am directed to inform you that the University authorities have accepted and granted approval to the Syllabus, Qusetion Bank of ~~of~~ M.Sc.Part- I Sem-II SEC-I (Non CGPA) Fundamental of Infrormation Technology: Information Secureity, under Faculty of Science and Technology.

It shall be implemented from the second Term of academic year 2019-20. A soft copy containing Syllabus, Nature of Qusetion Paper and Qusetion Bank is enclosed herewith, and also made available on university website **www.unishivaji.ac.in. (Online syllabus)**

You are therefore requested to bring this to the notice of all Students and Teachers concerned.

Thanking you,

Yours faithfully,

Dy Registrar

Copy to:

1)	I/c Dean, Faculty of Science and Technology	7)	B. Sc./ M. Sc. Exam Section
2)	Director, Board of Examinations & Evaluation	8)	IT Cell
3)	Chairman, All BOS and Ad-hoc board	9)	P.G.Admission
4)	Appointment Section	10)	P.G.Seminar.
5)	Affilation Section T-1/T-2	11)	Director, Centre for Distance Education
6)	Eligibility Section		

Skill Enhancement Course [SEC-I] Non-CGPA

Lectures per Week: 02

Hours per week: 02 Credit: 02

Course Outcomes:

1. To inculcate awareness of Information security among students.

2. Acquaintance with basic terminology of security

3. Develop a basic understanding of Internet security, Digital certificates, Browser security.

4. Develop an understanding of online transaction and email security.

SEC I- Fundamental of Information Technology: Information Security		**30Hrs**
Unit: I	Fundamentals of Security Basic terms, Computer security, elements of security, vulnerability of computer, Threats to system security, Antivirus: Types, need of antivirus and functions,	10Hrs.
Unit: II	Internet security Data Security:Data encryption, Digital certificates, Digital Signature Browser security, Child online security, Internet security laws	10Hrs.
Unit: III	Online transaction security Introduction, working of online transaction, Payment gateway, Threats and security. Email security	10 Hrs.

Skill Enhancement Course [SEC-II] Non-CGPA

Lectures per Week: 02

Hours per week: 02Credit: 02

Course outcomes:

1. To inculcate awareness of Cyber security among students.

2. Students to have firm understanding on secure email communication.

3. Exposure to Identity thefts and techniques to countermeasure the same.

4. Know the legal compliances of Information security.

SEC II- Fundamental of Information Technology: Cyber security		**30Hrs**
Unit: I	Secure email communication: Introduction, Architecture, threats, Digital certificates, security methods and tools	10Hrs.
Unit: II	Social engineering: Introduction, types, introduction to Identity theft, causes and after effects, techniques to countermeasure Social Engineering and Identity theft.	10Hrs.
Unit: III	Information security and legal Compliance: Introduction, HIPPA, FERPA, PCI DSS	10 Hrs.

Nature of Question Paper Pattern

- **25 multiple choice questions with four alternatives.**

Question Paper Pattern

M.Sc. I SEC-I Fundamental of Information Technology: Information Security

Skill Enhancement Course - I

Time Allotted: 1:00 hrs Total Marks: 50

Instructions

- All questions are compulsory.
- Each question carries 2 marks
- Tick correct option.

Q1. Twenty Five multiple choice questions with four alternatives.

Nature of Question Paper Pattern

M.Sc. II SEC-II Fundamental of Information Technology: Cyber security

Skill Enhancement Course- II

Time Allotted: 1.00 hrs Total Marks: 50

Instructions

- All questions are compulsory.
- Each question carries 2 marks.
- Tick correct option

Q1. Twenty Five multiple choice questions with four alternatives.

M.Sc. (CBCS)

SEC I- Fundamental of Information Technology: Information Security

Unit-I: Fundamentals of Security

Question Bank

Que. 1. Rewrite the following questions choosing the correct alternative:

1) The first computer virus is ----------------

a) Sasser b) Creeper

c) Blaster d) I Love You

2) To protect a computer from virus, you should install -------- in your computer

a) antivirus b) disk defragmenter

c) disk cleanup d) backup wizard

3) Which of the following is known as Malicious software?

a) maliciousware b) illegalware

c) badware d) malware

4)MCAfe is an example of

a) virus b) quick heal

c) antivirus d) photo editor

5)A ------- is a computer program that can invade computer and perform a variety of functions ranging from annoying(e.g. popping up messages as a joke) to dangerous (e.g. deleting files)

a) computer virus b) antivirus

c) Ms word d) ms Access

6) When a logic bomb is activated by a time related event, it is known as -----

a) trosen horse b) time bomb

c) virus d) time related bomb sequence

7)------- are often delivered to a PC through an email attachment and are often designed to do harm.

a) virus b) email

c) portal d) spam

8) VIRUS stands for

a) Very Intelligent Result Until Source b) Vital Information Resource Under Siege

c) Viral Important Record User Searched d) Very Interchanged Resource Under Search

9) What is short for malicious software (is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems)?

a) Malisoft b) Malairasoft

c) Moleculewar d) Malware

10) A virus that migrates freely within a large population of unauthorized email user is called a ------

a) macro b) flame war

c) plagiarism d) worm

11) -------- are attempts by individuals to obtain confidential information from you to falsifying their identity.

a) Phishing scams b) Phishing trips

c) Spyware scams d) Computer viruses

12) Authentication is

a) hard to assure identity of user on a remote system. b) insertion.

c) modification d) none of above

13) A -------- is a computer program that can replicate itself and spread from one computer to another.

a) PenDrive b) Computer Virus

c) Mouse d) Antivurs

14)Which of the following virus overtake computer system, when it boots and destroy information?

a) Stealth virus b) Trojan

c) Boot infectors d) System infectors

15) Key logger is a

a) Antivirus b) Spyware

c) Firmware d) All of the above

16) To protect yourself from computer hacker, you should turn on a

a) Firewall b) Script

c) Antivirus d) VLC

17) Firewalls are used to protect against --------

a) virus attacks b) fire attacks

c) unauthorised access d) data driven attacks

18) Which of the following describes programs that can run independently travel from system to system and disrupt computer communication?

a) Viruses b) Worm

c) Trojans d) Droppers

19) Code red is a(n) ----------

a) Word Processing Software b) Photo Editing Software

c) Antivirus d) Virus

20) Which of the following would most likely not be a symptom of a virus?

a) Existing program files and icons disappear

b) The CD–ROM stops functioning

c) The web browser opens to an unusual home page

d) Odd message or images are displayed on the screen

21)…………….. are used in denial of service attacks, typically against targeted web sites.

a) Trojan horse b) Zombie

c) Worm d) Virus

22) …………………….. is a form of virus explicitly designed to hide itself from detection by antivirus software.

a) Macro Virus b) Parasitic Virus

c) Stealth virus d) Polymorphic Virus

23) The type(s) of auto executing macros, in Microsoft word is/are

a) Command macro b) Auto macro

c) Auto execute d) All of the above

24) A ……………… is a program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks.

a) Trap doors b) Zombie

c) Virus d) Worm

25) What is a firewall?

a) A program that protects against viruses.

b) A wall that is reinforced and cannot catch on fire.

c) A filter for an internet connection that monitors outgoing and incoming activity

d) None

26) In general how many key elements constitute the entire security structure?

a) 1 b) 2

c) 3 d) 4

27) When you use the word _____ it means you are protecting your data from getting disclosed.

a) Confidentiality b) Integrity

c) Authentication d) Availability

28) When integrity is lacking in a security system, _________ occurs.

a) Database hacking b) Data deletion

c) Data tampering d) Data leakage

29) One common way to maintain data availability is __________

a) Data clustering b) Data backup

c) Data recovery d) Data Altering

30) This is an attack on a computer system that takes advantage of a particular vulnerability that the system offers to intruders.

a) port scan b) denial of service

c) exploit d) logic bomb

31) This is a type of network security attack in which the intruder takes control of a communication between two entities and masquerades as one of them.

a) hijacking b) identity theft

c) smurf attack d) tunneling

32) This is a compromised Web site that is being used as an attack launch point in a denial-of-service attack.

a) bastion host b) packet monkey

c) dongle d) zombie

33) ___________ is a weakness that can be exploited by attackers.

a) System with Virus b) System without firewall

c) System with vulnerabilities d) System with strong password

34) A/An __________ is a piece of software or a segment of command that usually take advantage of a bug to cause unintended actions and behaviors.

a) malware b) trojan

c) worms d) exploit

35) ___________ is a technique used by penetration testers to compromise any system within a network for targeting other systems.

a) Exploiting b) Cracking

c) Hacking d) Pivoting

36) A _________ is a software bug that attackers can take advantage to gain unauthorized access in a system.

a) System error b) Bugged system

c) Security bug d) System virus

37) Security bugs are also known as _______

a) security defect b) security problems

c) system defect d) software error

38) Which of the following is not session layer vulnerability?

a) Mishandling of undefined, poorly defined

b) Spoofing and hijacking of data based on failed authentication attempts

c) Passing of session-credentials allowing intercept and unauthorized use

d) Weak or non-existent authentication mechanisms

39)Which of the following is not an example of presentation layer issues?

a) Poor handling of unexpected input can lead to the execution of arbitrary instructions

b) Unintentional or ill-directed use of superficially supplied input

c) Cryptographic flaws in the system may get exploited to evade privacy

d) Weak or non-existent authentication mechanisms

40) Which of the following is an example of Transport layer vulnerability?

a) weak or non-existent mechanisms for authentication

b) overloading of transport-layer mechanisms

c) poor handling of unexpected input

d) highly complex application security controls

41) Which of the following is an example of session layer vulnerability?

a) Weak or non-existent mechanisms for authentication

b) overloading of transport-layer mechanisms

c) poor handling of unexpected input

d) highly complex application security controls

42) Which of the following is an example of presentation layer vulnerability?

a) weak or non-existent mechanisms for authentication

b) overloading of transport-layer mechanisms

c) highly complex application security controls

d) poor handling of unexpected input

43) Possible threat to any information cannot be ________________

a) reduced b) transferred

c) protected d) ignored

44) Lack of access control policy is a _____________

a) Bug b) Threat

c) Vulnerability d) Attack

45)From the options below, which of them is not a vulnerability to information security?

a) flood b) without deleting data, disposal of storage media

c) unchanged default password d) latest patches and updates not done

46) Which of the following information security technology is used for avoiding browser-based hacking?

a) Anti-malware in browsers b) Remote browser access

c) Adware remover in browsers d) Incognito mode in a browser

47) Viruses which executes when computer starts is

a) Macro b) file infector

c) boot sector d) salami shaving

48) Special program which can detect and remove viruses from computer is called

a) virus b) antivirus

c)boot sector d)salami shaving

49) Example of computer antivirus program includes

a) Norton b) McAfee

c) Dr.Solomon toolkit d) all of these

50) The DES algorithm has a key length of

a) 128 Bits b) 32 Bits

c) 64 Bits d) 16 Bits

Answers:

Unit-I: Fundamentals of Security

Q. No.	Answer
1	b) Creeper
2	a) antivirus
3	a) maliciousware
4	c) antivirus
5	a) computer virus
6	b) time bomb
7	a) virus
8	b) Vital Information Resource Under Siege
9	d) Malware
10	a) macro
11	a) Phishing scams
12	a) hard to assure identity of user on a remote system.
13	b) Computer Virus
14	a) Stealth virus
15	b) Spyware
16	a) Firewall
17	c) unauthorised access
18	b) Worm
19	d) Virus
20	b) The CD–ROM stops functioning
21	b) Zombie
22	c) Stealth virus
23	d) All of the above
24	b) Zombie
25	c) A filter for an internet connection that monitors outgoing and incoming activity

26	d) 4
27	a) Confidentiality
28	c) Data tampering
29	b) Data backup
30	c) exploit
31	a) hijacking
32	d) zombie
33	c) System with vulnerabilities
34	d) exploit
35	d) Pivoting
36	c) Security bug
37	a) security defect
38	a) Mishandling of undefined, poorly defined
39	d) Weak or non-existent authentication mechanisms
40	b) overloading of transport-layer mechanisms
41	b) overloading of transport-layer mechanisms
42	d) poor handling of unexpected input
43	d) ignored
44	c) Vulnerability
45	a) flood
46	b) Remote browser access
47	c) boot sector
48	b) antivirus
49	d) all of these
50	c) 64 Bits

Unit-II: Internet Security

Question Bank

1) The DES Algorithm Cipher System consists of ____________rounds (iterations) each with a round key

a) 12 b) 18

c) 9 d) 16

2) In asymmetric key cryptography, the private key is kept by

a) sender b) receiver

c) sender and receiver d) all the connected devices to the network

3) In cryptography, the order of the letters in a message is rearranged by

a) transpositional ciphers

b) substitution ciphers

c) both transpositional ciphers and substitution ciphers

d) none of the mentioned

4) Cryptanalysis is used

a) to find some insecurity in a cryptographic scheme

b) to increase the speed

c) to encrypt the data

d) none of the mention

5) Cryptographic hash function takes an arbitrary block of data and returns

a) fixed size bit string

b) variable size bit string

c) both fixed size bit string and variable size bit string

d) none of the mentioned

6) Input message in Cryptography is called;

a) Plain text b) Cipher Text

c) Plain and cipher d) None of the above ( )

7) Asymmetric key is also called:

a) Secret key b) Public key

c) Private key d) None of the above

8) RSA stands for:

a) Rivest Shamir and Adleman b) Rock Shane and Amozen

c) Rivest Shane and Amozen d) Rock Shamir and Adleman

9) A digital signature need a :

a) Public key system b) Private key system

c) Public and private key system d) None of the above

10) Which layer filters the proxy firewall?

a) Application b) Transport layer

c) Network Layer d) None of the above

11) Secure Hash function or algorithm developed by:

a) NIST b) IEEE

c) ANSI d) None of the above

12).......................is an encryption method used to offer secure communication by e- mail:

a) Mail server b) PGP

c) SSL d) None of the above

13) Network security ensures:

a) Detecting attacks b) Preventing attacks

c) Recovering attacks d) All of the above

14) The process to discover plain text or key is known as:

a) Cryptanalysis b) Crypto design

c) Crypto processing d) Crypto graphic

15) Hacking refers to:

a) Data access without permission b) Data updation without permission

c) Data deletion without permission d) All of the above.

16) Encryption protects against:

a) Attacks b) Viruses

c) Manipulation of data d) All of the above

17) Hash function is used to produce:

a) Finger print of a file b) Useful for message authentication

c) Both a and b d) None of the above

18) Block cipher processes:

a) 1000 bits at a time b) One bit block of data at a time

c) Both a and b d) None of the above

19) Decryption algorithm:

a) Encrypts input data b) Decrypts the encrypted data

c) Both a and b d) None of the above

20) What is the name of the network attack that floods it with useless traffic?

a) Virus b) Trojan horse

c) DOS attach d) Spoofing

21) RSA algorithm uses variable sized key that is usually between........and bits.

a) 256, 1048 b) 256, 2048

c) 512, 1048 d) 512, 2048

22) What is an advantage of DSS overRSA?

a) It can provide faster digital signature

b) It uses fewer resources and encrypts quicker because it uses symmetric keys

c) It is a block cipher versus a stream cipher

d) It employs a one-time encryption pad

23) The codified language can be termed as:

a) Clear text b) Unclear text

c) Code text d) Cipher text

24) Cryptology means:

a) Cryptology+ Crypto design

b) Cryptology Cryptanalysis

c) Cryptograph itself known as cryptology also

d) None of the above

25) The input block length in AES is:

a) 56 bits b) 64 bits

c) 112 bits d) 128 bits

26) An attack on a cipher text message where the attacker attempts to use all possible Permutations and combinations is called:

a) Brute-Plaintext attack b) Birthday attack

c) Known-Plaintext attack d) Chosen-plaintext attack

27) Hash collision means:

a) Two keys for one message

b) One key for two message

c) Two different keys for different message

d) Always the same key

28) Encryption strength is based on:

a) Strength of algorithm b) Secrecy of key

c) Length of key d) All of the above

29) In an authentication using symmetric keys, if 10 people need to communicate, we need................ Keys.

a) 10 b) 20

c) 30 d) 45

30) In an efficient algorithm for factoring large number is discovered, which of the Following schemes will be known to be not secure?

a) Diffle-Hellman b) RSA

c) AES d) None of the above

31) Session Key establishes:

a) Logical connection b) Physical Connection

c) Both a and b d) None of the above

32) In the digital signature technique, the sender of the message uses.................to create cipher text:

a) Own symmetric key b) Own private key

c) The receiver's private key d) Receiver's public key ( )

33) The symmetric (Shared) key in the Diffle-Hellman protocol is:

a) k = g xy and p b) K = g xy mod q

c) K = (R2)x d) All of the above

34) Secure socket layer is designed to provide, security and compression services to data Granted from................

a) Application Layer b) Transport Layer

c) Both a) and b) d) None of the above

35) Which of the following is not type of permutation in P-boxes?

a) Plain permutation b) Straight permutation

c) Expansion permutation d) Compression permutation

36) Which of the following is not type of permutation in P-boxes?

a) Plain permutation b) Straight permutation

c) Expansion permutation d) Compression permutation

37) SHA-1 is similar to:

a) RSA b) DES

c) MD5 d) Rijndael

38) Kerberos is an authentication scheme that can used to implement:

a) Public key cryptography b) Digital signature

c) Hash function d) Single sign on

39) Transposition cipher involves:

a) Replacement of blocks of text with other blocks

b) Replacement of characters of text with other character

c) Strict row to column replacement

d) Some permutation on the input text to produce cipher text

40) Which of the following is not a block cipher operating mode?

a) ECB b) CBF

c) OFB d) CBC

41) If an efficient algorithm for factoring large number is discovered which of this Following schemes will be known to be not secure?

a) AES b) Diffle-Hellman

c) RSA d) EI Gammal

42) What are MD4 and MD5?

a) Symmetric Encryption Algorithms b) Asymmetric encryption Algorithms

c) Hashing algorithms d) Digital certificates

43) TDES means:

a) Triple digital encryption standard b) Triangular data encryption standard

c) Triple data encryption standard d) Triangular digital encryption standard

44) If an attacker stole a password file that contained one way encrypted passwords, what type of an attack would he/she perform to find the encrypted password?

a) Man- in-the middle attack b) Birthday attack

c) Denial of service attack d) Dictionary attack

45) Masquerade attack is another name of:

a) Virus attack b) Spoofing

c) DOS attack d) Trojan Horse

46) Which of the following is not a type of cyber crime?

a) Data theft b) Forgery

c) Damage to data and system d) Installing antivirus for protection

47) What is the name of the IT law that India is having in the Indian legislature?

a) India's Technology (IT) Act, 2000

b) India's Digital Information Technology (DIT) Act, 2000

c) India's Information Technology (IT) Act, 2000

d) The Technology Act, 2008

48) In which year India's IT Act came into existence?

a)2000 b) 2001

c) 2002 d) 2003

49) What is the full form of ITA-2000?

a) Information Tech Act -2000 b) Indian Technology Act -2000

c) International Technology Act -2000 d) Information Technology Act -2000

50) What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds?

a) Cracking or illegally hack into any system

b) Putting antivirus into the victim

c) Stealing data

d) Stealing hardware components

51) Which of the following information security technology is used for avoiding browser-based hacking?

a) Anti-malware in browsers b) Remote browser access

c) Adware remover in browsers d) Incognito mode in a browser

52) Attempting to gain access to a network using an employee's credentials is called the _____________ mode of ethical hacking.

a) Local networking b) Social engineering

c) Physical entry d) Remote networking

53)What are the types of scanning?

a) Port, network, and services b) Network, vulnerability, and port

c) Passive, active, and interactive d) Server, client, and network

54) Why would HTTP Tunneling be used?

a) To identify proxy servers b) Web activity is not scanned

c) To bypass a firewall d) HTTP is a easy protocol to work with

55) Why would a hacker use a proxy server?

a) To create a stronger connection with the target.

b) To create a ghost server on the network.

c) To obtain a remote access connection.

d) To hide malicious activity on the network.

Answers:

Unit-II: Internet Security

Q. No.	Answer
1	d) 16
2	b) receiver
3	a) transpositional ciphers
4	a) to find some insecurity in a cryptographic scheme
5	a) fixed size bit string
6	a) Plain text
7	b) Public key
8	a) Rivest Shamir and Adleman
9	a) Public key system
10	a) Application
11	a) NIST
12	b) PGP
13	d) All of the above
14	a) Cryptanalysis
15	a) Data access without permission
16	a) Attacks
17	b) Useful for message authentication
18	d) None of the above
19	b) Decrypts the encrypted data
20	c) DOS attach
21	a) 256, 1048
22	a) It can provide faster digital signature
23	d) Cipher text
24	c) Cryptograph itself known as cryptology also
25	d) 128 bits

26	a) Brute-Plaintext attack
27	b) One key for two message
28	b) Secrecy of key
29	d) 45
30	b) RSA
31	a) Logical connection
32	b) Own private key
33	b) K = g xy mod q
34	a) Application Layer
35	a) Plain permutation
36	a) Plain permutation
37	c) MD5
38	b) Digital signature
39	d) Some permutation on the input text to produce cipher text
40	b) CBF
41	c) RSA
42	c) Hashing algorithms
43	c) Triple data encryption standard
44	d) Dictionary attack
45	b) Spoofing
46	d) Installing antivirus for protection
47	c) India’s Information Technology (IT) Act, 2000
48	a)2000
49	d) Information Technology Act -2000
50	a) Cracking or illegally hack into any system
51	b) Remote browser access
52	a) Local networking
53	b) Network, vulnerability, and port
54	c) To bypass a firewall
55	d) To hide malicious activity on the network.

Unit-III: Online Transaction Security

Question Bank

1) Which is form of electronic cash ?

a) Credit card b) digital cash

c) net banking transfer d) debit card

2) …………..option lets the buyer pay when he/she receives the product

a) Credit card b) digital cash

c) net banking transfer d) cash on delivery

3)……………………is a payment method in which the transfer of fund or money happens online over electronic fund transfer.

a) OLTP b) cash on delivery

c) cheque d) none

4)…………………protocol uses different encryption and hashing techniques to secure payments over internet done through credit cards.

a) SET b) AODV

c) HTTP d) All of above

5)Payment Gateway also helps you to accept………………………

a) credit card and electronics checks b) debit card

c) error correction d) none of these

6) virtual terminal is basically used for-------------------

a) manual credit transaction b) shopping cart

c) access data from remote server d) none

7)what is e-commerce?

a) it refers to the use of the computer network

b) it refers to the idea of extracting business intelligence

c) both a and c

d) it refers to the buying and selling of goods and services

8) In which of the following, personal digital assistants (PDAs) are used for buying and selling of goods and services?

a) E-commerce b) M-commerce

c) V-commerce d) All of the above

9)____________ is the method for keeping sensitive information in email communication & accounts secure against unofficial access, loss, or compromise.

a) Email security b) Email hacking

c) Email protection d) Email safeguarding

10) Which of them is not a major way of stealing email information?

a) Stealing cookies b) reverse Engineering

c) Password Phishing d) Social Engineering

11)_____________ is a famous technological medium for the spread of malware, facing problems of spam, & phishing attacks.

a) Cloud b) Pen drive

c) Website d) Email

12)which of them is not a proper method for email security?

a) Use Strong password b) Use email Encryption

c) Spam filters and malware scanners d) click on unknown links to explore

13)which of them is an example of grabbing email information?

a) Cookie stealing b) Reverse engineering

c) Port scanning d) Banner grabbing

14) Using email hacking illicit hackers can send & spread ___________ virus _____________ and spam emails.

a) trojans, redirected malicious URLs b) antivirus, patches

c) cracked software, redirected malicious URLs d) malware, security patches

15) Fraudulent email messages are some fake email messages that seem legitimate which asks for your confidential bank details such as _____________ details _________ and passwords.

a) credit card, antivirus name b) credit card, login ID

c) cell phone, antivirus name d) car model, account

16) Unsolicited Bulk E-mails (UBI) are called __________

a) SMS b) MMS

c) Spam emails d) Malicious emails

Answers:

Unit-III: Online Transaction Security

Q. No.	Answer
1	b) digital cash
2	d) cash on delivery
3	a) OLTP
4	a) SET
5	a) credit card and electronics checks
6	a) manual credit transaction
7	d) it refers to the buying and selling of goods and services
8	b) M-commerce
9	a) Email security
10	b) reverse Engineering
11	d) Email
12	d) click on unknown links to explore
13	a) Cookie stealing
14	a) trojans, redirected malicious URLs

15	b) credit card, login ID
16	c) Spam emails

SEC II- Fundamental of Information Technology: Cyber security

Unit-I: Secure email communication

Question Bank

1) Which of the following is not a strong security protocol?

   a) HTTPS b) SSL

   c) SMTP d) SFTP

2) ___________ ensures the integrity and security of data that are passing over a network.

   a) Firewall b) Antivirus

   c) Pen testing Tools d) Network-security protocols

3) Which of the following is not a secured mail transferring methodology?

   a) POP3 b) SSMTP

   c) Mail using PGP d) S/MIME

4) __________ is a set of conventions & rules set for communicating two or more devices residing in the same network?

   a) Security policies b) Protocols

   c) Wireless network d) Network algorithms

5) HTTPS is abbreviated as _________

   a) Hypertexts Transfer Protocol Secured

   b) Secured Hyper Text Transfer Protocol

   c) Hyperlinked Text Transfer Protocol Secured

   d) Hyper Text Transfer Protocol Secure

6) SSL primarily focuses on _______

   a) integrity and authenticity b) integrity and non-repudiation

   c) authenticity and privacy d) confidentiality and integrity

7) In SSL, what is used for authenticating a message?

a) MAC (Message Access Code) b) MAC (Message Authentication Code)

c) MAC (Machine Authentication Code) d) MAC (Machine Access Code)

8) __________ is used for encrypting data at network level.

a) IPSec b) HTTPS

c) SMTP d) S/MIME

9) S/MIME is abbreviated as __________________

a) Secure/Multimedia Internet Mailing Extensions

b) Secure/Multipurpose Internet Mailing Extensions

c) Secure/Multimedia Internet Mail Extensions

d) Secure/Multipurpose Internet Mail Extensions

10) Users are able to see a pad-lock icon in the address bar of the browser when there is _______ connection.

a) HTTP b) HTTPS

c) SMTP d) SFTP

11) Why did SSL certificate require in HTTP?

a) For making security weak

b) For making information move faster

c) For encrypted data sent over HTTP protocol

d) For sending and receiving emails unencrypted

12) SFTP is abbreviated as ________

a) Secure File Transfer Protocol b) Secured File Transfer Protocol

c) Secure Folder Transfer Protocol d) Secure File Transferring Protocol

13) PCT is abbreviated as ________

a) Private Connecting Technology b) Personal Communication Technology

c) Private Communication Technique d) Private Communication Technology

14) In architecture of e-mail, we can have

a)2 Scenarios b) 3 Scenarios

c) 4 Scenarios d) 6 Scenarios

15) MIME stands for

a) Multipurpose Internet Mail Extensions

b) Multipurpose Internet Mail Email

c) Multipurpose International Mail Entity

d) Multipurpose International Mail End

16) Mail access starts with client when user needs to download e-mail from the

a)Mail Box b) Mail Server

c) Mail Host d) Internet

17) When sender and receiver of an e-mail are on same system, we need only two

a)IP b) Domain

a) Servers d) User Agents

18) _____________ is a famous technological medium for the spread of malware, facing problems of spam, & phishing attacks.

a) Cloud b) Pen drive

c) Website d) Email

19) Which of them is not a proper method for email security?

a) Use Strong password b) Use email Encryption

c) Spam filters and malware scanners d) Click on unknown links to explore

20) The stored cookie which contains all your personal data about that website can be stolen away by _____________ using _____________ or trojans.

a) attackers, malware b) hackers, antivirus

c) penetration testers, malware d) penetration testers, virus

21) Unsolicited Bulk E-mails (UBI) are called __________

a) SMS　　b) MMS

c) Spam emails　　d) Malicious emails

22) Which of these systems use timestamps as an expiration date?

a) Public-Key Certificates　　b) Public announcements

c) Publicly available directories　　d) Public-Key authority

23) Which system uses a trusted third party interface?

a) Public-Key Certificates　　b) Public announcements

c) Publicly available directories　　d) Public-Key authority

24) It is desirable to revoke a certificate before it expires because

a) the user is no longer certified by this CA

b) the CA's certificate is assumed to be compromised

c) the user's private key is assumed to be compromised

d) all of the mentioned

25) CRL stands for

a) Cipher Reusable List　　b) Certificate Revocation Language

c) Certificate Revocation List　　d) Certificate Resolution Language

26) Which of the following is not a part of an Extension?

a) Extension Identifier　　b) Extension value

c) Criticality Indicator　　d) All of the mentioned constitute the Extension

27) Which of the following attach is not used by LC4 to recover Windows password?

a) Brute-force attack　　b) Dictionary attack

c) MiTM attack　　d) Hybrid attacks

28) ____________is the world’s most popular vulnerability scanner used in companies for checking vulnerabilities in the network.

a) Wireshark b) Nessus

c) Snort d) WebInspect

29) _____________ is a tool which can detect registry issues in an operating system.

a) Network Stumbler b) Ettercap

c) Maltego d) LANguard Network Security Scanner

30) ToneLoc is abbreviated as __________

a) Tone Locking b) Tone Locator

c) Tone Locker d) Tune Locator

31) __________ is a debugger and exploration tool.

a) Netdog b) Netcat

c) Tcpdump d) BackTrack

32) All of the following are example of real security and privacy threats excepts :

a) Hackers c) Virus

b) Spam d) Worm

33) __________ is a popular command-line packet analyser.

a) Wireshark b) Snort

c) Metasploit d) Tcpdump

34) ________________ is a platform that essentially keeps the log of data from networks, devices as well as applications in a single location.

a) EventLog Analyser b) NordVPN

c) Wireshark d) PacketFilter Analyzer

35) ______________ is competent to restore corrupted Exchange Server Database files as well as recovering unapproachable mails in mailboxes.

a) Outlook b) Nessus

c) Mailbox Exchange Recovery d) Mail Exchange Recovery toolkit

36) ________________ helps in protecting businesses against data breaches that may make threats to cloud.

a) Centrify b) Mailbox Exchange Recovery

c) Nessus d) Dashline

37) __________ is a popular corporate security tool that is used to detect the attack on email with cloud only services.

a) Cain and Abel b) Proofpoint

c) Angry IP Scanner d) Ettercap

38) _____________ helps in protecting corporate data, communications and other assets.

a) Snort b) Cipher Cloud

c) Burp Suit d) Wireshark

39) Threats are categorized as:

a)Passive or active b) Traffic

c) Masquerade d) Others

40(Interruption affects

a)availability b)

a) integrity

c) authenticity d) none of the above

41) which of the following program is used by a user to send and receives emails?

a) Mail transfer agent c) Mail delivery agent

b) Mail user agent d) Mail reading agent

42) There are _______ major ways of stealing email information.

a) 2 b) 3

c) 4 d) 5

43) Which of them is not a major way of stealing email information?

a) Stealing cookies b) Reverse Engineering

c) Password Phishing d) Social Engineering

44) Using email hacking illicit hackers can send & spread ___________ virus _____________ and spam emails.

a) trojans, redirected malicious URLs

b) antivirus, patches

c) cracked software, redirected malicious URLs

d) malware, security patches

45) _______________ needs to be turned off in order to prevent from this attack.

a) Email scripting b) Email attachments

c) Email services d) Third party email programs

Answers:

Unit-I: Secure email communication

Q. No.	Answer
1	c) SMTP
2	d) Network-security protocols
3	a) POP3
4	b) Protocols
5	d) Hyper Text Transfer Protocol Secure
6	a) integrity and authenticity
7	b) MAC (Message Authentication Code)
8	a) IPSec
9	d) Secure/Multipurpose Internet Mail Extensions

10	b) HTTPS
11	c) For encrypted data sent over HTTP protocol
12	a) Secure File Transfer Protocol
13	d) Private Communication Technology
14	d) 6 Scenarios
15	a)Multipurpose Internet Mail Extensions
16	a)Mail Box
17	d) User Agents
18	d) Email
19	d) Click on unknown links to explore
20	a) attackers, malware
21	c) Spam emails
22	a) Public-Key Certificates
23	a) Public-Key Certificates
24	d) all of the mentioned
25	d) Certificate Resolution Language
26	d) All of the mentioned constitute the Extension
27	c) MiTM attack
28	b) Nessus
29	d) LANguard Network Security Scanner
30	c) Tone Locker
31	b) Netcat
32	b)Spam
33	d) Tcpdump
34	a) EventLog Analyser
35	c) Mailbox Exchange Recovery
36	a) Centrify
37	b) Proofpoint
38	b) Cipher Cloud
39	a)Passive or active

40	a)availability
41	b)Mail user agent
42	c) 4
43	b) Reverse Engineering
44	a) trojans, redirected malicious URLs
45	a) Email scripting

Unit-II: Social Engineering

Question Bank

1) ___________ is a special form of attack using which hackers' exploit – human psychology.

a) Cross Site Scripting b) Insecure network

c) Social Engineering d) Reverse Engineering

2) Which of the following do not comes under Social Engineering?

a) Tailgating b) Phishing

c) Pre texting d) Spamming

3) _________ involves scams where an individual (usually an attacker) lie to a person (the target victim) to acquire privilege data.

a) Phishing b) Pre texting

c) Spamming d) Vishing

4) Which of the following is the technique used to look for information in trash or around dustbin container?

a) Pretexting b) Baiting

c) Quid Pro Quo d) Dumpster diving

5) Which of the following is not an example of social engineering?

a) Dumpster diving b) Shoulder surfing

c) Carding d) Spear phishing

6) In a phishing, attackers target the ________ technology to so social engineering.

a) Emails b) WI-FI network

c) Operating systems d) Surveillance camera

7) Tailgating is also termed as ___________

a) Piggybacking b) Pretexting

c) Phishing d) Baiting

8) Stealing pen drives and DVDs after tailgating is an example of lack of _______ security.

a) network security b) physical security

c) database security d) wireless security

9) Stealing pen drives and DVDs after tailgating is an example of lack of _______ security.

a) network security b) physical security

c) database security d) wireless security

10) Which of the following is not considering the adequate measure for physical security?

a) Lock the drawers

b) Keep strong passwords for corporate laptops and mobile phones

c) Keep confidential organization's document file open in the desk

d) Hide your hand against camera while inserting the PIN code

11) Which of the following is not a physical security measure to protect against physical hacking?

a) Add front desk & restrict unknown access to the back room

b) Create a phishing policy

c) Analyze how employees maintain their physical data and data storage peripheral devices

d) Updating the patches in the software you're working at your office laptop.

12) Which of them is not an example of physical hacking?

a) Walk-in using piggybacking b) Sneak-in

c) Break-in and steal d) Phishing

13) Physical _________ is important to check & test for possible physical breaches.

a) penetration test b) security check

c) hacking d) access

14) Phishing takes place using ___________

a) Instant Messaging c) Email

b) Websites d) Piggybacking

15) Training and Education of end users can be used to prevent _______

a) Phishing c) Tailgating / Piggybacking

b) Session hijacking d) both a and b

16) Social Engineering can be thwarted using what kinds of controls?

a) Technical c) administrative

b) Physical d) all of the above

17) Social engineering can use all the following except ________

a) Mobile phones c) instant messaging

b) Trojan horses d) viruses

18) Social engineering is designed to _________

a) Manipulate human behavior c) make people distrustful

b) Infect a system d) gain a physical advantage

19) Phishing can be mitigated through the use of ________

a) Spam filtering c) education

b) Antivirus d) anti-malware

20) Which mechanism can be used to influence a targeted individual?

a) Means of dress or appearance c) technological controls

b) Physical controls d) training

21) What os the best option for thwarting social engineering attacks?

a) Technology c) training

b) Policies d) physical controls

22) What is a vulnerability scan designed to provide to those executing it?

a) A way to find open ports	c) a way to diagram a network
b) A proxy attack	d) a way to reveal vulnerabilities

23) In social engineering a proxy is used to

a) Assist in scanning	c) perform a scan
b) Keep an attacker's origin hidden	d) automate the discovery of vulnerabilities

Answers:

Unit-II: Social Engineering

Q. No.	Answer
1	c) Social Engineering
2	d) Spamming
3	b) Pre texting
4	d) Dumpster diving
5	c) Carding
6	a) Emails
7	a) Piggybacking
8	b) physical security
9	d) wireless security
10	c) Keep confidential organization's document file open in the desk
11	d) Updating the patches in the software you're working at your office laptop.
12	d) Phishing
13	a) penetration test
14	c) Email
15	d) both a and b
16	d) all of the above
17	d) viruses
18	a)Manipulate human behavior
19	a)Spam filtering
20	a)Means of dress or appearance
21	c) training

22	d) a way to reveal vulnerabilities
23	b)Keep an attacker’s origin hidden

Unit-III: Information Security and legal Compliance

Question Bank

1) _______ is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction.

   a) Network Security b) Database Security

   c) Information Security d) Physical Security

2) From the options below, which of them is not a threat to information security?

   a) Disaster b) Eavesdropping

   c) Information leakage d) Unchanged default password

3) From the options below, which of them is not a vulnerability to information security?

   a) flood b) without deleting data, disposal of storage media

   c) unchanged default password d) latest patches and updates not done

4) _____ platforms are used for safety and protection of information in the cloud.

   a) Cloud workload protection platforms b) Cloud security protocols

   c) AWS d) One Drive

5) Which of the following information security technology is used for avoiding browser-based hacking?

   a) Anti-malware in browsers b) Remote browser access

   c) Adware remover in browsers d) Incognito mode in a browser

6) The full form of EDR is _______

   a) Endpoint Detection and recovery b) Early detection and response

   c) Endpoint Detection and response d) Endless Detection and Recovery

7) _______ technology is used for analyzing and monitoring traffic in network and information flow.

a) Cloud access security brokers (CASBs)　b) Managed detection and response (MDR)

c) Network Security Firewall　d) Network traffic analysis (NTA)

8) Compromising confidential information comes under _________

a) Bug　b) Threat

c) Vulnerability　d) Attack

9) Lack of access control policy is a _____________

a) Bug　b) Threat

c) Vulnerability　d) Attack

10) Possible threat to any information cannot be ________________

a) reduced　b) transferred

c) protected　d) ignored

11) PCI-DSS stands for _______

a) The Portable Card Industry Data Secure Standard

b) The Payment Copy Industry Data Security Standard

c) The Payment Card Industry Data Security Standard

d) The Payment Card Instruction Data Sedding Standard

12) HIPAA stands for___________

a) Human Insurance Portability and Access Act

b) Health Insurance Portability and Accountability Act

c) Health Inactivity Portability and Accountability Act

d) Health Inactivity Portability and Accounting Act

Answers:

Unit-III: Information Security and legal Compliance

Q. No.	Answer
1	c) Information Security
2	d) Unchanged default password
3	a) flood
4	a) Cloud workload protection platforms
5	b) Remote browser access
6	c) Endpoint Detection and response
7	d) Network traffic analysis (NTA)
8	b) Threat
9	c) Vulnerability
10	d) ignored
11	c)The Payment Card Industry Data Security Standard
12	b)Health Insurance Portability and Accountability Act