040010504 – Cyber Security

Unit – 1 Cyber Security

SHORT ANSWER QUESTIONS:-

1. What does the word cybercrime describe?
2. “Greedy for fame” keeps the criminal in which category?
3. Why competing companies use employees for committing cybercrime?
4. ”Geeta” receives mail from Meena” which was not sent by Meena. Which is the crime behind it and how would you define it?
5. ”Employees seeking revenge” this comes under which type of criminals .Give another example of that.
6. ”URL manipulation is a technique to perform phishing”. This statement is true or false. Justify your answer.
7. Differentiate spear phishing from phishing.
8. First recorded cybercrime was recorded against which device and what was the crime named?
9. Defamation with the help of computerizes known as which crime? Give other example of that crime.
10. Password sniffing is a crime that belongs to which two categories.
11. Give an example of crimes that are committed against financial transactions.
12. “Soliciting the sale of false mark sheets "is which type of crime? Also give proper definition.
13. “Attacker interacting with the victims repetitively”. This crime comes under which category.

LONG ANSWER QUESTIONS:-

1. “The idea is to make alteration so significant that in single case it would go unnoticed”. Name the attack. Also list and explain different types of attacks which comes under this category.
2. Write atleast three differences between cyberwarfare and cyberterrorism with appropriate example.
3. Differentiate cybercrime from cyberfraud with appropriate example.
4. With appropriate case study explain phishing.
5. What Indian penal code states about cyberdefammation.Explain in detail.
6. Explain atleast four cybercrimes against organization.
7. List and explain the terminologies of cybercrime.
8. Password sniffing is an attack that comes under two categories of cybercrime. Name the categories and also explain at least 3 attacks from each category.
9. With diagram explaintypes of cyber criminals in detail.
10. “Pedophiles are connected to child pornography”. Explain this statement in detail.

Practical/Scenario based questions:

1.Meena young girl was about to get married to Mahesh. She was really pleased because despite it being an arranged marriage, she had liked the boy. He had seemed to be open-minded and pleasant. Then, one day when she met Mahesh, he looked worried and even a little upset. He was not really interested in talking to her. When asked he told her that, members of his family had been receiving emails that contained malicious things about Meena's character. Some of them spoke of affairs, which she had in the past. He told her that, his parents were justifiably very upset and were also considering breaking off the engagement. Fortunately, Mahesh was able to prevail upon his parents and the other elders of his house to approach the police instead of blindly believing what was contained in the mails. During investigation, it was revealed that the person sending those emails was none other than Meena's stepfather. He had sent these emails so as to break up the marriage. The girl's marriage would have caused him to lose control of her property of which he was the guardian till she go.

Read the case carefully and answer the following:

i. Which type of criminal Meena's stepfather is?
ii. Identify the cybercrime done by him.
iii. Name the category to which this cybercrime belongs?
iv. Write the definition of identified cybercrime?

2. A student of the Air Force Balbharati School, Surat, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.

Read the case carefully and answer the following:

i. Which type of criminal student is?
ii. Identify the cybercrime done by him.
iii. Name the category to which this cybercrime belongs.
iv. Write the definition of identified cybercrime.

3.Mr.MalhotraC.E.O of an textile company introduced a new device called loom which repeatedly weaved clothes at rapid speed. It was a bad news for workers as machine handled many workers task itself. Many workers were disappointed and damaged the device. Identify the crime and also define it.

4.Mrs.Kohli got unwanted messages and repeated calls at every odd hours forcing her to talk and chat with the different people. Her husband's friend stealed her phone number and gave it to his friends to harrasher. She was fed up and this messages created havoc in her personal life and she reported to police and filed an FIR against them. Read the case carefully and answer the following.

i. Identify the cybercrime.
ii. Name the category to which this cybercrime belongs.
iii. Write the definition of identified cybercrime.

5.Arun was using the internet hours of Suresh without the knowledge of him. He downloaded the materials which were not freely available on web. Identify the crime with proper definition.

6. Suzzane and James are two NRIs who were influencing and motivating children to give pornographic pictures.
Read the above statement and answer the following questions.
a) What are this NRI's known as ?
b) Name the crime committed by them.
3) How this people work to commit such crime?

FILL IN THE BLANKS:-

1. ____________________ is used to describe the internet and other computer networks.
2. Cybersquatting is derived from the term ___________.
3. Password sniffing belongs to the category of ____________ and ____________. Of cybercrimes.
4. People who create electronic spam are called _____________.
5. ______________ takes place when defamation takes place with the help of computers.
6. _________ is written defamation and _____________ is oral defamation.
7. _________________________ attacks are used to commit financial crimes.
8. The first stage of web jacking is ____________________.
9. An illegal intrusion, posing as a genuine user is known as _____________________.
10. ________________ mean visual deception.
11. __________________ are the people who coerce minors to engage in sexual activities.
12. _______________ is a popular means of sharing and distributing information on the web with respect to specific topic or subjects.
13. When a criminal uses someone else's identity for his/her own illegal purposes is known as ______________.
14. __________________ is the art of breaking into phone or other communication systems.
15. The goal of crimes targeted at individuals is to exploit human weaknesses such as ______________ and _____________.
16. ______________ category of cybercrime involves the attacker interacting with the victims repetitively.

MULTIPLE CHOICE QUESTIONS:-

1) A crime conducted in which a computer was directly and significantly instrumental
   a) Computer crime
   b) Cyber Space
   c) Cyber squatting
   d) Cyber punk

2) Any illegal behavior, directed by means of electronic operation, that targets the security of computer systems and the data proceed by them
   a) Cyber Crime
   b) E-crime
   c) High-tech crime
   d) All

3) Worldwide network of computer networks that uses the TCP/IP for communication to facilitate transmission and exchange of data
   a) Shared Database
   b) Cyber Space
   c) E mail
   d) Internet

4) Politically planed and motivated attack against information is known as
   a) Cyber Fraud
   b) Cyber squatting
   c) Cyber terrorism

d) Cyber Crime

5) Which one is not a group of category of Cyber criminals.
   a) Hungry for recognition
   b) Not interested in recognition
   c) Spammers
   d) Insiders

6) Email is one that appears to originate from one source but actually has been sent from another source.
   a) Forwarded Email
   b) Spam Email
   c) Spoofed Email
   d) Bulk Email

7) Which are the cyber crime comes under Cybercrime against Society
   a) Forgery
   b) Cyber terrorism
   c) Web jacking
   d) All

8) When some once forcefully takes control of a website, it is known as
   a) Website Hacking
   b) Remote connection
   c) Web jacking
   d) Web controlling

9) EMP stands for
   a) Employee
   b) Excessive Multiple Posting
   c) Executed by Management Person
   d) All

10) People whom physically or psychologically force minors to engage in sexual activities, which the minors would not consciously consent.
   a) Pedophiles
   b) Physiologist
   c) Genuine People
   d) Teenagers

Unit – 2 Cyber offenses

SHORT ANSWER QUESTIONS:-

1. Define the following terms:
   a. Hacker b. Cracker c. Phreaker
2. Enlist the categories of vulnerabilities in a network.
3. Define the term Reconnaissance.
4. What do you mean by footprinting?
5. What do you mean by passive attack?
6. Define term network sniffing?
7. What do you mean by an active attack?

8. What do you mean by scanning?
9. Differentiate between port scanning and network scanning.
10. List the types of social engineering.
11. Define Dumpster Diving.
12. What do you understand by cyber stalking?
13. Enlist the types of stalkers.
14. Give the classification about the botnets.
15. Differentiate between ID theft and financial frauds.
16. What do you mean by triangulation?
17. State a difference between mosquioto trojan and skull trojan.
18. What do you mean by scavenging?

LONG ANSWER QUESTIONS:-

1. Differentiate between passive and active attacks.
2. Enlist five toolkits for passive attacks and active attack and describe one of them.
3. Describe port scanning in detail.
4. What is social engineering? Explain an example of any one type of social engineering.
5. Elucidate human based social engineering in depth.
6. Elucidate computer based social engineering in depth.
7. Differentiate between shoulder surfing and dumpster diving.
8. Justify how pop-up windows can be said as a social engineering offense.
9. What is cyberstalking? Give the classification of stalkers and explain both .
10. Write a major difference between online and offline stalker?
11. Illuminate in detail how does stalking work?
12. What is a botnet? Describe with diagram how do botnets create business.
13. Describe the preventive measures that can be used against botnets.
14. What is an attack vector? Describe in detail how are attack vectors launched.
15. List the types of attacks against 3G mobile networks.
16. Briefly discuss the detail about credit card frauds with example.
17. Discuss modern techniques of credit card frauds.

FILL IN THE BLANKS:-

1. Criminals plan __________ and ____________ type of attacks.
2. _____________ types of attacks are attempted to alter the system.
3. ______________ types of attacks are attempted to gain information of the target.
4. Reconnaissance begins with the phase ___________________.
5. Active reconnaissance involves the risk of detection, which is also known as ______________________.
6. Tools used for penetration testing are also used for _________________.
7. The objectives of scanning are ___________ , _________________ and ______________ scanning.
8. Social engineering is the technique to ____________ people.
9. The greatest technique by social engineers to deceive people is ______________.
10. Looking into the trash for information is known as _______________.
11. _______________ is equivalent to dumpster diving.
12. Searching through object residue to acquire sensitive data is known as ___________.

13. Cyberstalking is the use of ____________ and __________________ to harass an individual or a group.
14. __________ and _____________ are the types of stalkers.
15. Botnets are also called as __________ networks.
16. The full form of PDP is _______________.

MULTIPLE CHOICE QUESTIONS:-

1) Gathering information about a target without his/her knowledge is known as
    a) Attack
    b) Active Attack
    c) Reconnaissance
    d) Passive Attack

2) Which two are the phases of gathering information for attackers
    a) Active Attack
    b) Passive Attack
    c) Direct Attack
    d) Both (a) and (b)

3) To examine intelligently while gathering information about the target is
    a) Investigation
    b) Scanning
    c) Tracing
    d) Intelligent

4) The attackers consume 10% time in
    a) Scanning
    b) Executing the malicious commands
    c) Scrutinizing
    d) Launching the attack

5) _______________ involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insider
    a) Scrutinizing
    b) Social Stalking
    c) Scanning
    d) Social Engineering

6) Searching through object residue to acquire sensitive data without authorization is know as
    a) Binning
    b) Scavenging
    c) Stalking
    d) Bulling

7) Which are the types of Stalkers ?
    a) Online
    b) Computer Based
    c) Offline
    d) (a) and (c) both

8) When the internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person is know as
   a) Cyber stalking
   b) Cyber bullying
   c) Cyber squatting
   d) Cyber Engineering
9) ________________ is network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the user knowledge
   a) Shared WiFi
   b) World Wide Web
   c) Botnet
   d) Intranet
10) An attacker can gain access to computer or to a network server to deliver a payload or malicious outcome is known as
   a) Botnet renting
   b) Active Vector
   c) Botnet selling
   d) Attack Vector

Unit – 3 Cyber crime methods and security mechanisms

SHORT ANSWER QUESTIONS:-

1. List down the stages of a network attack.
2. What do you mean by initial uncovering?
3. What is network probing?
4. What is the main difference between DoS and DDoS?
5. List out the levels of DoS attacks.
6. What is ping of death attack?
7. What do you mean by SQL injection?
8. What is a blind SQL injection?
9. List the types of buffer overflows.
10. What is a stack based buffer overflow?
11. What is NOP?
12. List the types of attacks on wireless networks.
13. What do you mean by sniffing?
14. What do you mean by encryption cracking?
15. Define frame spoofing.
16. Define MAC address spoofing.

LONG ANSWER QUESTIONS:-

1. Differentiate between network probe and network capture.
2. Write a short note on DoS attack.
3. List and Explain classification and levels of DoS attack.
4. List out the levels of Dos attacks and explain any two of them in detail.
5. Differentiate between bandwidth attacks and unintentional DoS attacks.
6. List out the tools used to launch a DDoS attack. Explain any one in detail.
7. Describe how to prevent from DoS/DDoS attacks.
8. Define SQL injection. How is an SQL injection attack carried out?

9. Write a short note on Blind SQL injection.
10. Describe the techniques used to prevent SQL injection attacks.
11. Define buffer overflow. List its types and explain any one in detail.
12. Describe the preventive techniques used to minimize buffer overflow attacks.
13. List the types of traditional attacks on wireless networks and explain any one in detail.
14. Write a short note on spoofing.
15. Write a short note on theft on internet hours.
16. Describe in detail how to secure a wireless network.

FILL IN THE BLANKS:-

1. Initial uncovering is also known as ________________.
2. Ping sweep is used to seek _____________.
3. __________ attack is an attempt to make a computer resource unavailable to its users.
4. The full form of USCERT is _________________.
5. Flood attack is also known as _______________.
6. The ping of death attack sends ________ packets.
7. SYN attack is also known as _______________.
8. _______________ is an example of an old DoS attack.
9. In_____________ type of attack large number of zombie systems are used for the purpose of the attack.
10. _________________ is used when results of the SQL injection is not visible to the attacker.
11. ______________ is an assembly level instruction which does effectively nothing.
12. Heap is a ___________ where dynamic objects are allocated.
13. Penetration of a wireless network through unauthorised access is known as __________.
14. ____________, _____________ and __________ are types of spoofing.
15. The first step to protect a network is to use _____________________.
16. _______________ is eavesdropping on the network.

MULTIPLE CHOICE QUESTIONS:-

1) _____________is not a part of DoS attacks
    a) Bandwidth attacks
    b) Logic attacks
    c) International attacks
    d) Protocol attacks

2) Flood attack is also known as
    a) Ping of death attack
    b) Ping flood
    c) Pink flood
    d) Ping of direct attack

3) ___________ is an attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them
    a) Smurf attack
    b) SYN attack
    c) Flood Attack

d) Teardrop Attack

4) Which system is known as secondary victims?
   a) Second System
   b) Targeted System
   c) Distributed System
   d) Zombie System

5) A small piece of code used as a payload in the exploitation of software vulnerability, is called
   a) Assembly code
   b) Shell code
   c) C and C++ code
   d) Malicious code

6) Which is not a type of mobile workers?
   a) Roaming user
   b) Nomad
   c) Road warrior
   d) Local user

7) ____________ is not a traditional techniques of attack on wireless networks
   a) Sniffing
   b) DoS
   c) MITM
   d) Squatting

8) _______________ is a code technique that exploits a security vulnerability occurring in the database layer of and application
   a) Shell code
   b) SQL injection
   c) PL/SQL block
   d) Blind SQL injection

9) _______________ and ______________ are type of Buffer Overflow?
   a) Heap Buffer Overflow
   b) State Base Buffer Overflow
   c) Heap Hope Buffer Overflow
   d) Stack Base Buffer Overflow

Unit 4 : Legal Perspectives of Cyber Security

SHORT ANSWER QUESTIONS:-

1. What is IPC? In which year was it published?
2. What is IEA? In which year was it published?
3. To which chapter of the ITA 2000 do digital and electronic signatures belong?
4. How is computer source code defined in section 65 of ITA 2000?
5. What is the punishment for publishing or transmitting obscene material in electronic form?
6. What is the penalty for breach of confidentiality and privacy?
7. What is PKI?
8. What is the role of a public key certificate?

9. What is X.509?
10. What do you mean by certificate user?

LONG ANSWER QUESTIONS:-

1. Write a short note on section 65 of ITA 2000.
2. Describe computer related offences and the corresponding penalty .
3. List the sections of ITA 2000 and explain section 72 and 74.
4. Write a short note on public key certificate.
5. Describe in brief X.509 digital certificates.
6. Describe the basic components of PKI.
7. What is non repudiation? Describe the basis for repudiation of a traditional signature.
8. Describe the crypto technical meaning of non repudiation.

FILL IN THE BLANKS:-

1. The Indian Evidence Act was formed in the year _________.
2. Section 65 of ITA 2000 includes ________________.
3. Computer related offences lead to imprisonment of ____ years.
4. The penalty for breach of confidentiality and privacy is ______________ Rs.
5. A public key certificate is a ___________________ statement.
6. X.509 certificates can be used for ______________.
7. __________ is a security protocol that provides privacy and authentication for your network traffic.
8. The trusted entity that issues and revokes public key certificates is known as __________________.
9. The entity that is trusted by the CA to register or vouch for the identity of users to a CA.
10. Certificate repository is an electronic site that holds _________________ and _____________.

MULTIPLE CHOICE QUESTIONS:-

1) An electronic site that hold a certificates and CRLs is known as
   a) E-CRLs Access
   b) E-Certificate Access
   c) Certificate revocation
   d) Certificate repository

2) _________ is a trusted entity that issues and revokes public-key certificates and CRLs
   a) Certification Authority
   b) Registration Authority
   c) Certifying Authorities
   d) Electronic Signature

3) ________________ is an entity that it trusted by the certification authority to register or vouch for the identity of user to a certificate authority
   a) CA
   b) CRA
   c) PKI
   d) RA

4) CCA stands for ________________________
   a) Certifying Common Authority
   b) Controller Certifying Author

c) Controller Certifying Authority
d) Certifying Controller Authority

Unit 5 : Digital Forensic Fundamentals

SHORT ANSWER QUESTIONS:-

1. What do you mean by digital forensics?
2. State the objective of cyberforensics.
3. What do you mean by computer forensics?
4. State the main difference between computer forensics and digital forensics.
5. Why is it difficult to give a precise definition of digital evidence?
6. Enlist uses of digital forensics.
7. What is a forensic policy?
8. Define: Chain of Custody.
9. What do you mean by fungibility?
10. List the two domains into which cyberforensics can be divided.
11. What does logical file system consist of?
12. Give the differences between physical and digital evidence.
13. What is oral evidence?
14. State the difference between logical context and physical context involved in identifying digital evidence.
15. Enlist the cardinal rules for evidence.
16. What is the task of an expert witness?
17. State any four broad-level elements of a forensics report.
18. List out the toolkits used in forensics for analysis and interpretation.
19. What do you mean by dead analysis?
20. What is the major difference between paper evidence and digital evidence?

LONG ANSWER QUESTIONS:-

1. Define digital forensics. Differentiate between digital forensics and computer forensics.
2. Write a short note on typical scenarios involved in digital forensics.
3. Where does evidence reside on computer systems? List its types and explain them.
4. What do you mean by evidence? State its types and explain them.
5. Describe the different context involved in identifying digital evidence.
6. Draw the diagram of process model for digital evidence and explain briefly digital evidence documentation.
7. List the phases of digital forensics life cycle. Explain preparation and identification phase.
8. Explain how to examine digital evidence in detail.
9. Explain how digital evidence is analyzed, interpreted and attributed.
10. List and describe the principles applied for maintaining the rules of digital evidence.
11. Write a short note on chain of custody concept.
12. Differentiate between preparation of evidence and identification of evidence.

FILL IN THE BLANKS:-

1. ______________ plays a key role in the investigation of cybercrime.
2. The objective of cyber forensics is to provide ______________________ of a specific or general activity.
3. _____________________ is a statement that clearly specifies the allowed and disallowed elements with regard to security.
4. _________________ includes everything that is used to determine or demonstrate the truth of assertion.
5. ____________________ is used in most evidence situations to maintain the integrity of the evidence.
6. Cyberforensics is divided into ____________________ and ______________________.
7. _____________ is a space allocated to a file but not used during internal fragmentation.
8. Documents that are produced for the inspection of the court are called _____________ evidence.
9. Digital forensics examiners must consider the __________________ of digital data.
10. Embedded flash memory falls under the family of ______________________.
11. The process of creating an exact duplicate of the original evidentiary media is called _________________.
12. ___________________ phase involves presentation and cross examination of expert witness.
13. __________________ is the central concept in cyber forensics investigation.

MULTIPLE CHOICE QUESTIONS:-

1) COFEE stands for _____________________
   a) Computer Online Forensics Evidence Extractor
   b) Computer Online Forensics Extractor Evidence
   c) Computer and Other Forensics Evidence Extractor
   d) Computer and Other Forensics Extractor Evidence

2) Cyber forensics can be divided into _______________ and __________________
   a) Computer Forensics
   b) Network Forensics
   c) Digital Forensics
   d) Scientific Forensics

3) Evidence only includes _________________evidence and ________________ evidence
   a) Oral
   b) Documentary
   c) Digital
   d) Original

4) Which is not a context involved in identifying a piece of digital evidence
   a) Physical
   b) Logical
   c) Electrical
   d) Legal

5) Which activity is not a part of reporting phase in forensics life cycle?
   a) Summarize
   b) Translate
   c) Draw conclusion
   d) Explain conclusion

6) Which activity is not a part of analysis phase in forensics life cycle?
   a) Determine significance
   b) Reconstruct fragments of data
   c) Recover Data
   d) Draw Conclusion

7) ___________________ is not a type of embedded memories.
   a) RAM
   b) ROM
   c) EPROM
   d) EEPROM

8) ___________________is the central concept in cyber forensics/digital forensics investigation
   a) Chain of custody
   b) Testifying
   c) Analysis
   d) Attribution

9) Following are the component for maintaining chain of custody
   1. Preserve
   2. Analyze
   3. Report
   4. Collect

   Right order of sequencing is
   a) 1,3,4,2
   b) 2,3,4,1
   c) 4,1,2,3
   d) 4,1,3,2

10) The tie between technical issues associated with the digital forensics evidence and the legal theories is the job of
    a) Expert witness
    b) Digital Forensics Department
    c) Technology expert
    d) All

Unit 6 : Forensics methods

SHORT ANSWER QUESTIONS:-

1. What do you mean by foot printing?
2. State the difference between Scanning and probing.
3. What do you mean by click kiddie?
4. Draw a diagram showing hacker categories with respect to profit and damage.
5. Which are the traditional data mining techniques?
6. What is entity extraction?
7. What do you mean by association rule mining?
8. What categories does device forensics include?
9. What do you mean by device seizure?
10. What is IMEI number?
11. How logical acquisition is differs from physical acquisition?
12. Which kind of forensic information can be availed from a smartphone?
13. List out any five iphone hardware components.
14. Enlist the forensics techniques utilized with an iPhone.
15. List out the forensics tools used for iPhones which have operating systems other than windows XP.
16. What does a PDA seizure do?
17. What is FCR? What does it do?
18. What is a cell seizure used for?
19. What is the function of acquisition terminal?
20. How is an EnCase evidence file generated?

LONG ANSWER QUESTIONS:-

1. Describe in detail scanning and probing.
2. Draw the diagram of OSI 7 layer model and list out the steps of network hacking.
3. Write a short note on installing backdoors.
4. List the carving tools and explain in detail file carving tools.
5. Explain in detail how data mining techniques are used in cyberforensics.
6. Give a detailed explanation of the types of data that can be acquired from a hand held device.
7. Write a short note on logical analysis of smartphones.
8. Describe the forensics techniques used with iPhones in detail.

9. Differentiate between MacLockPick and WOLF.
10. State differentiate between physical acquisition and logical acquisition.
11. Enlist market tools available for forensics and explain any one in detail.
12. Differentiate between EnCase and Palm DD.
13. Explain in detail about PDA seizure.
14. Write a short note on forensics card reader.
15. Describe in brief ForensicSIM.
16. State the differentiate between cell seizure and MOBILedit! .
17. Provide an overview of how "data mining" techniques can be applied in cyberforensics.
18. What is a "Jailbroken" device? What are the security implications and possible impact on cyber crime?

FILL IN THE BLANKS:-

1. The OSI 7 Layer Model addresses the network _____________ and network _____________ process.
2. ___________________ includes a combination of tools and techniques used to create a security posture of an organization.
3. Uneducated hackers are known as ________________.
4. _________________, __________________ and ______________ are types of carving tools.
5. _____________, ____________________ and _________________ are techniques of data mining.
6. _____________________ technique discovers frequently occurring item sets in a database and presents the pattern as rules.
7. _____________ comes first as the line of defense in hand held forensics.
8. Cell phone forensics includes the analysis of ____________ and _________________.

MULTIPLE CHOICE QUESTIONS:-

1) Uneducated hackers are known as __________________
   a) Newbie
   b) Exploit buyer
   c) Script kiddies
   d) Exploiters

2) Foot printing includes combination of _________________ and ______________ used to create full profile of the organization's security posture
   a) Network blocks
   b) Techniques
   c) Domain Name
   d) Tools

3) Criminal activities can arise from the use of ______________ sites.
   a) Hackers
   b) Developers
   c) Social Network
   d) All

4) Which protocol is not belongs to Session Layer?
    a) HTML
    b) HTTP
    c) RPC
    d) SMTP

5) In which layer ping does not work?
    a) Application
    b) Transport
    c) Session
    d) Presentation

6) The _______________ number of a cell phone is a very important starting point for the FIR
    a) Mobile
    b) IMEI
    c) Model
    d) EIR

7) ____________ is not come under the Cellular phones category
    a) CDMA
    b) Black Berry's
    c) GSM
    d) Iden

8) In Cell Seizure, phone book cannot contain____________
    a) own numbers
    b) speed dialing
    c) fixed dialing
    d) dialed numbers

9) MOBILedit cannot allows examiner to acquire logically, search, examine and report data from
    a) CDMA
    b) PCA
    c) GSM
    d) PDD

10) Before 100 years ago the first Mobile telephone was invented and patented by
    a) Dr. Joel S. Engel
    b) Nathan B. Stubblefield
    c) Martin Copper
    d) John F. Mitchell