INTRODUCTION OF CYBERCRIME

Multiple Choice Type Questions

1. What is the full form of CERT/CC? [WBUT 2015, 2018]
   a) Computer Engineering Response Team Co-ordination Centre
   b) Computer Emergency Record Team Co-ordination Centre
   c) Computer Emergency Response Team Co-ordination Centre
   d) Computer Engineering Record Team Co-ordination Centre

Answer: (c)

2. LDAP stands for [WBUT 2015, 2018]
   a) Lightweight Directory Access protocol
   b) Lightweight Data Access Protocol
   c) Lightweight Domain Access Protocol
   d) Lightweight DNS Access protocol

Answer: (a)

3. The term 'Bluetooth' has been taken from [WBUT 2015]
   a) Danish blue sea b) Fine blue sea
   c) Danish king Harald Batand d) Norway hill

Answer: (c)

4. Programs that multiply like viruses but spread from computer to computer are called as: [WBUT 2015]
   a) Worms b) Virus c) Boot d) None of these

Answer: (a)

5. The notorious art of breaking into phone or other communication systems is known as [WBUT 2016]
   a) hacking b) cracking c) phreaking d) none of these

Answer: (c)

6. The term ..... refers to a bad or criminal hacker. [WBUT 2016]
   a) black hat b) white c) gray hat d) none of these

Answer: (a)

7. A defense method that is effective today may not remain so for long because [WBUT 2016]
   a) defense method become obsolete
   b) defense method may expire
   c) attackers are constantly updating attacks vectors
   d) none of these

Answer: (c)

8. Hacktivism is [MODEL QUESTION]
   a) Activism b) Hacking for a cause
   c) Passive hacking d) Malicious hacking

Answer: (b)

9. Banner grabbing is an example of what? [MODEL QUESTION]
   a) Passive operating system fingerprinting
   b) Active operating system fingerprinting
   c) Footprinting
   d) Application analysis

Answer: (a)

10. Which of the following is a cybercrime? [MODEL QUESTION]
    a) Hacking b) Cyber bulling c) Virus attack d) All of these

Answer: (d)

11. What is enumeration? [MODEL QUESTION]
    a) Identifying active systems on the network
    b) Cracking passwords
    c) Identifying users and machine names
    d) Identifying routers and firewalls

Answer: (c)

Short Answer Type Questions

1. What is software piracy? Discuss about the preventive measures against software piracy. [WBUT 2015]

Answer:

1st Part:

Software piracy is the stealing of legally protected software. Under copyright law, software piracy occurs when copyright protected software is copied, distributed, modified or sold. Software piracy is considered direct copyright infringement when it denies copyright holders due compensation for use of their creative works.

2nd Part:

Here are some of the tips to prevent or lessen software piracy:

Code Key - For the past 5 to 7 years, software developers have devised a plan to lessen or prevent software piracy. This is by using a code key. A code key comes with the software that we buy. Before fully installing the software on our computer, we must provide the specific code key that came with the software. After providing the code key, we can run the software on our computer. The code key also locks after it has been used. This is so that the software cannot be installed on other computers after it has been installed on one. We will have to call the manufacturer of the software to be able to use the code key again. This is not good news to people who pirate software.

Open Source - Open source software is described as a free software that anyone can download from the Internet. A lot of different software can are licensed as open source. Open source software are under the license free software license. There are also different upgrades for these open source software that can also be freely downloaded from the Internet. By using open source software, people don't need to worry about spending a lot of money for original copies of software. This will also lessen the number of people who are using pirated software as there are alternative programs that can be used and they do not have to pay fines when they are caught.

Hardware Key - A hardware key is a device that is used for anti-piracy. This tool prevents software vendors to distribute their products or use them without authorization from the copyright owner of the software. The hardware key works when it is attached to a computer. It monitors software licensing and enforces licensing of the protected software that are detected on the computer. This tool will lessen software vendors from illegally distributing the software that they have and is a good prevention measure for piracy.

Anti-Piracy Software - There are different types of anti-piracy software that are available for free. Anti-piracy software is used to prevent illegal duplication or illegal use of copyrighted software. There is also an anti-piracy software that prevents hackers from getting into the software and copying it without consent from the copyright owner. Some of them are also already integrated on the disks of the software that contains the program. This may also be for piracy music. The anti-piracy association is also looking for other ways to prevent software piracy. Reporting anti-piracy may prevent it from happening.

2. What are the different types of cybercriminals? Explain each one briefly.
[WBUT 2016, 2018]

Answer:

When any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:

Hacking: *This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.*

Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

Malicious Software: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

Child soliciting and Abuse: This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

3. What is hacking? Differentiate between white-hat hacking and black-hat hacking.
[WBUT 2016]

Answer:

1st Part:

Hacking is unauthorized intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose.

2nd Part:

Like all hackers, black hat hackers usually have extensive knowledge about breaking into computer networks and bypassing security protocols. They are also responsible for writing malware, which is a method used to gain access to these systems.

Their primary motivation is usually for personal or financial gain, but they can also be involved in cyber espionage, protest or perhaps are just addicted to the thrill of cybercrime. Black hat hackers can range from amateurs getting their feet wet by spreading malware, to experienced hackers that aim to steal data, specifically financial information, personal information and login credentials. Not only do black hat hackers seek to steal data, they also seek to modify or destroy data as well.

White hat hackers choose to use their powers for good rather than evil. Also known as "ethical hackers," white hat hackers can sometimes be paid employees or contractors

working for companies as security specialists that attempt to find security holes via hacking.

White hat hackers employ the same methods of hacking as black hats, with one exception- they do it with permission from the owner of the system first, which makes the process completely legal. White hat hackers perform penetration testing, test in-place security systems and perform vulnerability assessments for companies. There are even courses, training, conferences and certifications for ethical hacking.

4. Explain the difference between hackers, Crackers and Phreakers. [WBUT 2017]
Answer:
Hackers: A **Hacker** is a person who is extremely interested in exploring the things and recondite workings of any computer system or **networking** system. Most often, hackers are the expert programmers. These are also called **Ethical Hackers** or white hat hackers. And the technique or hacking they perform is called ethical hacking.

Ethical Hacking Means you think like Hackers. i.e. First you Hack the Systems and find out the loop holes and then try to correct those Loop Holes. These type of hackers protect the cyberworld from every possible threat and fixes the future coming security loop holes. These peoples are also called as "GURU's" of Computer Security.

Crackers: Crackers or Black Hat hackers or cheaters or simply criminals, they are called criminals because they are having the mindset of causing harm to security and they steals very useful data and use it in wrong ways.

Phreakers: Phreakers are people who specialize in attacks on the telephone system. The word, which became popular in the mid-1980s, is probably a combination of the words *phone* and *freak*. (Phreakers are also known as "phreaks" or "phone phreaks.") In the early days, phreakers whistled or used an instrument to mimic the tones the phone system then used to route calls and identify payment, especially as a way to avoid paying for an expensive call. Modern phreaking involves breaking into and manipulating the phone company's computer system, making it a specialized kind of hacking.

5. What is forgery? [WBUT 2017]
Answer:
Forgery includes imitation of original paper or online documents for the intent to harm reputation, or cheat, individual or a group by means of telecommunication network is forgery. It includes fraudulent transaction of credit cards, postage stamps, seals, currency, immigration documents, signatures, bank checks, academic credentials, digital signatures on electronic documents, even medicines.

Example: In year 2008, a cyber crime originated in UK, named as DarkMarket used to sell credit card, login informations to members who used to commit financial crimes and fraudulent transactions.

6. What is the maximum penalty for forgery? [MODEL QUESTION]
Answer:
If caught under the act of forgery, defined under Indian Penal Code section 463, 464 an offender will be punished with imprisonment from three to five years or will be charged with a fine upto 2 lakhs or both.

7. What are the classifications of hackers? [MODEL QUESTION]
Answer:
Hackers are categorized into three kinds as black hat or crackers, white hat or ethical hackers, and grey hackers. Black hat hackers are normally crackers. They tamper website contents, forward spams, flood the network, and impersonate accounts. They always have malicious intent. White hat persons are ethical hackers who is responsible for finding the loopholes of a system. Industries employ white hats to find security cracks in the system or they are also employed if any attack has taken place. Study reports revealed that most of the industrial attacks are from inside. Someone who knows the security system very well and uses this skill to pose a threat to the organization can be called as grey hat. They behave ethical sometimes and crackers at other times.

8. What are the files that store passwords for Windows and Linux? [MODEL QUESTION]
Answer:
Windows stores encrypted files in SAM file under system32 while Linux stores passwords in/etc/shadow file.

9. a) Give a brief comparison between a conventional crime and a cyber crime.
b) List the motives and reasons behind cyber crimes. [MODEL QUESTION]
Answer:
a) Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment."

Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those crime, where either the computer is an object or subject of the conduct constituting crime. "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime."

There is apparently no distinction between cyber and conventional crime. However on a deep introspection we may say that there exists a fine line of demarcation between the conventional and cyber crime. The demarcation lies in the involvement of the medium in cases of cyber crime. The prerequisite for cyber crime is that there should be an involvement of the virtual cyber medium at any stage.

b) The crimes and criminals in the cyber world vary little from their physical world counterparts. Historically, and today, the same laws are used to prosecute both (i.e.: trespass, fraud, theft, copyright violation).

The motives and profiles of criminals in the virtual world are as varied as in the physical world. Motives include financial benefit, thrill seeking, revenge, knowledge, and beliefs. Where the two worlds begin to diverge is in the lingo being built for the criminal using the computer in his crimes. A script kiddie is someone with a low technical skill level and of a young age. A hacktivist seeks to further his views by promoting them or striking out at those who hold opposing views. A web defacer targets websites that can be penetrated and changed. Crackers circumvent copy protection mechanisms. Pirates make or distribute unauthorized copies of protected programs or works. Lamers have a low technical skill level and largely reuse the work of others. Phreakers target telephone systems.

The term hacker is primarily used to describe those who participate in the insightful or intuitive exploration of systems. These activities are, in of themselves, benign but the term has also become linked with the cyber criminal. The term cracker is generally reserved for hackers with criminal intentions.
Hackers often align themselves in groups. They exchange details of their exploits on web sites and through Internet Relay Chat (IRC) messages. They contribute technical knowledge to their group and even participate in collaborative attacks.

10. What are the different types of password hacking method?
[MODEL QUESTION]

Answer:
There are two different categories for password hacking one is active and another is passive. Passive attack includes sniffing, masquerading, eavesdropping or playing man in the middle attack, dictionary attack, brute force attack. Active attack can include guessing, shoulder surfing, or social engineering.

11. Define the terms social engineering, man in the middle attack.
[MODEL QUESTION]

Answer:
Social engineering:
It is psychological manipulation of persons ultimately gaining their trust to reveal confidential information about the organization or the system. There are different types of social engineering techniques used to lure a victim to reveal secret information. Hackers use people's good nature to make this kind of access into organization. Pretexting, vishing, tailgating etc. are the normally used as social engineering methods.

Man-in-the middle attack:
Attacker acts in between server and client connection. He splits the TCP connection into two and acts as server to the client and a client to the server. Any message is intercepted by the attacker and he is able to manipulate both client and server in his own way.

12. What is eavesdropping and hybrid attack? **[MODEL QUESTION]**

Answer:
Eavesdropping:
It is snooping into conversation of unsuspecting parties over telephone lines, instant messages, Wireless LANs, etc. Attacker use tools like Airsnort, Ethereal and sniff around in any forms of communication that is considered to be private. This includes capturing of network packet in the communication medium.

Hybrid attack:
It is a password attack which combines the flavor of dictionary attack and brute force attack.

13. Define strong, weak and random password with examples. [MODEL QUESTION]

Answer:
A password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase.

Weak passwords refer to any passwords that can be easily guessed, either because it's so personal to a person or because it hardly takes any time to find it via the brute-force method, where a hacker (here, a hacker being anyone who's intent on finding your password, be they a criminal in Belarus or your nosey kids) runs through all possible password options.

A random password generator is software program or hardware device that takes input from a random or pseudo-random number generator and automatically generates a password. Random passwords can be generated manually, using simple sources of randomness such as dice or coins, or they can be generated using a computer.

Long Answer Type Questions

1. What is cyberspace? Describe the different types of cybercrimes briefly. Discuss the phases involved in planning cybercrime. Explain Cyber defamation briefly.
[WBUT 2016]

Answer:

1st Part:

Cyberspace is the online global environment that can be accessed through an increasing number of ICT device (like mobile phones, computers, gaming devices).

2nd Part:

When any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:

Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

Malicious Software: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

Child soliciting and Abuse: This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

3rd part:

Following are three major phases are involved in planning of cyber crime.

1. Reconnaissance

This is first step towards cyber attacks, it is one kind of passive attack. "Reconnaissance" means an act of reconnoitering. In this phase attacker try explore and gain every possible information about target.

In hacking world, Hacking start with "foot printing". Foot printing provide overall system structure, loop holes and exploration of those vulnerability. Attacker utilize this phase is to understand system, personal information, networking ports and services.

2. Scanning and scrutinizing

In this phase attacker collect validity of information as well as find out existing vulnerability. It is key phase before actual attack happen.

- **Port scanning:** Identify all ports and services (open / closed)
- **Network scanning:** Verify IP address and network information before cyber attacks.
- **Vulnerability scanning:** Checking loop hole in system.

Scrutinizing phase is also called enumeration.

- Validate user accounts and groups
- Find out list of network resource and how many network devices are shared?
- Different types of OS and application.

3. Launching an attack

Using step two information actual launching attack to gain system information. Once step two complete cyber attacker ready to launch attack.

1. Crack the password.
2. Exploit the privilege
3. Execute malicious command
4. Hide the files
5. Final but most important is cover the track.

4th part:

Cyber defamation is a new concept but the traditional definition of the term is defamation of a person through a new and a potential medium. The term defamation is used to define the injury that incurred to the reputation of a person in the eyes of a third person. The so called injury can be done by verbally or written, or by signs or visible representations. The intention of the person, making the defamatory statement against whom, must be to lower the reputation of that person in the eyes of the general public.

2. Is there any risk for cloud computing from cybercrime? Justify it. [WBUT 2016]

Answer:

One of the utmost concerns with cloud computing has always been the issue of data privacy and security. When a client decides to employ the use of cloud computing, the

data no longer belongs to the client alone. The vendor, or the service provider, stores the user's data on its own virtualized server and as such, vendors gain full access to the information available, confidential or not. Further, the servers are moved outside the traditional security perimeter making it easy for the reach of cyber criminals. This is a growing concern particularly when cloud computing stores sensitive data about customers.

Also, Cloud computing is often referred to as virtual, dynamic and borderless. These features of the cloud build a new layer of risk on the uncertainty over where sensitive data resides. The risk includes the wide distribution of information across different jurisdictions, each having different legal frameworks regarding data security and privacy. This makes it even more difficult to govern and regulate the information.

According to sources, cyber criminals can either manipulate the connection to the cloud or attack the data centre and cloud itself. However, there are no global standards or laws that regulate cloud computing against cyber criminals, yet. Governments and regulatory organizations need to recognize the potentials in cloud computing and take initiatives to create cloud specific laws and standards in order to make the cloud a safe and secure place for transactions.

3. What is blind SQL injection attack? How can it be prevented? [WBUT 2017, 2018]

Answer:

Blind SQL injection attack can be explained by describing a example which is as follows: Let's think of a blind man with a white cane who is trying to move around his house. How does he know that he is in his kitchen? He feels around for familiar things, while tapping with his cane for the same purpose. The moment his hands or cane come into contact with something familiar, he changes direction and starts tapping and feeling again. He repeats this process till he is in the kitchen. Various objects around the house told him that he was on the right track, although he himself couldn't see any of them.

The attacker will send query after query to the web application, which won't display a result at any point, but will give the attacker some response...to his input. It's now up to the attacker to look at the response and decide whether his query succeeded or not. Lets revisit the blind man example. There were only 2 possible responses that would make sense to the blind man. True OR False. There wasn't any other option. If he found a familiar object...TRUE, if not FALSE. Similarly the attacker has to form queries that will return TRUE or FALSE. If the query returns TRUE page1.html will be displayed and if FALSE error.html would be displayed. And he can continuously tweak his queries again and again till he retrieves whatever data he wants from the application.

2nd part: Methods of prevention:

Trust no-one: It should be assumed that all user-submitted data is evil and validate everything.

Don't use dynamic SQL when it can be avoided: used prepared statements, parameterized queries or stored procedures instead whenever possible.

Update and patch: vulnerabilities in applications and databases that hackers can exploit using SQL injection are regularly discovered, so it's vital to apply patches and updates as soon as possible.

Firewall: Consider a web application firewall (WAF) – either software or appliance based – to help filter out malicious data. Good ones will have a comprehensive set of default rules, and make it easy to add new ones whenever necessary. A WAF can be particularly useful to provide some security protection against a particular new vulnerability before a patch is available.

Reduce your attack surface: Get rid of any database functionality that you don't need to prevent a hacker taking advantage of it. For example, the xp_cmdshell extended stored procedure in MS SQL spawns a Windows command shell and passes in a string for execution, which could be very useful indeed for a hacker. The Windows process spawned by **xp_cmdshell** has the same security privileges as the SQL Server service account.

Use appropriate privileges: don't connect to your database using an account with admin-level privileges unless there is some compelling reason to do so. Using a limited access account is far safer, and can limit what a hacker is able to do.

Keep your secrets secret: Assume that your application is not secure and act accordingly by encrypting or hashing passwords and other confidential data including connection strings.

4. Differentiate direct and indirect losses for cyber crime. [WBUT 2018]

Answer:

a) Criminals take advantage of technology in many different ways. The Internet is a great tool for scammers and other miscreants, since it allows them to ply their trade while hiding behind a shield of digital anonymity. Cyber crime affects society in several different ways, both online and in the offline world. There are direct impacts on an individual but there are indirect effects also that affects the society. Some direct and indirect losses are:

Identity Theft: Becoming the victim of cyber crime can have long-lasting effects on your life. One common technique scammers employ is phishing, sending false emails purporting to come from a bank or other financial institution requesting personal information. If you hand over this information, it can allow the criminal to access your bank and credit accounts, as well as open new accounts and destroy your credit rating. This type of damage can take months or even years to fix, so protecting your personal information online is an important skill to learn.

Security Costs: Cyber criminals also focus their attacks on businesses, both large and small. Hackers may attempt to take over company servers to steal information or use the machines for their own purposes, requiring companies to hire staff and update software to keep intruders out. According to EWeek, a survey of large companies found an average expenditure of $8.9 million per year on cyber security, with 100 percent of firms surveyed reporting at least one malware incident in the preceding 12 months and 71 percent reporting the hijacking of company computers by outsiders.

Monetary Losses: The overall monetary losses from cyber crime can be immense. According to a 2012 report by Symantec, more than 1.5 million people fall victim to some sort of cyber crime every day, ranging from simple password theft to extensive monetary swindles. With an average loss of $197 per victim, this adds up to more than $110 billion dollars lost to cyber crime worldwide every year. As consumers get wise to traditional avenues of attack, cyber criminals have developed new techniques involving mobile devices and social networks to keep their illicit gains flowing.

Piracy: The cyber crime of piracy has had major effects on the entertainment, music and software industries. Claims of damages are hard to estimate and even harder to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of dollars per year. In response, copyright holders have lobbied for stricter laws against intellectual property theft, resulting in laws like the Digital Millennium Copyright Act. These laws allow copyright holders to target file sharers and sue them for large sums of money to counteract the financial damage of their activities online.

5. What do cyber criminal targets? **[WBUT 2018]**

Answer:

The industries most frequently targeted by hackers were as follows:

- 24% of breaches affected financial organizations
- 15% of breaches involved healthcare organizations
- 12% Public sector entities
- 15% Retail and Accommodation combined

It's obvious why cyber criminals would target financial and healthcare institutions, since these organizations deal very heavily in confidential information. Not surprisingly, the report found that 73% of breaches were financially motivated. Public sector is a rather interesting area, though some of this could be related to hacktivism, a type of cyber-crime that's been steadily on the rise. Retail and other types of accommodation organizations also handle a good deal of customer data, particularly as it relates to financial and personal identification material. The most important thing we'd like to point out is that even those organizations that fall outside the main categories of cybersecurity targets should operate under the assumption and expectation that they will likely also become a victim at some point. In other words, no company is safe. Small businesses to enterprise level, and organizations in every industry across the globe are all at risk of becoming a target of cyber-criminals. The best way to defend against these threats is to leverage the

power of technology that is available to you. Remember – attacks are coming in at an alarming rate and increasing in both volume and complexity. Likewise, tools like anti-virus software and firewalls are no match for sophisticated social engineering campaigns. A combination of employee education and automated cybersecurity incident response can provide an extra barrier of protection. It can also help with the most important step – remediation – getting critical systems back up and running quickly and mitigating damages.

6. Write short notes on Software Piracy. **[WBUT 2016]**

Answer:

According to some people "Software piracy is copying and use of Software without proper license from the developer. Similarly, simultaneous use of single user license software by multiple users or loading of a single user license software at multiple sites, also amounts to software piracy. Using trial version software for commercial gains is also piracy, Piracy is also can be punishable if you install an pirated software do your work and then delete this software from the machine with enough evidences to show the activity. Any Copyright infringement is the unauthorized use of copyrighted material in a manner that violates one of the copyright owner's exclusive rights, such as, the right to reproduce or to make derivative works that build upon it. For electronic and audio-visual media, such unauthorized reproduction and distribution of a copyrighted work is often referred to as piracy (however there is no legal basis for the term 'piracy')". There are different types of software piracy such as copying of copyrighted materials and using multiple copies of the same without license. Even if a person installs and uses the copy of the material and then removes it from the system, it will also be reported as software piracy. It includes installation on hard drive or on servers and clients with same version and no license. If a company illegally sells the product of another company without their permission or authorization with or without alteration of the original product can be considered as piracy.

Apart from getting caught and termed a three years of imprisonment, an offender can be charged with fine of Rs. 50,000 to Rs. 2 lakhs or both. The software can be corrupted or can be of low or degraded quality. The software can contain malwares or Trojans that can cause data theft or may lead to disabled system or infected network. Pirated software can cause reputation loss in a business and can end contracts with the clients.

7. What are the different types of software piracy? What are the risks involved in using pirated software? **[MODEL QUESTION]**

Answer: ***Refer Question No. 4 of Long Answer Type Questions.***

8. What do you mean by network intrusion? What are the methods of preventing network intrusion? **[MODEL QUESTION]**

Answer:

1st Part:

Network intrusion is unauthorized access to a remote network following the vulnerabilities of a network system. Attackers gain information about the organizations network by simply querying DNS servers, mail servers. Path and map of the network is

gathered by simple ICMP query tools. Names of active hosts and their IP addresses are gathered during the reconnaissance period. Using tools as fping, nslookup, traceroute, attackers gain as much of information from a network. A rejected reply will denote presence of a firewall will make the intruder alert. He can find out potential weaker systems and strictly restricted systems just by enquiring the domain. As for example, hosts under Active directory domain means they are subjected to strict security policies than local machines. Attackers will try to find out less secured system and make access to a network. Once they have access to the IP and the type of OS installed in the system they will try to find out open ports and installed applications. Using telnet remotely an attacker can hack into a remote switch, router or a host. If the servers and network can be compromised any remote login tools like terminal servers or remote desktop connection can be used to control the systems. Webservers are compromised at port 80. If the directory browsing option in IIS is not configured properly the hacker can download a whole lot of information. By changing port numbers the attacker can block, delete, change web site contents easily. Anyone with minimal hacking skills can use webspiders to filter email-IDs. Simple cookies and sessions can be used in fake websites to trace a user's activity, note down his username and password. Care should be taken by administrators while using share and tmp folders, because these are the mostly visited areas to gain any kind of information from the organization.

2nd Part:

Ways to tackle an intrusion are preemption, prevention, deterrence, deflection, and detection. Taking preventive measures like installing IDS and firewall can reduce intrusion. Taking possible measures when an ongoing intrusion has already been detected can reduce the intensity of the attack. Honey pots are used to lure attackers away from original systems to any other systems. There are two types of intrusion detection system network based intrusion detection (NID) and distributed intrusion detection (DID). Network Intrusion Detection system monitors any kind of packet for any unwanted or sudden increase of flow of traffic. It can identify any kind of remote login users and constantly watches for any malicious activity. Sometimes the direction of traffic gives an important indication of intrusion. Common analysis pattern includes substring match, protocol event detection. A very slow web server-can be an indication of DOS attack. Buffer overflow, worms, CGI scripts are the probable cause of any network intrusion. These are taken care in context based signature, protocol decode analysis, traffic pattern and heuristics analysis. In a distributed network intrusion detection system there are multiple IDS system installed in different parts of a network instead of a central server. This increases fault tolerance and performance during an attack.

9. Write short notes on the following: [MODEL QUESTION]
a) Forgery
b) Brute force attack
Answer:
a) Forgery:

Offences of computer forgery and counterfeiting have become rampant as it is very easy to counterfeit a document like birth certificate and use the same to perpetuate any crime.

The authenticity of electronic documents hence needs to be safeguarded by making forgery with the help of computers abs explicit offence punishable by law.

When a perpetrator alters documents stored in computerized form, the crime committed may be forgery. In this instance, computer systems are the target of criminal activity. Computers, however, can also be used as instruments with which to commit forgery. A new generation of fraudulent alteration or counterfeiting emerged when computerized color laser copiers became available. These copiers are capable of high-resolution copying, modification of documents, and even the creation of false documents without benefit of an original, and they produce documents whose quality is indistinguishable from that of authentic documents except by an expert.

These schemes take very little computer knowledge to perpetrate. Counterfeit checks, invoices and stationery can be produced using scanners, color printers, and graphics software. Such forgeries are difficult to detect for the untrained eye. It is relatively easy to scan a logo into a computer system and go from there.

b) Brute force attack:

Brute force attack uses dictionary and alphanumeric combination to break the password. Starting from a single word to combination of multiple words the brute force attack uses multiple attempts to make a successful entry to system. If enough time is given brute force attack is an effective password cracking method. Reverse brute force attack involves using a single password and a number of machines to access. To protect a password from a brute force a strong key is used. If the length of the cipher is n bits the worstcase time complexity for the algorithm to decode is $O(2^n)$. Tools like Dirb, webRoot uses brute force attack to gain access to web resources. Webservers are given strong passwords and sometimes they lock with multiple trial and error attempts to protect against brute force. Brute force is not effective for encrypted messages that use key length considerably of greater length.

CATEGORY OF CYBERCRIME

Multiple Choice Type Questions

1. Skimming means [WBUT 2015, 2018]
   a) Stealing ATM PIN information b) Stealing telephone information
   c) Stealing identity d) None of these
   Answer: (a)

2. Changing of raw data is known as [WBUT 2015, 2018]
   a) Salami attack b) Data diddling
   c) Forgery d) Web Jacking
   Answer: (b)

3. Pharming is used for [WBUT 2015, 2018]
   a) Data hiding b) Data alteration
   c) Hosts file poisoning d) File overriding
   Answer: (b)

4. Creating a fake website which looks very identical to a real website is called [WBUT 2016]
   a) sniffing b) spoofing c) hijacking d) phishing
   Answer: (d)

5. The attacker setup typo and matching domain names of the target and install websites for similar look and feel is [WBUT 2017]
   a) Phishing b) Pharming
   c) Backup theft d) None of these
   Answer: (b)

6. Sniffing is a technique used for [WBUT 2017]
   a) Attacks on computer hardware b) Attacks on computer software
   c) Attacks on operating system d) Attacks on wireless network
   Answer: (d)

7. The use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization is termed: [WBUT 2017]
   a) Cyberspace b) Cyber Stalking
   c) Pornography d) None of these
   Answer: (b)

8. What type of attack relies in the trusting nature of employees and the art of deception? [WBUT 2017]
   a) Social Engineering b) Fraud
   c) Phishing d) Dumpster Diving
   Answer: (a)

Short Answer Type Questions

1. What is Reconnaissance in the world of Hacking? [WBUT 2017]

Answer:
Reconnaissance means gathering of information without the knowledge of the person. It involves active and passive reconnaissance of the target machine. Gathering account information, identifying operating system, name and version of OS, getting IP and hostname of the machine. Passive information gathering may involve sniffing network traffic and filtering information from messages. Active reconnaissance is finding open ports, names by asking information from network although chances of getting caught are more.

2. What is Salami Attack? [WBUT 2017]

Answer:
A salami attack is when small attacks add up to one major attack that can go undetected due to the nature of this type of cyber crime. It also known as salami slicing/penny shaving where the attacker uses an online database to seize the information of customers, that is bank/credit card details, deducting minuscule amounts from every account over a period of time. These amounts naturally add up to large sums of money that is unnoticeably taken from the collective accounts.

3. Explain the difference between passive and active attacks. [WBUT 2017]

Answer:
Active attacks alter the system or network operations while passive attack gathers information about the system without altering the system. Active attack can involve infecting the system with virus or worms or can span upto deleting the entire hard drive. Normally passive attacks remain undetected. Active attack can flood the entire network with unnecessary packets and can render it slow while passive attack can sniff network packets without changing them. Passive attackers can know the presence of certain user accounts along with their password while active attackers use this information to render the system useless to the owner.

4. What is Cyber bullying? [WBUT 2017]

Answer:
Cyber bullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.
Examples of cyber bullying include mean text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

5. Define Depth of defence (DoD). [WBUT 2018]

Answer:
Depth of Defense (DoD) also called Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack. This multi-layered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors. Defense in Depth is commonly referred to as the "castle approach" because it mirrors the layered defenses of a medieval castle. Before you can penetrate a castle you are faced with the moat, ramparts, draw-bridge, towers, battlements and so on.

6. Differentiate Inside and Outside attack. **[MODEL QUESTION]**
Answer:
Inside attack takes place from inside of secured perimeters of an organization. Normally, Insider has more access to resources of the organization. This may include selling of confidential information of an organization to any competitor. Also time taken by an inside attacker is always less than an outside intruder. Outside attack takes place from remote site or from Internet. Resources gathered by the attacker is less than the previous case. Outside attack may bypass firewall and NAT.

Long Answer Type Questions

1. Define Cybercrime? Discuss about various types of Cybercrime. **[WBUT 2017]**
Answer:
Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access.
Different types of cyber crime are as follows:

1. Hacking
In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. They're usually technology buffs who have expert-level skills in one particular software program or language. As for motives, there could be several, but the most common are pretty simple and can be explained by a human tendancy such as greed, fame, power, etc. Some people do it purely to show-off their expertise – ranging from relatively harmless activities such as modifying software (and even hardware) to carry out tasks that are outside the creator's intent, others just want to cause destruction. Different techniques used by hackers are as follows:

a) SQL injections
b) Theft of FTP password.
c) cross site scripting.

2. Virus dissemination
Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. "Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term "worm" is sometimes used to mean selfreplicating "malware" (MALicious softWARE).

3. Logic bombs
A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as "time-bombs". For example, the infamous "Friday the 13th" virus which attacked the host systems only on specific dates; it "exploded" (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

4. Denial-of-Service attack
A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it.

5. Phishing
This a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing.

2. Define Cyber stalking. How stalking works? **[WBUT 2017]**
Answer:
1st part:
Refer to Question No. 3.c) of Long Answer Type Questions.

2nd part:

'Cyberstalking' refers to a particular type of stalking in which the stalker uses the internet and technology to harass the victim. This can involve anything from posting unwanted messages on a social networking site, to setting up websites with false or slanderous information about the victim, to trying to access the victim's personal information, such as bank accounts. Not a lot is known about the relationship between cyberstalking and physical stalking, but it is clear that as technology becomes more commonplace it is becoming a more common method of harassment for stalkers.

3. a) Describe the steps to reduce cyber risk.
b) Who are the cyber criminals? **[WBUT 2018]**

Answer:

a) Here are some suggestions to reduce the risk of an attack:

Tighten your current security system: Your system and all the software your organization uses offer guidelines for maximizing security controls that you should follow. Some are as simple as turning off unnecessary services or using the lowest privileges settings.

Use patches: All it takes is a tiny hole in your system for hackers to poke their way in. It's critical to run regular scans of your security system and all software to keep them updated with patches.

Protect outbound data: Just as you protect your system from incoming malware and bots with a firewall, you need to make sure certain data never leaves your system. It's important to focus on egress filtering, to prevent rogue employees or employees making honest mistakes from releasing sensitive data or malicious software from your network.

Raise awareness: It's important for everyone in the organization to be savvy and alert about security issues. This means watching for phishing scams sent through email and messaging apps that appear bonafide but are actually attempts to retrieve credentials or sensitive data or release malware into the system.

Be smart about passwords: Most organizations have password policies that address reuse and strength of user passwords. But one area that often is overlooked is the local administrator's PC password is the same as the password used on servers. It wouldn't take a hacker long to infiltrate the entire system and create internal and external havoc with that information.

Don't ignore physical security: Just as you wouldn't leave your car keys in the ignition of your car for thieves, you shouldn't leave ID badges, credit cards, personnel and

financial files, and cell phones/tablets lying around. Staff should be trained to keep these items on their person or locked away when not in use.

Encrypt data: All PCs and personal information stored in databases and on servers should be encrypted. This is the best way to protect against hackers gaining access to sensitive data.

Purchase a Cyber Insurance policy: If you do experience a cyber breach, a solid Cyber insurance policy will cover your losses and costs to repair the damage.

b) Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit. Cybercriminals are known to access the cybercriminal underground markets found in the deep web to trade malicious goods and services, such as hacking tools and stolen data. Cybercriminal underground markets are known to specialize in certain products or services.

4. Write short notes on the following:
a) Active attacks **[WBUT 2015]**
b) Hacking Cybercrime **[WBUT 2015]**
c) Cyber stalking **[WBUT 2015, 2016]**
d) Backdoor **[WBUT 2017]**

Answer:

a) Active attacks:

An active attack is an attempt "to alter system resources or affect their operation." It includes the falsification of data and transactions through such means as: (1) alteration, deletion, or addition; (2) changing the apparent origin of the message; (3) changing the actual destination of the message; (4) altering the sequence of blocks of data or items in the message: 5) replaying previously transmitted or stored data to create a new false message; or (6) falsifying an acknowledgement for a genuine message.

An active attack is "[a]n attack on the authentication protocol where the attacker transmits data to the claimant or verifier. Examples of active attacks include a man-in-the-middle, impersonation, and session hijacking."

b) Hacking Cybercrime:

In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking. The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and

hackers are most commonly associated with malicious programming attacks on the Internet and other networks.

There are many definitions of hacking. Here we will define hacking as identifying weakness in computer systems and/or networks and exploiting the weaknesses to gain access. An example of hacking is using by passing the login algorithm to gain access to a system. A hacker is a person who finds and exploits weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

- **Ethical Hacker (White hat):** A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration testing and vulnerability assessments.
- **Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
- **Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
- **Script kiddies:** A non-skilled person who gains access to computer systems using already made tools.
- **Hacktivist:** A hacker who use hacking to send social, religious, and political etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
- **Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers.

c) Cyber stalking:

Cyber stalking is the means by which a person is harassed over Internet, mobile phone, SMS, email. This can range from mere annoyance to serious crimes. According to some "Cyber stalking involves a disturbed obsession with the target, and a perverse desire to control that target in some way, even by attacking the target's family members." Cyber stalkers can interfere into someone's life by means of modern telecommunication medium. They choose any persons at random. Most of the potential target belong s to women, children, teenagers. Cyber stalkers can target an individual or a group. These kind of stalkers want ultimate submission from their victims. By hacking into someone's Internet activity such as email, Facebook or any social media they can even threat or

blackmail to the victims existence. These cyber bullies can even use children for offensive actions. Cyber stalking uses same techniques as the hackers but researches about victims likes and dislikes and uses against them. In India Criminal Law (Ammendment) Bill of 2013 includes law for handling cyber stalking. Section 66A of IT act deals with such kind of offenses. In section 354D - "anyone who monitors an individual's electronic communication and causes fear or distress is guilty of stalking, just as they are if they follow or attempt to contact them in the real world. The offender could get a fine and three years in jail." Although there is no organized law against cyber stalking still it is considered as a serious offense.

d) Backdoor:

A software bug or some undocumented software feature that a cracker leaves behind, after exploiting a system, to be able to reenter at a later point in time. Note, however, that back or trap doors can be a function of poor software design; that is, during its development, a programmer may have built in a software bug that was not removed when the software was put in production. The unwitting consumer who purchases the software becomes, in a sense, a target-in-waiting for a crack attack.

Back doors try to evade conventional clean-up methods by system administrators, such as ongoing changes to passwords, cleaning of the registry/configuration files, and the removal of suspicious software. Moreover, back doors tend to evade logging procedures; thus, even though every incoming connection to a system is supposedly logged, chances are that the back door provides a means of logging in without being logged. Finally, back doors are covert in the real sense that they hide well. Even if the system administrator scans a system looking for suspicious software, chances are the back door has used techniques capable of missing the scan.

One more essential point about back doors is this: Users of computer systems are, in large part, the cause of their own cracking misfortunes. Although most computers today allow BIOS passwords (the software that first runs when the computer starts) to be set to prevent the booting of the computer without an administrator's first typing the password, because so many users lose or forget their passwords, BIOSes frequently have back door passwords to permit the legitimate password to be set. Furthermore, much remote network equipment such as routers, switches, and dial-up banks have back doors for remote telnet.

4. What are the phases of hacking? **[MODEL QUESTION]**

Answer:

Hacking can be organized into five phases reconnaissance, scanning, gaining access, maintaining access and covering tracks.

Reconnaissance means gathering of information without the knowledge of the person. It involves active and passive reconnaissance of the target machine. Gathering account information, identifying operating system, name and version of OS, getting IP and hostname of the machine. Passive information gathering may involve sniffing network traffic and filtering information from messages. Active reconnaissance is finding open ports, names by asking information from network although chances of getting caught are more.

Reconnaissance phase is elaborated in scanning. The information gathered during first phase is used extensively here. User accounts, IP, hostnames, installed applications etc. are obtained in this phase. There are three types of scanning like port scanning, network scanning, and vulnerability scanning. In port scanning open ports and services are checked. In network scanning IP addresses are obtained. In vulnerability scanning, names and versions of OS and installed applications and their weaknesses are scanned. All starts with probing into network and looking for active hosts, once they are found IP address, hostname is obtained. Then OS finger printing is carried out looking for version and type of OS. Once it is determined installed applications and open ports are scanned. This can be done actively and passively. Scanning tools like TCP scan, TCP ping, UDP scan, SYN, XMAS tree scan tools use port scanning mechanism by setting FLAGS for normal communication and easily capture any open port. Hackers use these tools to find any response from open ports of unsuspecting hosts and establish connection like a normal machine. Properly installed and configured firewalls and intrusion detection system (IDS) can check active port scanning. One such scanning method is war dialing technique which is used to gain access to a remote modem and network. Hackers starts enumeration for obtaining user names, groups, services, network resources, NETBIOS names, file ownerships and permissions after scanning and gathering information.

In the third phase hackers uses this account information to gain access to the system. Gaining access includes Denial of Service attack (DOS), brute force attack etc. First they crack passwords either manually or using password cracking tools. Then they exploit the applications. Finally they hide the applications, create backdoors to maintain access to the system anonymously. Last phase of maintaining continued access is by covering all the tracks and disabling the firewall. They normally delete the system log files and any related information that can grow any suspicion.

5. What is buffer overflow? Explain various types of buffer overflow. How to minimize buffer overflow? **[MODEL QUESTION]**

Answer:

1st Part:

A buffer overflow occurs when more data are written to a buffer than it can hold. The excess data is written to the adjacent memory, overwriting the contents of that location and causing unpredictable results in a program. Buffer overflows happen when there is improper validation (no bounds prior to the data being written. It is considered a bug or weakness in the software.

2nd Part:

A buffer overflow is an exploit that takes advantage of a program that is waiting on a user's input. There are two main types of buffer overflow attacks: stack based and heap based. Heap-based attacks flood the memory space reserved for a program, but the difficulty involved with performing such an attack makes them rare. Stack-based buffer overflows are by far the most common.

In a stack-based buffer overrun, the program being exploited uses a memory object known as a stack to store user input. Normally, the stack is empty until the program requires user input. At that point, the program writes a return memory address to the stack and then the user's input is placed on top of it. When the stack is processed, the user's input gets sent to the return address specified by the program.

3rd Part:

A buffer overflow attack requires two things. First, a buffer overflow must occur in the program. Second, the attacker must be able to use the buffer overflow to overwrite a security sensitive piece of data (a security flag, function pointer, return address, etc.).
If we want to prevent buffer overflows completely we must stop one of these two things, i. e. either:

1. Prevent all buffer overflows or
2. Prevent all sensitive information from being overwritten

Both these solutions are costly in terms of efficiency and many programs therefore settle for a partial goal, such as:

- Prevent use of dangerous functions: gets, strcpy, etc.
- Prevent return addresses from being overwritten
- Prevent data supplied by the attacker from being executed (stops the attacker from jumping into his own buffer)

There are several possible levels where a defence mechanism can be inserted. At the language level we can make changes to the C language itself to reduce the risk of buffer overflows. At the source code level we can use static or dynamic source code analyzers to

check our code for buffer overflow problems. At the compiler level we can change the compiler so that it does bounds checking or protects certain addresses from overwriting. At the operating system level we can change the rules for which memory pages that should be allowed to hold executable content.

CYBERCRIME MOBILE & WIRELESS DEVICES

Multiple Choice Type Questions

1. Sniffing is a technique used for [WBUT 2015]
   a) Attacks on computer hardware
   b) Attacks on computer software
   c) Attacks on operating system
   d) Attacks on wireless network

Answer: (d)

2. The name of the virus that will erase all IMEI and IMSI information from both your phone and SIM card is [WBUT 2016, 2018]
   a) TDL-4 b) XALAN c) SCA d) MDEF

Answer: (b)

3. Which one is true? [WBUT 2016]
   a) bluesnarfing is claimed to be much more serious than bluejacking
   b) bluejacking is claimed to be much more serious than bluesnarfing
   c) bluejacking is claimed to be same serious as bluesnarfing
   d) none of these

Answer: (a)

4. This is a program in which malicious or harmful code is contained inside apparently harmless programming or data [WBUT 2017]
   a) War dialer
   b) Spam trap
   c) Trojan horse
   d) Email

Answer: (c)

5. In cyber law terminology 'DDoS' means [WBUT 2017]
   a) Distributed Denial of Service
   b) Disc Operating System
   c) Distant Operator Service
   d) None of these

Answer: (a)

6. WEP stands for what? [MODEL QUESTION]
   a) Wireless Encryption Protocol
   b) Wired Equivalent Privacy
   c) Wireless Encryption Privacy
   d) Wired Encryption Protocol

Answer: (b)

7. What makes WEP crackable? [MODEL QUESTION]
   a) Same key used for encryption and authentication
   b) Length of the key
   c) Weakness of IV
   d) RC4

Answer: (c)

8. Which form of encryption does WPA use? [MODEL QUESTION]
a) AES b) TKIP c) LEAP d) Shared key
Answer: (b)

9. In cyber law terminology 'DOS' means: [MODEL QUESTION]
a) Denial of Service b) Disc Operating System
c) Distant Operator Service d) None of these
Answer: (a)

10. Which form of authentication does WPA2 use? [MODEL QUESTION]
a) Passphrase only b) 802.1x/EAP/RADIUS
c) Passphrase or 802.1x/EAP/RADIUS d) AES
Answer: (c)

11. What is cryptography? [MODEL QUESTION]
a) The study of computer science
b) The study of mathematics
c) The study of encryption
d) The creation of encryption algorithms
Answer: (c)

12. Hacking web server & taking control on another person's website is called as Web..... [MODEL QUESTION]
a) Spoofing b) Hijacking
c) Spamming d) None of these
Answer: (a)

13. What is the process of replacing some characters with others in an encryption key? [MODEL QUESTION]
a) Transposition b) Subtraction
c) Substitution d) Translation
Answer: (c)

14. Data encrypted with the server's public key can be decrypted with which key? [MODEL QUESTION]
a) Server's public key b) Server's private key
c) Client's public key d) Client's private key
Answer: (d)

15. The practice of making a transmission appears to come from an authorized user. [MODEL QUESTION]
a) Hacking b) Spoofing
c) Spamming d) Spamdexing
Answer: (b)

16. Which type of encryption is the fastest to use for large amounts of data? [MODEL QUESTION]
a) Symmetric b) Public
c) Private d) Asymmetric
Answer: (a)

Short Answer Type Questions

1. Name different virus, worms that can affect portable devices like laptop, mobile phones. [MODEL QUESTION]
Answer:
Virus: Duts, Cdropper, Fontal, 3gexplorer
Worms: IKee, Lasco
Trojans: Skulls, Gingermaster, DroidKungFu, MOSQIT-A
Malwares: Cabir, Commwarrior

2. What are the different types of virus found in hosts? [MODEL QUESTION]
Answer:
Different viruses are programmed to achieve the purpose without getting detected by anti-virus softwares.

- ***Polymorphic viruses:*** These viruses encrypt the code in a different way with each infection and can change to different forms to try to evade detection.
- ***Stealth viruses:*** Modifies time and date stamp of the file and hides the normal virus characteristics so as to prevent the virus from being noticed as a new file.
- ***Fast and slow infectors:*** These bypasses detection by anti-virus softwares by infecting very quickly or very slowly.
- ***Sparse infectors:*** These viruses infect only selected applications.
- ***Armored viruses:*** To prevent detection they are normally encrypted.
- ***Multipartite viruses:*** Create multiple infections.
- ***Cavity (space-filler) viruses:*** These viruses attach to empty areas of files.
- ***Tunneling viruses:*** These are tunneled through different protocol to allow it to pass through a firewall.
- ***Camouflage viruses:*** These viruses appear to be another program.
- ***NTFS and Active Directory viruses:*** These specifically attack the NT file system or Active Directory on Windows systems.

3. What are the phases of Bluetooth connection and what are the types of attack in Bluetooth device? [MODEL QUESTION]
Answer:
A device operates in "passive mode", meaning that it is **listening** to the network. The master device sends an inquiry request to all devices found within its range, one must run an inquiry to try to **discover** the other. Any device listening for such a request will respond with its address, and possibly its name and other information. **Paging** is the process of forming a connection between two Bluetooth devices. Before this connection

can be initiated, each device needs to know the address of the other. After a device has completed the paging process, it enters the **connection** state.

Discovery: During discovery phase, Bluescanner, Bluesniff, these tools gathers as much possible information from a device such as device identification, type and version of OS, even hidden devices and all its technical specifications. This is called reconnaissance phase. Some tools can send unwanted spam messages at the discovery phase. This is called Bluejacking. Model, version or the entire blueprint of the target device can be obtained. Sending anonymous message to the target device is also one way of Bluetooth hacking. Some softwares are designed to push and pull data as OBEX pull attack. This process is called BlueSnarfing.

Breaking and entering: After information gathering, an attacker can obtain phone records,photos,music files, important information like Redsnarf and Bloover. In Bluebugging electronic business card transfer process can be used to add the hacker's device as a trusted device without the user's knowledge. This trusted status can then be used to take control of the phone and the data within.

4. Classify attacks on mobile devices. **[MODEL QUESTION]**

Answer:

Mobile device attacks can be split into four main categories:

***OS Attacks*:** Loopholes in operating systems create vulnerabilities that are open to attack. Vendors try to solve these with patches.

***Malware or virus Attacks*:** There has been a constant rise in malware for mobile devices. The focus is on deleting files and rendering the system unusable.

***Mobile App Attacks*:** Poor coding and improper development creates loopholes and compromises security.

***Communication Network Attacks*:** Communications such as Bluetooth and Wi-Fi connections make devices vulnerable.

5. What is Distributed system for wireless environment? **[MODEL QUESTION]**

Answer:

When two or more mobile stations are connected together via peer to peer connection they form basic service set(BSS). When more than one BSS are connected via access point or base stations and routers that is called distributed system.

6. a) What is Denial of Service attack? **[MODEL QUESTION]**

b) What are the different types of Denial of Service attacks?

Answer:

a) A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a

distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target.

b) Different mechanisms are used by different types of denial service attacks.

Flood attacks

The flood attack is quite a simple concept where the attackers send a large number of requests which cannot be handled by a server. This is done in relentless way unless the server gets buckled and then gives up to the attacker. The server can again go back to normal operation when the attack ends. These attacks are quite common as they can be easily executed easily. You can easily get access to programs that can be used for such attacks. There are different forms of flood attacks. These include:

SYN flood- In this type of the flood attacks, SYN requests are sent repeatedly by the attackers, which the target ultimately accepts. The server can slow down or even get crashed due to such attacks. It involves the exchange of the ACK and the SYN messages.

Ping flooding- This is a process in which the target servers are flooded with ICMP echo requests. In this attack, the usage of bandwidth increases greatly. This eventually slows down or stops the operations of the server.

Smurf attack- The ping messages are pinged by the surf attacks to the broadcast IP addresses. If there is any response from the target machine and ICMP echo requests are broadcasted, then the attack spreads to a large number of machines. This problem has been almost fixed by the modern routers and this type of attack is now less common.

UDP attacks- In this kind of flood attack, high volume of UDP packet are sent for occupying the servers. This prevents the legitimate clients from getting access to the server. In this process, the attacker needs to find a free UDP port.

Logic attacks

The vulnerabilities of a network are exploited by this type of denial of service attacks. The intrusion method is quite different from the flood attacks. These attacks depend on the non standard traffic and the security holes in a system are exploited. These attacks locate the discoverable weakness of the network and then use them.

7. What are the phases of association between mobile station and access point? **[MODEL QUESTION]**

Answer:

A mobile station can receive five types of services provided by AP and those are association, reassociation, disassociation, distribution, and integration.

A station must affiliate itself with the BSS infrastructure if it wants to use the LAN. This is done by associating itself with an access point. A station can only be associated with one AP.

Reassociation allows the station to switch its association from one AP to another. Both association and reassociation are initiated by the station. Disassociation is when the association between the station and the AP is terminated. This can be initiated by either party. In case of mobile station moving from one region under AP to another handoff takes place. Distribution is simply getting the data from the sender to the intended receiver. The message is sent to the local AP, then distributed through the DS to another AP that the recipient is associated with. Integration is when the output AP is a portal.

8. What is SSID? **[MODEL QUESTION]**

Answer:

The Service Set Identifier (SSID), 48 bit, is used for wireless network in infrastructure mode and also in ad-hoc mode. The SSID is a configurable client identification that allows clients to communicate to a particular base station. Only clients systems that are configured with the same SSID as the AP can communicate with it. SSIDs provide a simple password arrangement between base stations and clients.

9. What is authentication and encryption? **[MODEL QUESTION]**

Answer:

Wireless devices deploy security using two methods, authentication and encryption. Authentication refers to the verification of client system. In the infrastructure mode, authentication is established between an AP and each station. Wireless encryption services must be the same on the client and the AP for communication to occur. Encryption algorithm is used so that other 802.11 users cannot eavesdrop on LAN traffic.

10. What are the security implementation for a wireless device? **[MODEL QUESTION]**

Answer:

Security as implemented in different layers are enlisted below.

Layer	Security protocol
Layer 1	Physical security against theft, loss or damage by PIN code or SIM lock, enabling tracking or hosting alert signal.
Layer 2	WEP,WPA, WPA2,802.11i
Layer 3	IPSec,SSL VPN
Upper layers	SSH,HTTPS,FTP(SSL)

11. Difference between WEP and WPA **[MODEL QUESTION]**

Answer:

	WEP	WPA
Secure and recommended	No	Yes
Stands for	Wired Equivalent Privacy	Wi-Fi Protected Access
What is it?	A security protocol for wireless networks introduced in 1999 to provide data confidentiality comparable to a traditional wired network.	A security protocol developed by the Wi-Fi Alliance in 2003 for use in securing wireless networks; designed to replace the WEP protocol.
Methods	Through the use of a security algorithm for IEEE 802.11 wireless networks it works to create a wireless network that is as secure as a wired network.	Works through the use of an AES based encryption algorithm for IEEE 802.11 wireless networks to ensure a secured wireless connection. Typically uses the TKIP protocol.
Uses	Wireless security through the use of an encryption key.	Wireless security through the use of a password.
Authentication method	Open system authentication or shared key authentication	Authentication through the use of a 64 digit hexadecimal key or an 8 to 63 character passcode.

12. Why WEP generally not used? **[MODEL QUESTION]**

Answer:

WEP is not a strong encryption key. It uses same concept as used in wired encryption algorithms. However, initialization vector of WEP is a 24-bit field sent in the cleartext portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes. Reuse of the same IV produces identical key streams for the protection of data, and because the IV is short, it guarantees that those streams will repeat. The fact that an eavesdropper knows 24-bits of every packet key, combined with a weakness in the RC4 key schedule, leads to a successful analytic attack that recovers the key after intercepting and analyzing only a relatively small amount of traffic. MAC protocol uses a non-cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledges packets that have the correct checksum. The combination of non-cryptographic checksums with stream ciphers often introduces vulnerabilities.

13. What are the different types of attack associated with WEP and name few softwares for this? **[MODEL QUESTION]**

Answer:

Brute force attack and FMS attack is used to break the encryption code of WEP. Tools used for WEP attack are Airsnort, Aircrack, WEPcrack.

14. What are the vulnerabilities of WPA and WPA2? **[MODEL QUESTION]**

Answer:

WPA and WPA2 are susceptible to dictionary attacks.

Long Answer Type Questions

1. What are the different kinds of attacks on mobile/cell phones? Explain with examples. **[WBUT 2017]**

Answer:

Attacks Description:

Browser exploits: These exploits are designed to take advantage of vulnerabilities in software used to access websites. Visiting certain web pages and/or clicking on certain

hyperlinks can trigger browser exploits that install malware or perform other adverse actions on a mobile device.
For example, an attacker could use the mozilla_compareto module -- a Metasploit module to have their system act as a Web server. When an unsuspecting victim connects to the evil attacker's site, it launches an attack against the browser itself, creating a shell on the target system for the malicious hacker.

Data interception: Data interception can occur when an attacker is eavesdropping on communications originating from or being sent to a mobile device.
Electronic eavesdropping is possible through various techniques, such as (1) man-in-the-middle attacks,(2) WiFi sniffing etc.
for example, a coworker may overhear your dinner plans because your speaker phone is set too loud. The opportunity to overhear a conversation is coupled with the carelessness of the parties in the conversation.

Keystroke logging: This is a type of malware that records keystrokes on mobile devices in order to capture sensitive information, such as credit card numbers.
For example, using an encrypted link (i.e., HTTPS rather than HTTP) to access bank or e-mail online is a good way to encrypt the transmission of private information as it flows across the Internet. However, it's vital to remember that the encryption process doesn't take place until the information leaves the machine. This creates a vulnerability that some people may not be aware of — keystroke logging. Software keystroke loggers, such as CyberSpy Software, intercept data as the user types. They typically store that data in hidden encrypted files on the user's computer.

Malware: Malware is often disguised as a game, patch, utility, or other useful third-party software application. Malware can include spyware, viruses, and Trojans. Once installed, malware can initiate a wide range of attacks and spread itself onto other devices. Examples: adware, bots, bugs, rootkits, spyware, Trojan horses, viruses, and worms.

Unauthorized location tracking: Location tracking allows the whereabouts of registered mobile devices to be known and monitored.

Network exploits: Network exploits take advantage of software flaws in the system that operates on local (e.g., Bluetooth)or cellular networks. Network exploits often can succeed without any user interaction, making them especially dangerous when used to automatically propagate malware. With special tools, attackers can find users on a Wi-Fi network, hijack the users' credentials, and use those credentials to impersonate a user online.

Phishing: Phishing is a scam that frequently uses e-mail or pop-up messages to deceive people into disclosing sensitive information.

Spamming: Spam is unsolicited commercial e-mail advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malicious software. Spam can appear in text messages as well as electronic mail.

Spoofing : Attackers may create fraudulent websites to "spoof" legitimate sites and in some cases may use the fraudulent sites to distribute malware to mobile devices.

Zero-day exploit: A zero-day exploit takes advantage of a security vulnerability before an update for the vulnerability is available. example: Windows: In May, Google security engineer Tavis Ormandy announced a zero-day flaw in all currently supported releases of the Windows OS. According to his claim, the troubled code is more than 20 years old, which means "pre-NT".

2. a) What is information? What information should you protect? What are the risks to your information and how much risk can you accept?
b) How can you ensure that you have the best possible understanding of the threat to your business?
c) How do you embed risk management within your computer?
[WBUT 2018]

Answer:
a) Information is data that is (1) accurate and timely, (2) specific and organized for a purpose, (3) presented within a context that gives it meaning and relevance, and (4) can lead to an increase in understanding and decrease in uncertainty. Information is valuable because it can affect behavior, a decision, or an outcome. Protecting sensitive information is the end goal of almost all IT security measures. Sensitive information refers to privileged or proprietary information that only certain people are allowed to see and that is therefore not accessible to everyone. If sensitive information is lost or used in any way other than intended, the result can be severe damage to the people or organization to which that information belongs. Some examples of sensitive information are as -
personal information, including Social Security Number and bank credentials, trade secrets, system vulnerability reports, pre-solicitation procurement documentation, computer security deficiency reports.
Its better to handle the risk to information at beginners stage but one can keep ignoring it till it starts indulging in damaging or mess up the sensitive and private information.

b) SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats) is a method of assessing a business, its resources, and its environment. Doing an analysis of this type is a good way to better understand a business and its markets, and can also show potential investors that all options open to, or affecting a business at a given time have been thought about thoroughly. The traditional approach to completing SWOT is to produce a blank grid of four columns— one each for strengths, weaknesses, opportunities, and weaknesses—and then list relevant factors beneath the appropriate heading. Don't worry

if some factors appear in more than one box and remember that a factor that appears to be a threat could also represent a potential opportunity. This process helps in business and also in finding out the upcoming threats.

c) The process of embedding looks very simple, define the thought process and way of documenting it, then train as many people as possible to do it. The difficult part is to convince people that this is a good use of their time. If you accept that embedding is more complicated than this, the process of embedding becomes:

- Identify risk and uncertainty management activities (a.k.a. controls) already operating, recognizing the wide range of different techniques and thought processes that can be used.
- Improve and refine them where appropriate.
- Ensure the activities generate evidence of having operated and of their own effectiveness (e.g., performance metrics, independent reports) to minimize the need for audit and control risk self assessment.

3. a) What would happen to the business if one of your risks becomes a reality?
b) Describe CKC in details.
c) What is criminal revenue?

[WBUT 2018]

Answer:

a) Making a strategy for risk management can involve more than just deciding whether to accept the risk or not. If your business is part of a bigger supply chain that involves retailers, distributors or primary producers, you can spread the risk across a number of areas. By spending time and resources on your risk management strategy, you'll provide a safe workplace and reduce the chances of negative impacts on your business. If a risk has already turned to reality then one need to To evaluate the risk, one should compare the level of risk for various events against your risk criteria (find out how to set risk criteria when you design a risk management plan). You should also check if existing risk management methods are enough to accept the risk. Sometimes businesses choose to accept risks and not spend any resources on avoiding them for the following reasons:

- The cost of treatment is much higher than the potential results of the risk.
- The risk level works out to be very low.
- The benefits of taking the risk greatly outweighs the possible damage.

b) The cyber kill chain is an industry-accepted methodology for understanding how an attacker will conduct the activities necessary to cause harm to your organization. An effective understanding of the cyber kill chain will greatly assist the information security professional in establishing strong controls and countermeasures, which will serve to protect their organization's assets.

Stage 1: Reconnaissance:-The first stage of the cyber kill chain is reconnaissance. In this stage, the attacker is assessing the target from outside of the organization from both a

technical and non-technical perspective. In this stage, the attacker is working to determine which targets will return the most benefit for the resources expended in exploiting the target's information systems. The attacker will be looking for information systems with few protections or exploitable vulnerabilities.

Active Information Gathering: -With active information gathering and reconnaissance, the attacker actively interacts with the target system. An example of active information gathering and reconnaissance is port scanning, where the attacker works to enumerate open ports. The goal of the attacker, in this case, is to uncover ports that are vulnerable to exploitation and therefore would provide a means for the attacker to access the target system.

Passive Information Gathering:- Passive information gathering and reconnaissance attempt to obtain information related to the target information systems without engaging those information systems directly.

2. Weaponization:-The second stage of the cyber kill chain is weaponization. During weaponization, the threat actor develops malware specifically crafted to the vulnerabilities discovered during the reconnaissance phase of the cyber kill chain. Based on the intelligence gathered in the reconnaissance phase, the attacker will tailor their toolset to meet the specific requirements of the target network.

3. Delivery:- The third stage in the cyber kill chain, delivery, involves transmitting the APT code from the attacker to the target information system for exploitation. Based on current research and analysis, a network attack is most likely to originate from a spear-phishing attack targeting an internal employee of the organization.
A carefully researched and crafted spear-phishing campaign against an organization based on information gathered during the reconnaissance phase would result in the organization's employees executing the APT malware code on their information systems. The spear phishing message will most likely contain an attachment such as a Microsoft Word or an Adobe PDF document. The attachment would contain code that, when executed, would result in the APT gaining a foothold on the organizational network.
Another available opportunity for exploitation is examining the organizational public IP space for mismanaged servers. A lack of cyber hygiene practices within an organization's network could result in vulnerable production systems.

4. Exploitation:-During the exploitation phase, the APT malware code is executed on the target network through remote or local mechanisms, taking advantage of discovered vulnerabilities to gain superuser access to the targeted organizational information system.

5. Installation:-Once the exploitation of the system has been successful, the APT malware code will install itself onto the targeted information system. At this point, the APT malware will begin to download additional software if network access is available. This allows the delivery payload to remain small and undetectable.

The small size of the malware in this example would have limited functionality. Therefore, the APT will download additional components to have better control of the exploited information systems and to penetrate further into the target organization's network.

6. **Command And Control:-** Command and control is the sixth phase of the cyber kill chain. Command and control, also known as C2, is when the attacker has put in place their management and communication APT code onto to the target network. This software allows the attacker to fully manage the APT code in the environment and allows the attacker to move deeper into the network, exfiltrate data and conduct destruction or denial of service operations.

7. **Actions On Objectives:-** The actions and objectives of the APT are dependent on its specific mission. The APT could be focused on data exfiltration, denial of service or destruction.

In the case of data exfiltration, the APT may be interested in organizational proprietary data such as engineering designs or employee and customer Personally Identifiable Information (PII). In the case of a denial of service, like the Ukrainian power outage of December 2015, the APT may disable a key component of the organization's infrastructure to temporarily disrupt services.

Finally, in the case of destruction, an APT like the Stuxnet worm may seek to operate industrial control systems outside of their manufacturer specifications, resulting in catastrophic failure.

c) Internal Revenue Service. Criminal Investigation (IRS-CI) investigates potential criminal violations of the U.S. Internal Revenue Code and related financial crimes in a manner intended to foster confidence in the tax system and deter violations of tax law. While other federal agencies[which?] also have investigative jurisdiction for money laundering and some bank secrecy act violations, the Internal Revenue Service (IRS) is the only federal agency that can investigate potential criminal violations of the Internal Revenue Code. The Criminal Investigation strategic plan is composed of four interdependent programs: Legal Source Tax Crimes; Illegal Source Financial Crimes; Narcotics Related Financial Crimes; and Counterterrorism Financing. These four programs are mutually supportive, and encourage utilization of all statutes within CI's jurisdiction, the grand jury process, and enforcement techniques to combat tax, money laundering and currency crime violations. Criminal Investigation must investigate and assist in the prosecution of those significant financial investigations that will generate the maximum deterrent effect, enhance voluntary compliance, and promote public confidence in the tax system.

4. What is the methodology for assessing the impact of IP theft? **[WBUT 2018]**

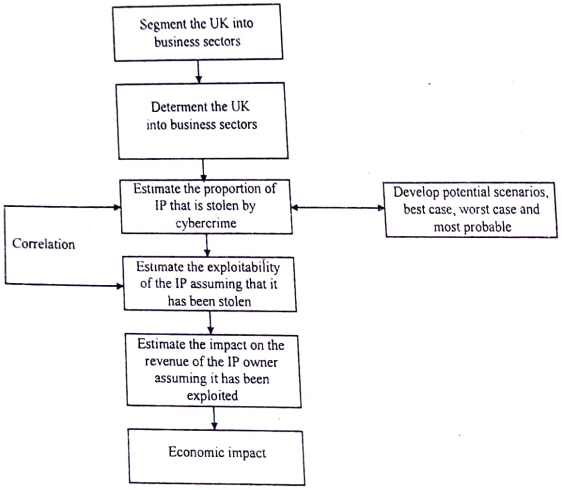
Answer:

In developing our methodology for measuring the impact of IP theft, we have made assumptions about:

1. the total amount of R&D spend in each UK business sector (using up-to-date and credible data where it is available)
2. the average estimated return on investment that each UK business sector would expect from its R&D spend (to estimate the true value of the IP and not just the current market worth)
3. the average estimated level of IP 'exploitability' for cyber criminals (recognising that not all IP can be easily exploited)
4. the level of economic impact that IP exploitation would have on the UK economy (recognising that, even though it may be exploited, stolen IP does not necessarily lose all its residual value).

In the absence of robust estimates for actual levels of IP theft, our methodology assumes that the 'business model' cyber criminals adhere to for IP theft follows the same principles of any other type of business46 : the desire to maximise financial gain and minimise business risk. For IP theft by cyber criminals, our methodology attempts to determine the means, motive and opportunities presented to potential attackers.

It recognizes that the nature of IP generated in different business sectors is different and has different levels of exploitability and economic impact if it is stolen. Therefore, the method used by our study to calculate the costs to the UK economy of IP theft through cyber crime started with the value added to the UK economy by each industry sector as given in the Blue Book47. We then estimated the fraction that was attributable to IP within the industry. This calculated the subsequent economic value. Once the economic value of the IP had been derived, estimates were made of the probability of cyber theft for each industry sector using three point estimates, with the subsequent IP exploitability and revenue impact also estimated as a percentage. The results give an estimate of the value lost to the economy due to IP theft across the different industry sectors. The methodology is illustrated below:



5. What are the steps to protect your mobile phone from cyber crime? **[WBUT 2018]**

Answer:

Few small steps to protect your mobile phone from cyber crime are:-

Set a passcode: Set a password on your mobile device so that if it is lost or stolen, your data is more difficult to access. One of the the biggest security risks is old fashioned carelessness. Data is most often taken from mobile phones when they're lost or stolen and aren't protected by a password. It's an open invitation for thieves to go rummaging around.

Check your phone bill: Be on the lookout for unusual behaviors on your phone, which could be a sign that it is infected. These behaviors may include unusual text messages, suspicious charges to the phone bill, or suddenly decreased battery life.

Download from trusted sources: Before downloading an app, conduct research to make sure the app is legit. This includes checking reviews, confirming the legitimacy of the app store and comparing the app sponsor's official website with the app store link to confirm consistency. Many apps from untrusted sources contain malware that once installed – can steal information, install viruses, and cause harm to your phone's contents.

Backup and secure your data: You should backup all of the data stored on your phone such as your contacts, documents and photos. These files can be stored on your computer,

on a removal storage card, or in the Cloud. This allows you to restore the information to your phone should it be lost, stolen or otherwise erased.

Understand app permissions before accepting them: You should be cautious about granting applications access to personal information on your phone or otherwise letting the application have access to perform functions on your phone. Make sure to also check the privacy settings for each app before installing.

Wipe data on your old phone before you donate, resell or recycle it: To protect your privacy, completely erase data off of your phone and reset the phone to its initial factory settings.

Make sure you have a security app: Download a mobile security app that scans every app you download for malware and spyware and can help you locate a lost or stolen device. Also, make sure the security app protects from unsafe websites.

Report stolen phones: If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider. This provides notice to all the major wireless service providers that the phone has been stolen and will allow for remote "bricking" of the phone so that it cannot be activated on any wireless network without your permission.

6. Write short notes on the following::

a) Mobile viruses. **[WBUT 2015]**

b) WAP kitting and WAP jacking **[WBUT 2017]**

Answer:

a) A mobile virus is an electronic virus that targets mobile phones or wireless-enabled Pads.

As wireless phone and PDA networks become more numerous and more complex, it has become more difficult to secure them against electronic attacks in the form of viruses or other malicious software.

Some of the common mobile viruses are as follows:

Cabir: Infects mobile phones running on Symbian OS. When a phone is infected, the message 'Caribe' is displayed on the phone's display and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals.

Duts: A parasitic file infecter virus and is the first known virus for the PocketPC platform. It attempts to infect all EXE files in the current directory (infects files that are bigger than 4096 bytes)

Skulls: A trojan horse piece of code. Once downloaded, the virus, called Skulls, replaces all phone desktop icons with images of a skull. It also will render all phone applications, including SMSes and MMSes useless

Commwarrior: First worm to use MMS messages in order to spread to other devices. Can spread through Bluetooth as well. It infects devices running under OS Symbian Series 60. The executable worm file once launched hunts for accessible Bluetooth devices and sends the infected files under a random name to various devices.

b) WAPjacking

WAPjacking changes the settings of existing firmware to bring some benefit to the attacker. While configurable parameters vary among router models and manufacturers, most routers destined for the home market allow users to select a DNS server, enable administrative access via the Internet, log usage statistics, send usage reports to an email address and control the traffic routing.

Changing the DNS server to one controlled by the attacker is one way to quietly misdirect legitimate link requests to fraudulent hosts. DNS poisoning, or pharming, is more efficient than phishing in bringing victims to phony websites because clients navigate to the sites by their own initiative, not at the behest of an email. Pharming attacks withstand the scrutiny of many anti-phishing tools because their analysis assumes correct domain name resolution. Stealing authentication credentials such as username and password becomes a trivial task. For example, when www.mybank.com is requested by the client's web browser, the wireless router asks the malicious DNS server for the IP address and receives the address of a duplicate host that is controlled by the attacker. The victim's login results in the disclosure of website credentials; most commonly this means username and password, however man-in-the-middle attacks will discover personalized data in more elaborate login processes such as PassMark's SiteKey. Alternatively, the malicious DNS could profile traffic. Instead of fraudulently resolving a domain name, it could simply log all DNS requests. The log is an aggregate profile of which domains their clients visit and when they visit them. For home routers, the space of clients is small, so the loss of precision due to aggregation is limited. In conjunction with a known email address, this behavioral profiling makes spear phishing much easier. This sort of attack could also be employed by stalkers or burglars to help identify when their victims are home.

WAPkitting:

In a WAPkitting attack, external software seizes control from the router's firmware. While most easily accomplished by exploiting open administrative access, WAPkitting can theoretically proceed by more traditional means such as buffer overflow. Almost all wireless home routers are based on integrated systems on chip (SoC) which combine a general purpose microprocessor, RAM, a small amount of permanent storage, a wireless network interface and a wired network switch. An embedded operating system coordinates the execution of the firewall, routing, domain name resolution and other

services. Like a desktop computer, these operating systems are vulnerable to malware, including total subversion. The web administration page on most home wireless routers is not only a configuration interface, but also a firmware replacement interface. None of the widely deployed systems known to us limit the upgrades to digitally signed firmware with WAPkits (since they are not signed by the manufacturer), it would not seal vulnerabilities due to software errors.

3. Name different virus, worms that can affect portable devices like laptop, mobile phones. [MODEL QUESTION]

Answer:

***Virus*:** Duts, Cdropper, Fontal, 3gexplorer
***Worms*:** IKee, Lasco
***Trojans*:** Skulls, Gingermaster, DroidKungFu, MOSQIT-A
***Malwares*:** Cabir, Commwarrior

4. What are the security challenges posted by mobile devices?[MODEL QUESTION]

Answer:

Cracking encryption and authentication mechanisms: The SSID is usually sent in the clear in a beacon packet. Most APs allow the WLAN administrator to hide the SSID. However, this isn't a robust security mechanism because some tools can read the SSID from other packets such as probe and data packets. Once decrypted the hackers can steal information, corrupt data.

Eavesdropping or sniffing:

Sniffing can be used to gather information while footprinting and reconnaissance.

Denial of Service:

Network can be flooded with DOS (or DDOS) attack.

AP masquerading or spoofing:

This kind of attack is performed as man-in-the-middle attack. Here attackers use rouge AP and act as legitimate base stations while connecting with mobile stations and also with the wired network. These are the security holes created by the hackers or mistakenly created by an employee.

MAC spoofing:

AP uses a list of MAC addresses for authentication purpose. However, MAC address can be easily spoofed .A hacker can identify a valid MAC address because the MAC headers are never encrypted.

Remote redirection attacks:

All packets used to inform another node about the location of a mobile node effectively is redirected away from the true location of the mobile node. This type of hijacking attacks

are called "remote redirection" attacks, since the malicious host, operating at a remote network is responsible for this.

Proximity based hacking:
Interference, cross-talk from similar range of frequency bands can easily be exploited if wireless devices are not configured properly.

5. Write short notes on the following: **[MODEL QUESTION]**
a) WEP
b) RC4 and RC5
c) WPA
Answer:
a) WEP:
Two processes are applied to the plaintext data. One encrypts the plaintext; the other protects the data from being modified by unauthorized personnel. The 40-bit secret key is connected with a 24-bit Initialization Vector (IV) resulting in a 64-bit total key size. The resulting key is input into the Pseudo-random Number Generator (PRNG). This PRNG (RC4) outputs a pseudorandom key sequence based on the input key. The resulting sequence is used to encrypt the data by doing a bitwise XOR. The result is encrypted bytes equal in length to the number of data bytes that are to be transmitted in the expanded data plus four bytes. This is because the key sequence is used to protect the 32-bit Integrity Check Value (ICV) as well as the data. To prevent unauthorized data modification, an *integrity algorithm*, CRC-32 operates on the plaintext to produce the ICV. The ciphertext is obtained by computing the ICV using CRC-32 over the message plaintext connecting the ICV to the plaintext choosing a random initialization vector (IV) and connecting this to the secret key inputting the secret key IV into the RC4 algorithm to produce pseudorandom key sequence encrypting the plaintext ICV by doing a bitwise XOR with the pseudorandom key sequence under RC4 to produce the ciphertext communicating the IV to the peer by placing it in front of the ciphertext. The IV, plaintext, and ICV triplet forms the actual data sent in the data frame. The IV of the incoming message is used to generate the key sequence necessary to decrypt the incoming message. Combining the ciphertext with the proper key sequence will give the original plaintext and ICV. The decryption is verified by performing the Integrity check algorithm on the recovered plaintext and comparing the output of the ICV' to the ICV submitted with the message.

If the ICV' is not equal to the ICV, the received message is in error, and an error indication is sent to the MAC management and back to the sending station.

b) RC4 and RC5:
RC4 cipher or "Rivest Cipher 4" invented in 1987 by Ron Rivest. It was used in many popular standards and protocols such as WEP, WPA, SSL or TLS. The RC4 algorithm generates a pseudo-random keystream that is then used to generate the ciphertext (by

XORing it with the plaintext). It is called pseudorandom because it generates a sequence of numbers that only approximates the properties of random numbers. The sequence of bytes generated is not random since the output is always the same for a given input but it has to approximate random properties to make it harder to crack. The keystream is generated from a variable length key. A pseudorandom number generator uses a function that produces a deterministic stream of bits that eventually repeats. The longer the period of repeat the more difficult it will be to do cryptanalysis. If the keystream is treated as a stream of bytes, then all of the 256 possible byte values should appear approximately equally often. The output of the pseudorandom number generator is conditioned on the value of the input key. The RC4 algorithm is remarkably simply and quite easy to explain. A variable-length key of from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S, with elements S[0], S[1], ..., S[255]. At all times, S contains a permutation of all 8-bit numbers from 0 through 255. For encryption and decryption, a byte is generated from S by selecting one of the 255 entries in a systematic fashion. As each value of k is generated, the entries in S are once again permuted. Normally, a key length of 128bit is used.

RC5 is a block cipher notable for its simplicity. RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255). The original suggested choice of parameters were a block size of 64 bits, a 128-bit key and 12 rounds. A key feature of RC5 is the use of data-dependent rotations; one of the goals of RC5 was to prompt the study and evaluation of such operations as a cryptographic primitive. RC5 also consists of a number of modular additions and eXclusive OR (XOR)s. The encryption and decryption routines can be specified in a few lines of code but the key schedule is more complex. The simplicity of the algorithm together with the novelty of the data-dependent rotations has made RC5 an attractive object of study for cryptanalysts. The RC5 is basically denoted as RC5-w/r/b where w=word size in bits, r=number of rounds, b=number of 8-bit byte in the key.

c) WPA:
Wi-Fi Protected Access was the Wi-Fi Alliance's direct response and replacement to the increasingly apparent vulnerabilities of the WEP standard. The most common WPA configuration is WPA-PSK (Pre-Shared Key). The keys used by WPA are 256-bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system. Some of the significant changes implemented with WPA included message integrity checks. Integrity checks are used to determine if an attacker had captured or altered packets passed between the access point and client) and the Temporal Key Integrity Protocol (TKIP). TKIP employs a per-packet key system that was radically more secure than fixed key used in the WEP system. TKIP was later superseded by Advanced Encryption Standard (AES). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. User authentication is generally missing in WEP. It is deployed in WPA through the extensible

authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

TOOLS AND METHODS USED IN CYBER CRIME

Multiple Choice Type Questions

1. Steganography is used in [WBUT 2015]
   a) Digital imaging b) Digital watermarking
   c) Digital signal processing d) Photoshop
   Answer: (a)

2. DOS attack is caused by [WBUT 2016]
   a) authentication b) alteration c) fabrication d) replay attacks
   Answer: (c)

3. A ..... replicates itself by creating its own copies, in order to bring the network to halt. [WBUT 2016]
   a) virus b) worm c) Trojan horse d) bomb
   Answer: (a)

4. Access to a computer program that bypasses security mechanism is called [WBUT 2017, 2018]
   a) Backdoor b) Trojan horse
   c) Strom Worm d) None of these
   Answer: (a)

5. The tool that acts like an offline browser is [WBUT 2018]
   a) HT track b) e-mail traker pro
   c) trace route d) none of these
   Answer: (a)

6. Which program generates random packets to launch DOS attack? [WBUT 2018]
   a) jolt 2 b) targa
   c) nemesy d) all of these
   Answer: (c)

Short Answer Type Questions

1. What is SQL injection? How it can be prevented? [WBUT 2015, 2017]
   Answer:
   SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements (also commonly referred to as a malicious payload) that control a web application's database server (also commonly referred to as a Relational Database Management System – RDBMS). Since an SQL injection vulnerability could

possibly affect any website or web application that makes use of an SQL-based database, the vulnerability is one of the oldest, most prevalent and most dangerous of web application vulnerabilities.

By leveraging an SQL injection vulnerability, given the right circumstances, an attacker can use it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQL injection can also be used to add, modify and delete records in a database, affecting data integrity.

To such an extent, SQL injection can provide an attacker with unauthorized access to sensitive data including, customer data, personally identifiable information (PII), trade secrets, intellectual property and other sensitive information.

An SQL injection needs just two conditions to exist – a relational database that uses SQL, and a user controllable input which is directly used in an SQL query.
SQL is a programming language designed for managing data stored in an RDBMS, therefore SQL can be used to access, modify and delete data. Furthermore, in specific cases, an RDBMS could also run commands on the operating system from an SQL statement.
Keeping the above in mind, when considering the following, it's easier to understand how lucrative a successful SQL injection attack can be for an attacker.

- An attacker can use SQL injection to bypass authentication or even impersonate specific users.
- One of SQL's primary functions is to select data based on a query and output the result of that query. An SQL injection vulnerability could allow the complete disclosure of data residing on a database server.
- Since web applications use SQL to alter data within a database, an attacker could use SQL injection to alter data stored in a database. Altering data affects data integrity and could cause repudiation issues, for instance, issues such as voiding transactions, altering balances and other records.
- SQL is used to delete records from a database. An attacker could use an SQL injection vulnerability to delete data from a database. Even if an appropriate backup strategy is employed, deletion of data could affect an application's availability until the database is restored.
- Some database servers are configured (intentional or otherwise) to allow arbitrary execution of operating system commands on the database server. Given the right conditions, an attacker could use SQL injection as the initial vector in an attack of an internal network that sits behind a firewall.

2. Write down the difference between Computer Virus and Worm. [WBUT 2015]

Answer:

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus

can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

3. What is virus hoax? Describe computer worm briefly. [WBUT 2016]

Answer:

1st Part:

A computer virus hoax is a message warning the recipients of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know.

2nd part: ***Refer to Question No. 2 of Short Answer Type Questions.***

4. What is Trojan Horse? What is the difference between Trojan Horse and Backdoors. [WBUT 2017]

Answer:

A Trojan is a disguised detrimental program hidden by any normal software. Trojans affect registry and system files in such a way that manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts, launch (DDOS) and infect other systems. A Trojan can be installed in users system while executing any legitimate software such as freeware, spyware-removal tools, games, music, and email-attachment. Example of Trojans are Backorifice, NetBus.

Backdoors are one kind of malicious programs which runs in the system without the user's knowledge and gives access to your personal information to the hackers when you are connected to the internet. These viruses are designed in such a way which gives remote access to the hackers. These hackers can easily place these viruses into your system if you visit any unauthorized web pages.

5. Discuss briefly about proxy server. [WBUT 2017]

Answer:

Proxy servers acts in between content servers and web browsers catching regularly accessed pages. Proxy servers also act in load balancing server, or can filter and route traffic to certain network by properly configuring access control lists. The proxy server can perform authentication and authorization and block access to certain websites and can enhance security of servers. Another important feature is its capability to protect the identity of the servers from the web clients. Reversely a web client can make anonymous

access by targeting the proxy servers. As proxy servers can let a client browse the network easily, hackers use this anonymity to access content servers. They access proxy servers and make it difficult to recognize the origin of attack. Anonymizer is a tool that can be used as proxy for this purpose. In Linux environment /etc/squid/squid.conf is used to configure the proxy server.

6. What are steps to protect Dos/DDos attack? **[WBUT 2017]**

Answer:

Network-ingress filtering: It is a kind of filtering method used to stop the attackers from using spoofed IP or name for accessing the inside network.

Rate-limiting network traffic: Sometimes attackers targets routers or modems with higher bandwidth. Some routers are configured to check this. They limit the amount of bandwidth or reroute the traffic in case of network congestion.

Intrusion detection systems: can help to detect whether a machine in your network is being used to launch a known attack

Host-auditing tools and Network-auditing tools and Automated network-tracing tools: Helps to detect any DOS software running in the environment by scanning files, streams of packet.

7. What is DNS redirection? **[WBUT 2017]**

Answer:

DNS redirection is the controversial practice of serving a Web page to a user that is different from either the one requested or one that might reasonably be expected, such as an error page. Typically, an ISP serves an ad-based page, rather than a 404 error message, when the user mistypes a URL.

8. What are the different types of DOS attacks? **[MODEL QUESTION]**

Answer:

(i) BOT and BOTNETS: are automated softwares, webrobots that use spam, gathers information, passes them to BOT servers over normal IRC or instant messaging. BOTNETS are a multiple number of BOTS.

(ii) Smurf: Sends multiple ICMP (echo requests) to flood the network with even larger number of (ICMP) echo reply.

(iii) SYN flood: sends multiple TCP SYN requests from spoofed IP and crashes the server.

(iv) Ping of Death: sends multiple IP packets which are large when reassembled and causes the system to crash.

9. What is the difference between proxy server and anonymizer? **[WBUT 2018]**

Answer:

A proxy server is a server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. Proxy servers have two main purposes: to improve performance and to filter requests.

An anonymizer is a proxy server that makes Internet activity untraceable. An anonymizer protects personally identifying information by hiding private information on the user's behalf. An anonymizer may also be known as anonymous proxy.

Long Answer Type Questions

1. a) What is DoS Attacks? Write down the tools used to launch DDoS attacks.
b) Write down the types or levels of DoS attacks?
c) Define Trojan virus with example. **[WBUT 2015]**

Answer:

a) 1st Part:

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting our computer and its network connection, or the computers and network of the sites we are trying to use, an attacker may be able to prevent us from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

2nd Part:

Few tools which are used to launch DDoS attacks are as follows:

LOIC

Low Orbit Ion Cannon (LOIC) is a simple flooding tool that can generate massive volumes of TCP, UDP, or HTTP traffic to subject a server to a heavy network load.

HOIC

High Orbit Ion Cannon (HOIC) quickly took the spotlight when it was used to target the U.S. Department of Justice in response to its decision to take down Megaupload.com. At its core, HOIC is a simple cross-platform basic script for sending HTTP POST and GET requests wrapped in an easy-to-use GUI. However, its effectiveness stems from add-on "booster" scripts—text files that contain additional basic code interpreted by the main application upon DDoS attack launch.

hping

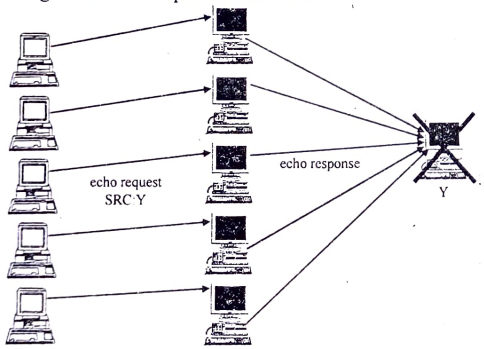
The DDoS attack tool hping is a fairly basic command line utility similar to the ping utility. However, it offers more functionality than simply sending an ICMP echo request. In fact, hping can be used to send large volumes of TCP traffic to a target while spoofing the source IP addresses, making it appear to be random or even to originate from a specific, user-defined source.

Slowloris
Many of the more intricate low and slow DDoS attack types rely on easy-to-use tools, yielding denial of service attacks that are much harder to detect. Developed by a gray hat hacker who goes by the handle "RSnake," Slowloris creates a DoS condition for a server by using a very slow HTTP request. By sending HTTP headers to the target site in tiny chunks as slowly as possible, the server is forced to continue to wait for the headers to arrive. If enough connections are opened to the server in this way, the server becomes unable to handle legitimate requests.

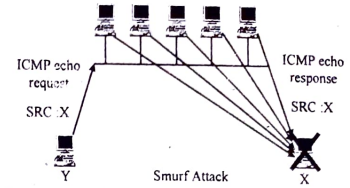
b) Types or Levels of Dos Attacks:

- **Bandwidth Attacks:** If we load any site, it takes certain time to "load". Loading means it appears on our screen with the images and texts. This "loading" consumes some amount of memory. Every site is given with a particular amount of bandwidth by its hosting, say for example 100Gb. Now if i get more visitors who consumes all my 100GB bandwidth, the hosting of the site can ban your site. So now if the attackers does the same. He can open 100 pages of a site and keep on refreshing and consume all the bandwidth and its out of service.
- **Logic Attacks:** These kinds of attack can exploit vulnerabilities in network software such as web server or the underlying TCP/IP stack
- **Protocol Attacks:** Exploiting a specific feature or implementation bug of some protocol installed at the victim in order to consume excess amounts of its resources. Protocols here are rules that is to be followed to send data over network. I found this document on 5 Protocol attacks which explains of you in detail on protocol attacks. Its a little bit geeky but worth trying it.

Here are some images which can explain a little more.



UDP Attack



Smurf Attack

c) A Trojan in the software world is a type of malware that is often the tool of choice for cyber criminals. Named for the tactics Greek warriors used to infiltrate Troy using an enormous wooden horse, a Trojan can be just as deceptive and destructive. In combating this type of computer security threat, just knowing what you're up against is a start. Once a Trojan penetrates a computer's security defenses, it can give control of the infected computer to the hacker. Since it usually runs as a background process, users of computers infected by a Trojan don't even know their systems have been compromised. At this point additional malware can be installed and sensitive data can be stolen. On a more sophisticated level, an infected computer can be used as a launch point to attack other computers and networks, thus covering the cyber criminal's tracks.

A good example of a Trojan Banker is Zeus, also called Zbot. The Zeus Trojan can add extra fields to a Web page with a form, like the pages one might visit when doing their online banking. Since it is the actual bank's Web page and not some forged site, a few extra fields to fill might not seem as suspicious to the user. The fields may be disguised as added security questions that could give the criminal needed information to gain access to the account later on. On the underground market, Zeus was being sold as a malware toolkit enabling less experienced cyber criminals access to the technology. Until 2011 when the source code was made public, the Zeus toolkit could cost up to $10,000.

2. Write short note on Botnet. **[WBUT 2015]**

OR,

Write the concept of 'Botnet' briefly. **[WBUT 2016]**

Answer:

A botnet is a network of compromised computers under the control of a malicious actor. Each individual device in a botnet is referred to as a bot. A bot is formed when a computer gets infected with malware that enables third-party control. Bots are also known as "zombie computers" due to their ability to operate under remote direction without their owners' knowledge. The attackers that control botnets are referred to as "bot herders" or "bot masters."

Attackers use botnets for a variety of purposes, many of them criminal. The most common applications for botnets include email spam campaigns, denial-of-service attacks, spreading adware/spyware, and data theft (particularly of financial information, online identities and user logins). A botnet attack starts with bot recruitment. Bot herders often recruit bots by spreading botnet viruses, worms, or other malware; it is also possible

to use web browser hacking to infect computers with bot malware. Once a computer has been infected with a botnet virus it will connect back to the bot herder's command and control (C&C) server. From here the attacker is capable of communicating with and controlling the bot. When the botnet grows to its desired size, the herder can exploit the botnet to carry out attacks (stealing information, overloading servers, click fraud, sending spam, etc.).

Zeus is a Trojan horse for Windows that was created to steal bank information using botnets. First discovered in 2007, Zeus spread through email, downloads, and online messaging to users across the globe. Zeus botnets used millions of zombie computers to execute keystroke logging and form grabbing attacks that targeted bank data, account logins, and private user data. The information gathered by Zeus botnets has been used in thousands of cases of online identity theft, credit card theft, and more.

3. What is a dictionary password cracking technique? How can we key loggers be used to commit a cybercrime? "The rapid application of wireless devices has increased the chances of cybercrimes" explain. Write the different tools used to launch DoS attack. Define SQL injection. **[WBUT 2016]**

Answer:

1st part:

Dictionary Attacks are a method of using a program to try a list of words on the interface or program that is protecting the area that you want to gain access to. The most simple password crackers using dictionary attacks use a list of common single words, aka a "dictionary". More advanced programs often use a dictionary on top of mixing in numbers or common symbols at the beginning or end of the guessed words.

2nd part:

Imagine a stranger standing over our shoulder watching us log in to our online bank account. This scenario plays out in the virtual world as cyber criminals virtually monitor keystrokes as we type on our computer keyboard. The monitoring occurs via applications called keyloggers. Clever criminals devise multiple methods to steal our information, though keylogging applications operate using similar principles.

Keyloggers are like matches -- they have constructive uses, such as starting a fire for cooking, but they are also useful for criminal use, such as burning down a building. Keyloggers are legal. Companies use them to monitor the activity of staff using their computers; parents use them to insure that their children do not surf to inappropriate websites and they also operate as backup devices. For instance, if we have a keylogger running while typing an important letter, the keylogger saves what we typed even if our computer crashes before we can save our file.

3rd part:

As wireless communication has grown, attacks on wireless devices have become more frequent. Some of the newer attacks are automated, attention is being directed toward drivers and thumb drives have become useful crime tools.

There have also been increases in the impact of cyber crimes, creating damage to companies, customers and the larger society. These damages are like pebbles thrown into water, expanding out from the initial point of contact. There are direct and indirect costs involved with a publicized unauthorized incursion into a company's system. Research findings on these costs indicate that retail firms which have been attacked are penalized financially as well as in terms of customers' willingness to continue to shop with them. Increasing use of mobile and wireless technologies create new risks where these devices and technologies are insufficiently secured and protected from misuse. Because new hardware devices are portable, they are more easily stolen and may often not have passwords used or data encrypted. In 2005, one survey found that 22 percent of people reported losing their mobile devices and of those, 81 percent had not encrypted the information in any way (Millman 2005).

4th part:

Refer to Question No. 1 of Long Answer Type Questions.

5th part:

Refer to Question No. 1 of Short Answer Type Questions.

4. Discuss about email spoofing and email spamming. **[WBUT 2017]**

Answer:

The word "spoof" means "falsified". A spoofed email is when the sender purposely alters parts of the email to masquerade as though it was authored by someone else. Commonly, the sender's name/address and the body of the message are formatted to appear from a legitimate source, as though the email came from a bank or a newspaper or legitimate company on the Web. Sometimes, the spoofer will make the email appear to come from a private citizen somewhere.

Email spamming refers to sending email to thousands and thousands of users – similar to a chain letter. Spamming is often done deliberately to use network resources. Email spamming may be combined with email spoofing, so that it is very difficult to determine the actual originating email address of the sender. Some email systems, including our Microsoft Exchange, have the ability to block incoming mail from a specific address. However, because these individuals change their email addresses frequently, it is difficult to prevent some spam from reaching your email inbox.

5. What is buffer overflow? Discuss about the types of buffer overflow. **[WBUT 2017]**

Answer:
Some of the web application threats include buffer overflow and SQL injection. Client side forms are used as simple tool for this hacking purpose

Buffer Overflow: Huge amounts of data are sent to a web application through a web form to execute commands so as to overflow the memory contents into another buffer area. This can overwrite the contents of another buffer which may be storing results of intermediate applications. It uses input to a poorly implemented, but (in intention) completely harmless application, typically with administrator privileges. Types of buffer overflows include stack-based overflow and heap-based overflow. The buffer overflow attack results from input that is longer than the implemented or intended. If the input is too long, we get bad program behavior. Different types of buffer overflow attacks include:

- **Control the process execution:** using memory pointers to directly or indirectly
- **Crash the process:** some codes can be redirected to a specific jump location which can spawn a command-line environment, or shell script, more child processes ultimately the parent process will wait indefinitely thus freezing or crashing the entire program.
- **Modify internal variables:** modify t he contents of memory registers.

6. Define Virus, Worm and Trojan horse. **[WBUT 2018]**

Answer:

Refer to Questions No.2 and 4(1st part) of Short Answer Type Questions.

7. Write short notes on the following:

a) Trojan Horse **[WBUT 2016]**
b) DDoS attack **[WBUT 2016]**
c) Tabjacking **[WBUT 2016]**
d) DOS and DDOS **[WBUT 2017]**

Answer:

a) ***Refer to Question No. 4(1st part) of Short Answer Type Questions.***

b) DDoS *is short for* **D***istributed* **D***enial of* **S***ervice.* DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

In a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to

distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

There are many types of DDoS attacks. Common attacks include the following:

- **Traffic attacks:** Traffic flooding attacks send a huge volume of TCP, UDP and ICPM packets to the target. Legitimate requests get lost and these attacks may be accompanied by malware exploitation.
- **Bandwidth attacks:** This DDos attack overloads the target with massive amounts of junk data. This results in a loss of network bandwidth and equipment resources and can lead to a complete denial of service.
- **Application attacks:** Application-layer data messages can deplete resources in the application layer, leaving the target's system services unavailable.

c) Tabjacking is a new form of malware that can enter our PC through vulnerabilities in our Web browser that allow hackers to insert malicious code into the tabs of our Web browser. The code is capable of hijacking the tab to a new Web page and inserting advertising pop-ups, worms, trojans, or other malware into our PC.

Mozilla Firefox made a browser that allows us to surf the Internet and switch to the pages we have chosen to view through the use of browser tabs. Not long after, Internet Explorer introduced a new version that has the same capabilities as Mozilla Firefox. The tabs allow us to open more Web pages within a single browser window and are designed to make our browser easier to use.

Although the tabs make surfing the Web a lot easier, they also introduce a new weakness where hackers can insert malicious code. When we open the tab the codes are run to hijack the tab to a Web page that the hacker wants us to view. The pages usually contain advertisements and may even contain additional adware that is inserted into our PC.
Tab jackers are also capable of inserting viruses and other malicious files into our PC that include spyware and keyloggers, as well as displaying phishing websites that encourage us to enter personal information that invites identity theft.

Once our PC has been tabjacked the problem will persist even if we try to reboot our PC's operating system, and the malware will reinsert itself without our consent every time we open our browser. The concept of tabjacking has been introduced as a result of the new browser design that allows us to view more than one Web page in our browser window. Hackers use tabjacking to exploit browser vulnerabilities on computers that are not running updates to antivirus software or are running on older operating systems.

While this form of malware is still in the phases of being studied, we can protect our PC against tabjacking by keeping our operating system and Web browser updated with all of the latest security patches and running a current antivirus protection program on our PC.

Also, make sure our antivirus program contains an anti-adware and antispyware application and is capable of automatically scanning for the latest virus updates. We can also use a reputable registry cleaner on a periodic basis to remove any unwanted or malicious files that may have made their way to our PC's registry.

d) DOS and DDOS:

DOS attacks are organized between client and server to flood the network with unnecessary packets. The server is overwhelmed with requests from spoofed addresses and thereby fails to reply services to the original clients. There are different categories of DOS attacks. Some send ICMP echo packets in large quantity while others send SYN packets for TCP connections. Some IP packets are send in large numbers so that original packet size exceeds and server fails to reassemble the packets. Any kind of DOS flooding leads to system crash. The result of DOS attack is either disconnection between server and client, server site becomes terribly slow, a particular client can be blocked out with this kind of attack. A DoS attack is usually an attack of last resort. It's considered an unsophisticated attack because it doesn't gain the hacker access to any information but rather annoys the target and interrupts their service. DoS attacks can be destructive. Some DOS attacks render the system as zombies. DDOS attacks sends packet to selected machines which in turn acts as master and sends huge number of packets to the network thus a multiple number of machines and their combined effect essentially disrupts the network connection.

8. Write short notes on Dumpster Diving. **[MODEL QUESTION]**

Answer:

a) Dumpster Diving:

In the IT world, dumpster diving refers to using various methods to get information about a technology user. In general, dumpster diving involves searching, through trash or garbage looking for something useful. This is often done to uncover useful information that may help an individual get access to a particular network. So, while the term can literally refer to looking through trash, it is used more often in the context of any method (especially physical methods) by which a hacker might look for information about a computer network.

In many cases, dumpster diving involves getting data about a user in order to impersonate that user and gain access to his or her user profiles or other restricted areas of the Internet or a local network.

To Protect ourselves From Dumpster Diving we need to do the following:

- Never discard documents containing information such as a Social Security number, driver's license number, or bank account number into a public trash bin.
- Always shred important documents we choose to discard as opposed to crumbling the paper and throwing them in the trash.

- Thoroughly cut up all old credit and debit cards so that the information is not legible and make sure all of confidential information gets disposed properly by using a trusted security shredding company.
- Dumpster diving is fairly easy to prevent. It basically consists of taking the extra steps to make sure your personal information is properly disposed. A little tedious work from the start can save you from the expensive headache related to identity theft.

PHISHING & IDENTITY THEFT

Multiple Choice Type Questions

1. Which of the following is a social engineering site? [WBUT 2015]

a) ebay b) Facebook
c) Amazon d) CWB

Answer: (a)

2. The method in which the Phishes identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data [WBUT 2017]

a) Dragnet b) Rod and reel
c) Gillnet d) Lodsterpot

Answer: (b)

3. Vishing is mean for [WBUT 2017]

a) SMS Phishing b) Voice Phishing
c) Phishing d) All of these

Answer: (b)

4. Act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity is called

a) Email bombing b) Spamming [MODEL QUESTION]
c) Cyber stalking d) Phishing

Answer: (d)

Short Answer Type Questions

1. What is vishing? [WBUT 2015]

OR,

Define Vishing. [WBUT 2016]
What are different vishing techniques? [WBUT 2015]

OR,

Define Vishing. State different Vishing techniques. [WBUT 2018]

Answer:

1st Part:

The telephone equivalent of phishing. Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

2nd Part:

Vishing techniques include:

Wardialing:

This is when the visher uses an automated system to call specific area codes with a message involving local or regional banks or credit unions. Once someone answers the phone, a generic or targeted recording begins, requesting that the listener enter bank account, credit, or debit card numbers, along with PIN codes.

VoIP:

Voice over Internet Protocol, or VoIP, is an Internet-based phone system that can facilitate vishing by allowing multiple technologies to work in tandem. Vishers are known to use VoIP to make calls, as well as to exploit databases connected to VoIP systems.

Caller ID Spoofing:

This is the practice of causing the telephone network to display a false number on the recipient's caller ID. A number of companies provide tools that facilitate caller ID spoofing. VoIP has known flaws that allow for caller ID spoofing. These tools are typically used to populate the caller ID with a specific bank or credit union, or just with the words "Bank" or "Credit Union."

Social Engineering:

Social engineering is a fancier, more technical form of lying. Social engineering (or social penetration) techniques are used to bypass sophisticated security hardware and software. The automated recordings used by vishers tend to be relatively professional and convincing.

Dumpster Diving:

One time and tested "hack" is simply digging through a bank's dumpster and salvaging any lists of client phone numbers. Once the visher has the list, he can program the numbers into his system for a more targeted attack.

2. Define Identity Theft (ID Theft). Write down the different technique of ID Theft. [WBUT 2015]

OR,

Explain the different types of Identity Theft briefly. [WBUT 2016]

OR,

What is ID theft? What are the techniques of ID theft? [WBUT 2017]

Answer:

1st Part:

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an

imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

2nd Part:

Identity theft is an ever-evolving crime.

Few techniques for identity theft is given below:

1. Phishing

Phishing grows daily as an effective source for identity thieves. They send phony, but authentic looking emails requesting personal information. Again, never, ever give out personal information to anyone we do not know personally. We have to be careful that we are really on the website we think we are on rather than a bogus on. And be sure your firewall, anti-virus and anti-spyware software is up to date.

2. Information retrieval

This sneaky technique slips past most people. Have you ever gotten rid of computers or other electronic equipment containing personal information? Thieves regularly check those dump sites. While they have little interest in a computer; they desire your hard drive with personal information on it. Avoid identity theft and have your hard drive professionally erased before disposing it.

3. Victim research

Even thieves do their research. But, in this case, they research o. Identity thieves search government registers, Internet search engines, and public records search services to gain the bits and pieces of information they need.

4. Pick pocketing

Most people think pickpockets don't exist anymore -- too low-tech. Think again. Pickpockets are alive and well and after your wallet -- complete with debit and credit cards. Whatever you do... do not store your PIN number in your wallet. This is the pick pocketer's greatest treasure.

5. Skimming

Skimming requires a device attached to an ATM or credit card machine. The device reads the magnetic strip on your bank, credit or debit card, which thieves use to commit fraud. Prevent identity theft by remaining alert to signs of strange devices on your machine.

6. Remote thievery

If you have a contactless or smartcard credit card, you could be in danger of this type of crime. Thieves read cards remotely with a compact radio frequency device.

7. Shoulder surfing

Shoulder surfing is another low-tech but efficient form of theft. The thief simply eavesdrops on transactions you make in public and pick up whatever useful information you disclose.

8. Computer identity theft

With the use of Trojan horses (a type of computer virus), hacking, and Zero day attacks, thieves get personal information from your computer.

9. Data breach

Most public offices try not to do this anymore, but every once in a while it still happens. This is when an office displays sensitive information, such as your social security number, on a label or in the newspaper.

3. Differentiate between whaling and Spear Phishing. **[WBUT 2016]**

Answer:

Spear phishing targets a group of people. For example, a spear phishing email can target employees of a specific company, customers of a specific company, or even a specific person.

Whaling targets high-level executives. As an example, a whaling attack targeted senior corporate executives using their actual name, company name, and phone number.

4. What is the law for Identity theft in India? **[MODEL QUESTION]**

Answer:

Section 66C, ITA states the law for identity theft:

"PUNISHMENT FOR IDENTITY THEFT Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh."

Long Answer Type Questions

1. a) What is phishing? **[WBUT 2015, 2017]**

Write down the different types of modern Phishing techniques. **[WBUT 2015]**

OR,

Write the different Phishing techniques briefly. **[WBUT 2016]**

OR,

What are the different methods of Phishing attack?

b) Explain the different method of Phishing. **[WBUT 2017]**

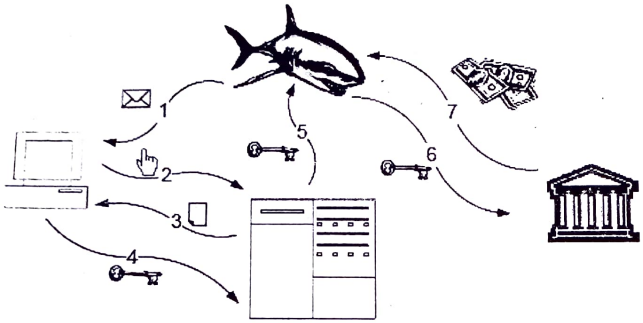
c) Write down the different phishing countermeasures. **[WBUT 2015]**

Answer:

a) 1st Part:

Phishing is online stealing of information by enticing the victims. The term originated from stealing of account information by using email messages. A phishing message will bait the unsuspected users by sending messages requiring immediate action. Normally, attacker uses name of legitimate bank and demands user username and password. The attacker will make users believe that their account will be reopened due to website maintenance and redirects the user to a fake website forcing them to use their credentials.

The Phishing attack steps are as follows:



Steps in a Phishing Attack

The steps are:

0. The phisher prepares for the attack.

Step 0 countermeasures include monitoring malicious activity to detect a phishing attack before it begins.

1. A malicious payload arrives through some propagation vector.

Step 1 countermeasures involve preventing a phishing message or security exploit from arriving.

2. The user takes an action that makes him or her vulnerable to an information compromise.

Step 2 countermeasures involve detecting phishing tactics and rendering phishing messages less deceptive.

3. The user is prompted for confidential information, either by a remote web site or locally by a Web Trojan.

Step 3 countermeasures are focused on preventing phishing content from reaching the user.

4. The user compromises confidential information.

Step 4 countermeasures concentrate on preventing information from being compromised.

5. The confidential information is transmitted from a phishing server to the phisher.

Step 5 countermeasures involve tracking information transmittal.

6. The confidential information is used to impersonate the user.

Step 6 countermeasures center on rendering the information useless to a phisher.

7. The phisher engages in fraud using the compromised information.

Step 7 countermeasures focus on preventing the phisher from receiving money.

2nd Part:

There are different types of phishing techniques used apart from email. They are as follows:

Email / Spam

Phishers may send the same email to millions of users, requesting them to fill in personal details. These details will be used by the phishers for their illegal activities. Phishing with email and spam is a very common phishing scam. Most of the messages have an urgent note which requires the user to enter credentials to update account information, change details, and verify accounts. Sometimes, they may be asked to fill out a form to access a new service through a link which is provided in the email.

Web Based Delivery

Web based delivery is one of the most sophisticated phishing techniques. Also known as "man-in-the-middle," the hacker is located in between the original website and the phishing system. The phisher traces details during a transaction between the legitimate website and the user. As the user continues to pass information, it is gathered by the phishers, without the user knowing about it.

Instant Messaging

Instant messaging is the method in which the user receives a message with a link directing them to a fake phishing website which has the same look and feel as the legitimate website. If the user doesn't look at the URL, it may be hard to tell the difference between the fake and legitimate websites. Then, the user is asked to provide personal information on the page.

Trojan Hosts

Trojan hosts are invisible hackers trying to log into your user account to collect credentials through the local machine. The acquired information is then transmitted to phishers.

Link Manipulation

Link manipulation is the technique in which the phisher sends a link to a website. When the user clicks on the deceptive link, it opens up the phisher's website instead of the website mentioned in the link. One of the anti-phishing techniques used to prevent link manipulation is to move the mouse over the link to view the actual address.

Key Loggers

Key loggers refer to the malware used to identify inputs from the keyboard. The information is sent to the hackers who will decipher passwords and other types of information. To prevent key loggers from accessing personal information, secure websites provide options to use mouse click to make entries through the virtual keyboard.

Session Hacking

In session hacking, the phisher exploits the web session control mechanism to steal information from the user. In a simple session hacking procedure known as session

sniffing, the phisher can use a sniffer to intercept relevant information so that he or she can access the Web server illegally.

System Reconfiguration

Phishers may send a message whereby the user is asked to reconfigure the settings of the computer. The message may come from a web address which resembles a reliable source.

Content Injection

Content injection is the technique where the phisher changes a part of the content on the page of a reliable website. This is done to mislead the user to go to a page outside the legitimate website where the user is asked to enter personal information.

Phishing through Search Engines

Some phishing scams involve search engines where the user is directed to products sites which may offer low cost products or services. When the user tries to buy the product by entering the credit card details, it's collected by the phishing site. There are many fake bank websites offering credit cards or loans to users at a low rate but they are actually phishing sites.

Phone Phishing

In phone phishing, the phisher makes phone calls to the user and asks the user to dial a number. The purpose is to get personal information of the bank account through the phone. Phone phishing is mostly done with a fake caller ID.

Malware Phishing

Phishing scams involving malware require it to be run on the user's computer. The malware is usually attached to the email sent to the user by the phishers. Once you click on the link, the malware will start functioning. Sometimes, the malware may also be attached to downloadable files.

b) 1st Part:

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

2nd Part:

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

c) Countermeasures phising attack:

1. Don't click on suspicious links.
2. Always check URL while entering your credentials for phishing page links.
3. Use antiphishing tools like Avast!, ESET Smart security. There are many anti-phishing toolbars which notify us about phishing pages like http://toolbar.netcraft.com/

2. Discuss the different types of social engineering. **[WBUT 2016]**

OR,

Explain the different attacks launched with attack vector. **[WBUT 2017]**

Answer:

Refer to Question No. 3.(a) of Long Answer type Questions.

3. What do you do if you become a victim of phishing and pharming? [WBUT 2018]

Answer:

Phishing and Pharming are household terms in the world of cyber attacks. Wherever there is a flow of valuable information, fraudsters are prowling. Cyber attacks are carried out by a person or a group against computers, computer networks, or a system of computers, most often to steal data or cause them to break down. Phishing and Pharming are especially dangerous because they use everyday internet services to get their victims. Some of the strategies are fake emails, deceptive attachments, and free download offers. On an ordinary day would you reveal your bank details to anyone who asked for it? Would you reveal your passwords to your e-mail or a shopping site? Of course not. Well, phishing and pharming scams are tools which make you do just that! Both terms apply to hackers on the internet committing theft and stealing important information from you.

Some phishers tend to leave signs in their emails. Signs to be on the lookout for include:

- Generic greetings such as "Dear Valued Customer"
- Immediate action such as "Failure to respond in five to ten days will terminate your account."
- E-mails that requests for personal information such as social security numbers or credit card numbers
- Links that are suspicious
- Misspellings and/or poor grammar
- If you receive such a message call the company or institution and asks questions.
- And remember to install an anti-virus software and keep it up-to-date.

To protect from pharming:

- Check the URL of any site that asks you to provide personal information. Make sure your session begins at the known authentic address of the site, with no additional characters appended to it.
- Maintain effective, up-to-date virus protection.

- Use a trusted, legitimate Internet Service Provider. Rigorous security at the ISP level is your first line of defense against pharming.
- Check the certificate. It takes just a few seconds to tell if a site you land on is legitimate and and check if the site carries a secure certificate from its legitimate owner.
- Block suspicious Web sites automatically. Anti-virus protection detects and blocks fake Web sites, making it easier for you to be confident most of the sites you are using are legitimate.

4. Write short notes on the following:
a) Social Engineering and Cybercrime. **[WBUT 2015]**
b) Spear Phishing **[WBUT 2017]**
c) Smishing **[WBUT 2017]**
Answer:

a) Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.
A social engineer runs what used to be called a "con game." Techniques such as appeal to vanity, appeal to authority and appeal to greed are often used in social engineering attacks. Many social engineering exploits simply rely on people's willingness to be helpful. For example, the attacker might pretend to be a co-worker who has some kind of urgent problem that requires access to additional network resources.

Popular types of social engineering attacks include:
Baiting:
Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.

Phishing:
Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.
Spear phishing: Spear phishing is like phishing, but tailored for a specific individual or organization.

Pretexting:
Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

Scareware:
Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.

b) Spear Phishing:
Spear phishing is an email that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC.

Email from a "Friend"
The spear phisher thrives on familiarity. He knows your name, your email address, and at least a little about you. The salutation on the email message is likely to be personalized: "Hi Bob" instead of "Dear Sir." The email may make reference to a "mutual friend." Or to a recent online purchase you've made. Because the email seems to come from someone you know, you may be less vigilant and give them the information they ask for. And when it's a company you know asking for urgent action, you may be tempted to act before thinking.

Using Your Web Presence Against You
How do you become a target of a spear phisher? From the information you put on the Internet from your PC or smartphone. For example, they might scan social networking sites, find your page, your email address, your friends list, and a recent post by you telling friends about the cool new camera you bought at an online retail site. Using that information, a spear phisher could pose as a friend, send you an email, and ask you for a password to your photo page. If you respond with the password, they'll try that password and variations to try to access your account on that online retail site you mentioned. If they find the right one, they'll use it to run up a nice tab for you. Or the spear phisher might use the same information to pose as somebody from the online retailer and ask you to reset your password, or re-verify your credit card number. If you do, he'll do you financial harm.

c) Smishing:
A nefarious text message could be on its way to a smartphone near you. This is a message, often purporting to be from your bank asking you for personal or financial information such as your account or ATM number. Providing the information is as good as handing thieves the keys to your bank balance.
Smishing is a portmanteau of "SMS" (short message services, better known as texting) and "phishing." When cybercriminals "phish," they send fraudulent emails that seek to trick the recipient into opening a malware-laden attachment or clicking on a malicious link. Smishing simply uses text messages instead of email.

There are a few things to keep in mind that will help you protect yourself against these attacks.

- ✓ You should regard urgent security alerts and you-must-act-now coupon redemptions, offers or deals as warning signs of a hacking attempt.
- ✓ No financial institution or merchant will send you a text message asking you to update your account information or confirm your ATM card code. If you get a message that seems to be from your bank or a merchant you do business with, and it asks you to click on something in the message, it's a fraud. Call your bank or merchant directly if you are in any doubt.
- ✓ Never click a reply link or phone number in a message you're not sure about.
- ✓ Look for suspicious numbers that don't look like real mobile phone numbers, like "5000". As these numbers link to email-to-text services, which are sometimes used by scam artists to avoid providing their actual phone numbers.
- ✓ Don't store your credit card or banking information on your smartphone. If the information isn't there, thieves can't steal it even if they do slip malware onto your phone.

5. Write short note on Identity Theft. **[MODEL QUESTION]**

Answer:

Identity (ID) theft is a crime where a thief steals your personal information, such as your full name or social security number, to commit fraud. The identity thief can use your information to fraudulently apply for credit, file taxes, or get medical services. These acts can damage your credit status, and cost you time and money to restore your good name. You may not know that you are the victim of ID theft until you experience a financial consequence (mystery bills, credit collections, denied loans) down the road from actions that the thief has taken with your stolen identity.

There are several common types of identity theft that can affect you:

Child ID theft

Children's IDs are vulnerable because the theft may go undetected for many years. By the time they are adults, the damage has already been done to their identities.

Tax ID theft

A thief uses your social security number to falsely file tax returns with the Internal Revenue Service or state government.

Medical ID theft

This form of ID theft happens when someone steals your personal information, such as your Medicare ID or health insurance member number to get medical services, or to issue fraudulent billing to your health insurance provider.

Senior ID theft

ID theft schemes that target seniors. Seniors are vulnerable to ID theft because they are in more frequent contact with medical professionals who get their medical insurance information, or caregivers and staff at long-term care facilities that have access to personal information or financial documents.

Social ID theft

A thief uses your name, photos, and other personal information to create a phony account on a social media platform.

CYBERCRIME & CYBERSECURITY

Multiple Choice Type Questions

1. Section 67 of ITA 2000 is associated with which of the following cybercrime? [WBUT 2015]
   a) Tempering with computer source documents
   b) Misrepresentation
   c) Publishing digital signature in false
   d) Transmitting obscene material in electronic from

Answer: (d)

2. Total number of cyber-crime cases were registered under the Indian IT act in 2007 is [WBUT 2016]
   a) 210 b) 207 c) 212 d) 211

Answer: 217

3. Indian Parliament passed ITA 2000 on [WBUT 2016]
   a) 15th August, 2000 b) 17th May, 2000
   c) 12th August, 2000 d) 12th May, 2000

Answer: (b)

4. Which of the following is India's first cyber law? [WBUT 2017]
   a) ITA 1998 b) ITA 1999
   c) ITA 2000 d) ITA 2001

Answer: (c)

5. Section 66F of IT Act deals with [WBUT 2018]
   a) Cyber stalking b) Email bombing
   c) Child pornography d) Cyber terrorism

Answer: (d)

6. Which of the following is the India's first Cyber Law? [WBUT 2018]
   a) ITA 2000 b) ITA 1999
   c) ITA 1998 d) ITA 2001

Answer: (a)

7. India's first cyber police station is located at [WBUT 2018]
   a) Delhi b) Bangalore
   c) Chennai d) Mumbai

Answer: (b)

8. Which section of IT Act covers most of the common crimes arising out of "Unauthorised Access"? [MODEL QUESTION]
   a) Section 66 b) Section 67
   c) Section 73 d) Section 74

Answer: (a)

Short Answer Type Questions

1. Discuss about the impact of IT act amendments on IT organizations. [WBUT 2015, 2018]

Answer:

The Information Technology (Amendment) Act, 2008, which came into effect in October 2009, has added Section 43 (A) to address data security and privacy issues. However, it is not without some concerns. Section 43 (A), which necessitates corporate bodies to protect all personal information they possess on computer resources, has received a mixed response from organizations. While some say the Act is a first step in a right direction, others feel that it won't have any major impact on Indian enterprises' security practices.

Few believe that Indian organizations in verticals like BFSI and IT services are already compliant with strict international regulations. For such organizations, security initiatives are often a result of business requirements than compliance. While it may not bring in radical changes for large organizations, the Act will help the small and medium enterprise (SME). "It will push SMEs to establish reasonable security controls as a mandatory practice," adds Samant.

Few disagrees that organizations like banks, service providers and telecom companies have enough security controls in place. "We often hear about leaks of customers' personal information, despite security controls. The new IT Act will ensure that security controls are firmed up, otherwise they will have to face legal implications."

While everyone considers the Information Technology (Amendment) Act, 2008 as a positive step, most there is also a need to educate enterprises about the Act. On this front, vendors like Websense and McAfee and law firms like Cyber Law Consulting claim to have begun educating their clients.

2. What is the meaning of the term 'cyber law'? Write the advantages of cyber law briefly. [WBUT 2016]

Answer:

Cyber crime refers to all illegal activities done using computers and the Internet, where the computer is used either as a tool or a target or both. Cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet. It is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law. It has a separate chapter XI entitled "Offences" in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine.

3. What is the difference between Staganography and Cryptography? [WBUT 2017]

Answer:

Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the

existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content. By combining Steganography and Cryptography one can achieve better security.

4. How easy is it to exploit stolen IP? **[WBUT 2018]**

Answer:

These are various ways one can exploit the IP address:

1. If one gets hold of IP address of a server, he/she could launch a Distributed Denial of Service (DDoS) attack on it, and make the service unavailable for the intended users.
2. could launch Brute Force SSH attacks and attempt to gain access to the machine.
3. could also scan for the services running OR any open ports on the host and would try to exploit it in some manner. (any FTP, Mail, MySQL, VNC etc.)
4. If the user and the hacker shares the same LAN, the hacker could target the user with Address Resolution Protocol spoofing and launch a Man in the Middle (communications attack) attack for all the internet communications.

IP address is like your home address but it's your duty to keep yourself safe from all kinds of attack. Always use a software firewall on your machine because you never know when/who all are trying to break into your host (house).IP address is part of every internet communication, so there is not much work to do. However the ways one can could disclose the IP to the attacker are browsing a web site/forum of the attacker, IM/chat with the attacker, you yourself are hosting any website or services.

5. What is the impact of cyber crime? **[WBUT 2018]**

Answer:

Individuals and businesses can suffer significant financial loss because of cyber crime with the most obvious impact being theft. Loss of business can also be significant in the instance of a denial of service attacks for large corporations. In addition, reputational damage can also be a significant factor following cyber crime. According to BBC Business News, Talk Talk lost almost a third of their share value following their data breach in 2015.

Businesses can be deliberately attacked because they have a high profile and possess valuable data, or there is some other publicity benefit in a successful attack.
Alternatively, the attack may be opportunistic, because cyber criminals have found vulnerabilities they can exploit. Almost every internet-facing entity will have exploitable vulnerabilities of some sort.

According to itgovernance.co.uk, cyber criminals are indiscriminate. Where there is a weakness, they will try to exploit it. Therefore, all businesses need to understand the cyber threats they may face, and take the appropriate steps to safeguard against them.
Within the past year, cybercrime victims have spent $126 billion globally and lost 19.7 hours – the time it would take to fly from New York City to Los Angeles four times – dealing with cybercrime.

The number of connected devices has exponentially grown in the last year and there is a constant need to be connected. In fact, people are willing to engage in risky online behavior in order to simply access Wi-Fi.

People are also known to share their passwords with friends, access financial information via unsecured Wi-Fi connections and click on suspicious links thereby increasing the vulnerability of their connected devices. Eighty percent of the consumers who took a compromising action in response to a potential phishing incident experienced negative consequences, including identify theft, money stolen from bank accounts, credit cards opened in their name and unauthorized apps installed on their device.

6. What is the need for cyber law in India or what are the legal aspects of cyber crime? **[MODEL QUESTION]**

Answer:

With the growth of Internet there is increase in tendency for unlawful activities that are normally intangible in terms of normal laws. A person can misuse any of the resources such as computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. for any kind of financial gain or satisfaction against personal vengeance. As trade in modern days involve huge amount online monetary transaction which can be compromised from a remote site anonymously. Leakage of personal or confidential information of any individual or organization can bring an end to the entire system. Impact of cyber crime is no less than any kind of crime those are done physically, but they cannot be treated with ordinary laws. These unlawful activities may include tampering with computer source documents, hacking with computer systems, data alteration violation of privacy, cyber terrorism, publishing or transmitting of material containing sexually explicit act, etc. in electronic form and other illegal activities. Cyberlaw touches almost all aspects of transactions and activities on and concerning the cyberspace. IT law covers mainly the digital information (including information security and electronic commerce) aspects and it has been described as "paper laws" for a "paperless environment" and especially designated for cyberspace.

7. What are the challenges to Indian law and cyber crime scenario in India? **[MODEL QUESTION]**

Answer:

The difficulties that are encountered in the Cyber Judiciary can be summarized as follows.

1. Adjudicators who are IT Secretaries are hesitant to take up additional responsibilities associated with Adjudication. Hence complainants are turned off (subject to exceptions in some States like Tamil Nadu) just like the Police Stations refuse to register Cyber Crime complaints.
2. Advocates familiar with the CPC are unable to accept the summary proceedings and the "Enquiry" nature of the proceedings at the Adjudication and find it difficult to adjust to the system. Gaining adjournments on flimsy grounds and taking unreasonable time for filing replies and counters every time is a strategy adopted by some counsels to delay matters. Since these are common in Civil Courts, there is a danger of the Cyber Judiciary system also going the Civil Judiciary way (as regards time required for completion of proceedings) unless the tendency is nipped in the bud.
3. Most of the participants are so tuned to CPC that they are unable to avoid being bogged down by procedures which may consist of application being made in a certain number of copies, in a certain format, with Court fee stamping been affixed, with 6 legal paper being used etc. and miss the essence of the "Principle of Natural Justice".
The casualty in this process is the "Time Limit" for completion of the adjudication or hearing of the Appeal in CAT.
4. Coupled with the time delays is the issue of change of guard of either the Adjudicator or the CAT chief. By the time the incumbent comes to get a hang of Cyber Crimes and nuances of Cyber Crime judiciary, their term may come to an end and the learning curve starts again.
5. Most of the Cyber Judicial offices are yet to use Virtual conference tools as provided in ITA 2000 and accompanying rules so as to reduce the cost of litigation and also to reduce delays.
6. Substantial work is therefore required to ensure that Cyber Judiciary system lives up to the great expectations raised by ITA 2000/8.

Long Answer Type Questions

1. a) Define The IT Act 2000. Write down the positive aspect of the ITA 2000. **[WBUT 2015]**

OR,

Write the positive aspects and weak areas of the ITA 2000. **[WBUT 2016]**

b) Write down the main object of IT act 2000.

c) Write down the amendments to the Indian IT Act. **[WBUT 2015]**

Answer:

a) *The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.*

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal

framework for the authentication and origin of electronic records / communications through digital signature.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

Digital signatures have been given legal validity and sanction in the Act.

The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

The Act now allows Government to issue notification on the web thus heralding e-governance.

The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

b) The IT ACT, 2000 – Objectives

- To provide legal recognition for transactions
- Carried out by means of electronic data interchange, and other means of electronic communication, commonly referred to as "electronic commerce", involving the use of alternatives to paper-based methods of communication and storage of information,
- To facilitate electronic filing of documents with the Government agencies
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934
- Aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.

c) IT Amendment Act (ITA-2008)

The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team (CERT-In).

The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; making the owner of a given IP address responsible for content accessed or distributed through it; and making corporations responsible for implementing effective data security practices and liable for breaches.

The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals. Section 69, for example, authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion. According to Pavan Duggal, a cyber law consultant and advocate at the Supreme Court of India, "The Act has provided Indian government with the power of surveillance, monitoring and blocking data traffic. The new powers under the amendment act tend to give Indian government a texture and color of being a surveillance state."

2. a) Write down the basic safety and security tips to prevent Cybercafe from cyber threat.

b) Write down the types and techniques of Credit card frauds. [WBUT 2015]

Answer:

a) Computers at public places such as internet cafe's can be a great place for hackers to glean sensitive information when we use the internet.

Here we suggest a few safety tips / countermeasures that will reduce the risk of getting hacked. For one-stop-shop protection seriously consider purchasing a IronKey USB device. This should keep machines safe and offer more protection than the countermeasures produced below. The IronKey in addition to providing an effective countermeasure to the exploits discussed above, also provides password protected hardware encryption that facilitate the secure storage of sensitive data. The IronKey has won numerous awards amongst the security community and is widely trusted and used by US government agencies and fortune 500 companies. The countermeasures without the use of an IronKey are:

Shoulder Surfers - Nothing technical here, just good observation / awareness skills. Need to be aware of the people around when typing in login details of any sort if there are people in the cyber cafe watching others, cover the keyboard when logging in.

Phishing Scams - Use more up-to-date versions of a browser when using the internet in a cyber cafe as they have anti-Phishing measures built into them. How do we run a modern browser when the version installed in the internet cafe is old? The options are to download and install it (which may not be possible due to restrictions), however a better way is to use portableapps (www.portableapps.com)and prepare a USB Flash Drive with

the latest version of firefox. This will give the option to "carry the application with you" and use it on any Windows machine. Also all browsing history will be stored on your USB Flash Drive and leave no remnants on the computer. However be aware that any digital certificates are stored on the computer and will need to be deleted A little education on how to identify a phishing site is the best form of protection, take a short quiz to see if you can recognise phishing websites and see if you can tell between a genuine site and a phishing site. After the quiz you will be well aware of how to spot a phishing site and ensure safety of online identity.

Network Sniffer - Most popular sites are secure as they protect credentials (user id and password) by encrypting them. However you should be mindful about the typical surfing habits performed in cyber cafe's. The messages on Email and Instant Messaging are not secure by default. Messages sent and received are not encrypted and can be captured by the Network Sniffer, if installed on the internet cafe computer. Do not send emails or messages by instant messenger which contain sensitive information. If we need to send a sensitive message, consider using a browser which utilises the "Tor anonymity network" (a technology to maintains anonymity). The Tor project are now offering a portable browse built upon firefox. This offering is knows as the Tor Browser Bundle and can be downloaded from the link previous. The Tor Bundle is a free which can be run off a USB flash memory. The Tor network is rather slow, however it will ensure your session is encrypted and the Sniffer in the cyber cafe rendered useless. Be aware that there are Tor Browser Bundle has limitations such as flash video and javascript are disabled and do not work. This may result in certain websites not functioning. So it may be better to fire up Tor Browser Bundle when you need to send something sensitive or keep your anonymity in the internet cafe. On-line Banking on the other hand is quite secure as your session is normally encrypted (provided the machine has not been compromised (e.g. modified hosts file) to redirect the online banking requests to a phishing site) or your credentials stolen by a keylogger trojan.

Keyloggers:

There are various approaches that can take to protect against keyloggers. There are suggestions on other websites that using virtual keyboards or cut and paste methods can bypass the keyloggers. The author has tested a few virtual keyboards that are marketed as offering protection against keyloggers, however the the keystrokes have been captured. Virtual keyboards certainly offer protection to hardware keyloggers, however sophisticated software keyloggers, sometimes installed as spyware / trojans can capture input from 'cut and paste' and virtual keyboard keypresses.

b) Manual or Electronic Credit Card Imprints

Data from a legitimate card is imprinted or the magnetic strip is skimmed. The information from the card is then later used for fraudulent transactions or for encoding fake cards.

Card-not-present (CNP) fraud
Credit card fraud can be perpetrated against you if the account number and expiry date of your card are known. The fraud may be by way of mail, phone or internet and does not require your physical card to be present unless the merchant requests the card verification code.

Counterfeit card fraud
This fraud usually involves skimming. The data is then transferred onto a fake magnetic stripe card. A skimmed counterfeit is used to produce a fully functional counterfeit card. There is an exact copy of the magnetic stripe.

Lost and stolen card fraud
This occurs when your card is physically stolen or lost and then used by a criminal, posing as you, to make unauthorized charges on your account.

Card ID theft
This occurs when a criminal has managed to obtain details about your card and uses the information to open or take over a card account in your name.
Mail non-receipt card fraud aka intercept fraud aka never received issue.

Doctored Cards
The metallic stripe on a card can be erased using a strong magnet. A criminal will do this and then alter details on the card to match those of a valid card. The card will not work and the criminal will then con the merchant into punching in the card details manually.

Fake Cards
Producing fake cards takes a lot of time, effort and skill. There are many security features particularly difficult to reproduce, for example, holograms.

Account Takeover
This can happen when a criminal, having gathered Manual or Electronic Credit Card Imprints.
Data from a legitimate card is imprinted or the magnetic strip is skimmed. The information from the card is then later used for fraudulent transactions or for encoding fake cards.

Card-not-present (CNP) fraud
Credit card fraud can be perpetrated against you if the account number and expiry date of your card are known. The fraud may be by way of mail, phone or internet and does not require your physical card to be present unless the merchant requests the card verification code.

3. What are the probable punishment in the following cases?
a) Publication for fraudulent purpose.
b) Disclosure of information in breach of contract.
c) Publication and transmission of containing sexually explicit act or conduct.
d) Cyber terrorism.
e) Hacking with computer system.

[WBUT 2018]

Answer:
a) Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years or with a fine which may extend to 2 lakh rupees, or with both.

b) Any act of mishandling, misappropriation or misuse of confidential information is also punishable under the Penal Code. When a person misappropriates confidential information that has been entrusted to him or her without authorization, such act amounts to a criminal breach of trust under Section 405 of the Penal Code. In a criminal breach of trust, entrustment of property (in this case, confidential company information) is the essential element. The accused is entrusted with property and with dominion or control over that property. In addition, any person who dishonestly misappropriates or converts for his or her own use any moveable property (in this case, confidential information) shall be liable for dishonest misappropriation under Section 403 of the Penal Code. Such an offence shall be punishable by up to two years' imprisonment, a fine or both.

c) Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

d) Whoever with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—
(i) denying or cause the denial of access to any person authorized to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
(iii) introducing or causing to introduce any computer contaminant,
and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70.
Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or

incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.
Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

e) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

4. Write short notes on the following: **[MODEL QUESTION]**
a) Digital signatures
b) Public key certificate
c) RSA

Answer:

a) Digital signatures:

A digital signature scheme typically consists of three algorithms:
A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
A signing algorithm that, given a message and a private key, produces a signature.
A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.
Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. Applications of digital signatures are authentication, integrity, non-repudiation. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. On the other hand the sender cannot deny that he has sent that document, which is called non-repudiation. As asymmetric key algorithm is used for data encryption the integrity of the message is ensured to the receiver.

b) Public key certificate:

A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. The public key infrastructure uses public key

cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. A public key infrastructure consists of:

- A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key
- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
- One or more directories where the certificates (with their public keys) are held
- A certificate management system

In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. Sender uses public key of the receiver to encrypt the message while receiver uses private key is used to decrypt text.

c) RSA algorithm:

Choose two large prime numbers P and Q.
Calculate $N = P \times Q$.
Select the public key (i.e. the encryption key) E such that it is not a factor of $(P - 1)$ and $(Q - 1)$.
Select the public key (i.e. the encryption key) E such that the following equation is true:
$(D \times E) \bmod (P - 1) \times (Q - 1) = 1$.
For encryption, calculate the cipher text CT from the plain text PT as follows:
$CT = PT^E \bmod N$.
Send CT as the chipper text to the receiver.
For decryption, calculate the plain text PT from the cipher text CT as follows:
$PT = CT^D \bmod N$.

QUESTION 2015

Group – A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for any ten of the following:

i) Sniffing is a technique used for
- a) Attacks on computer hardware
- b) Attacks on computer software
- c) Attacks on operating system
- ✓d) Attacks on wireless network

ii) Which of the following is a social engineering site?
- ✓a) ebay
- b) Facebook
- c) Amazon
- d) CWB

iii) Section 67 of ITA 2000 is associated with which of the following cybercrime?
- a) Tempering with computer source documents
- b) Misrepresentation
- c) Publishing digital signature in false
- ✓d) Transmitting obscene material in electronic from

iv) Skimming means
- ✓a) Stealing ATM PIN information
- b) Stealing telephone information
- c) Stealing identity
- d) None of these

v) What is the full form of CERT/CC?
- a) Computer Engineering Response Team Co-ordination Centre
- b) Computer Emergency Record Team Co-ordination Centre
- ✓c) Computer Emergency Response Team Co-ordination Centre
- d) Computer Engineering Record Team Co-ordination Centre

vi) Steganography is used in
- ✓a) Digital imaging
- b) Digital watermarking
- c) Digital signal processing
- d) Photoshop

vii) Changing of raw data is known as
- a) Salami attack
- ✓b) Data diddling
- c) Forgery
- d) Web Jacking

viii) Pharming is used for
- a) Data hiding
- ✓b) Data alteration
- c) Hosts file poisoning
- d) File overriding

ix) LDAP stands for
- ✓a) Lightweight Directory Access protocol
- b) Lightweight Data Access Protocol
- c) Lightweight Domain Access Protocol
- d) Lightweight DNS Access protocol

x) The term 'Bluetooth' has been taken from
- a) Danish blue sea
- b) Fine blue sea
- ✓c) Danish king Harald Batand
- d) Norway hill

Group – B

(Short Answer Type Questions)

2. Discuss about the impact of IT act amendments on IT organizations.

See Topic: CYBERCRIME AND CYBERSECURITY, Short Answer Type Question No. 1.

3. What is SQL injection? How it can be prevented?

See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Short Answer Type Question No. 1.

4. What is vishing? What are different vishing techniques?

See Topic: PHISING AND IDENTITY THEFT, Short Answer Type Question No. 1.

5. What is software piracy? Discuss about the preventive measures against software piracy

See Topic: INTRODUCTION TO CYBERCRIME, Short Answer Type Question No. 1.

6. Define Identity Theft (ID Theft). Write down the different technique of ID Theft.

See Topic: PHISING AND IDENTITY THEFT, Short Answer Type Question No. 2.

Group – C

(Long Answer Type Questions)

7. a) What is DoS Attacks? Write down the tools used to launch DDoS attacks.
b) Write down the types or levels of DoS attacks?
c) Define Trojan virus with example.

See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Long Answer Type Question No. 1.

8. a) Define The IT Act 2000. Write down the positive aspect of the ITA 2000.
b) Write down the main object of IT act 2000.
c) Write down the amendments to the Indian IT Act.

See Topic: CYBERCRIME AND CYBERSECURITY, Long Answer Type Question No. 1.

9. a) What is phishing? Write down the different types of modern Phishing techniques.
b) Explain the different method of Phishing.
c) Write down the different phishing countermeasures.

See Topic: PHISING AND IDENTITY THEFT, Long Answer Type Question No. 1.

10. a) Write down the basic safety and security tips to prevent Cybercafe from cyber threat.
b) Write down the types and techniques of Credit card frauds.
c) Write down the difference between Computer Virus and Worm.
a) **See Topic: CYBERCRIME AND CYBERSECURITY, Long Answer Type Question No. 2(a).**
b) **See Topic: CYBERCRIME AND CYBERSECURITY, Long Answer Type Question No. 2(b).**
c) **See Topic: TOOLS AND METHODS USED IN CYBER CRIME, Short Answer Type Question No. 2.**

11. Write the short notes any three of the following:
a) Social Engineering and Cybercrime
b) Active attacks
c) Hacking Cybercrime
d) Botnet
e) Cyber stalking
f) Mobile viruses
a) See Topic: PHISING AND IDENTITY THEFT, Long Answer Type Question No. 4(a).
b) See Topic: CATEGORY OF CYBERCRIME, Long Answer Type Question No. 4(a).
c) See Topic: CATEGORY OF CYBERCRIME, Long Answer Type Question No. 4(b).
d) See Topic: TOOLS AND METHODS USED IN CYBER CRIME, Long Answer Type Question No. 2.
e) See Topic: CATEGORY OF CYBERCRIME, Long Answer Type Question No. 4(c).
f) See Topic: CYBERCRIME MOBILE AND WIRELESS DEVICES, Long Answer Type Question No. 6(a).

QUESTION 2016

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for any ten of the following:

i) The notorious art of breaking into phone or other communication systems is known as
a) hacking b) cracking ✓c) phreaking d) none of these

ii) The name of the virus that will erase all IMEI and IMSI information from both your phone and SIM card is
a) TDL-4 ✓b) XALAN c) SCA d) MDEF

iii) The term ..... refers to a bad or criminal hacker.
✓a) black hat b) white c) gray hat d) none of these

iv) Which one is true?
✓a) bluesnarfing is claimed to be much more serious than bluejacking
b) bluejacking is claimed to be much more serious than bluesnarfing
c) bluejacking is claimed to be same serious as bluesnarfing
d) none of these

v) Creating a fake website which looks very identical to a real website is called
a) sniffing b) spoofing c) hijacking ✓d) phishing

vi) DOS attack is caused by
a) authentication b) alteration ✓c) fabrication d) replay attacks

vii) A ..... replicates itself by creating its own copies, in order to bring the network to halt.
✓a) virus b) worm c) Trojan horse d) bomb

viii) Total number of cyber-crime cases were registered under the Indian IT act in 2007 is
a) 210 b) 207 c) 212 d) 211

ix) A defense method that is effective today may not remain so for long because
a) defense method become obsolete
b) defense method may expire
✓c) attackers are constantly updating attacks vectors
d) none of these

x) Indian Parliament passed ITA 2000 on
a) 15th August, 2000 ✓b) 17th May, 2000
c) 12th August, 2000 d) 12th May, 2000

Group – B
(Short Answer Type Questions)

2. What are the different types of cybercriminals? Explain each one briefly.
See Topic: INTRODUCTION TO CYBERCRIME, Short Answer Type Question No. 2.

3. What is hacking? Differentiate between white-hat hacking and black-hat hacking.
See Topic: INTRODUCTION TO CYBERCRIME, Short Answer Type Question No. 3.

4. What is virus hoax? Describe computer worm briefly.
See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Short Answer Type Question No. 3.

5. Explain the different types of Identity Theft briefly.
See Topic: PHISING AND IDENTITY THEFT, Short Answer Type Question No. 2.

6. What is the meaning of the term 'cyber law'? Write the advantages of cyber law briefly.
See Topic: CYBERCRIME AND CYBERSECURITY, Short Answer Type Question No. 2.

Group – C

(Long Answer Type Questions)

7. What is cyberspace? Describe the different types of cybercrimes briefly. Discuss the phases involved in planning cybercrime. Explain Cyber defamation briefly.

See Topic: INTRODUCTION TO CYBERCRIME, Long Answer Type Question No. 1.

8. Write the concept of 'Botnet' briefly. Discuss the different types of social engineering. Is there any risk for cloud computing from cybercrime? Justify it. Define Vishing.

Answer:

1st part: See Topic: TOOLS AND METHODS USED IN CYBER CRIME, Long Answer Type Question No. 2.

2nd part: See Topic: PHISING AND IDENTITY THEFT, Long Answer Type Question No. 2.

3rd part: See Topic: INTRODUCTION TO CYBERCRIME, Long Answer Type Question No. 2.

4th part: See Topic: PHISING AND IDENTITY THEFT, Short Answer Type Question No.1.(1st part)

9. What is a dictionary password cracking technique? How can we key loggers be used to commit a cybercrime? "The rapid application of wireless devices has increased the chances of cybercrimes" explain. Write the different tools used to launch DoS attack. Define SQL injection.

See Topic: TOOLS AND METHODS USED IN CYBER CRIME, Long Answer Type Question No. 3.

10. Differentiate between whaling and Spear Phishing. Write the different Phishing techniques briefly. Write the positive aspects and weak areas of the ITA 2000.

1st part: See Topic: PHISING AND IDENTITY THEFT, Short Answer Type Question No.3.

2nd part: See Topic: PHISING AND IDENTITY THEFT, Long Answer Type Question No.1.a).(2nd part).

3rd part: See Topic: CYBERCRIME AND CYBERSECURITY, Long Answer Type Question No. 1.a).

11. Write short notes on any three of the following:

a) Cyber stalking

b) Trojan Horse

c) DDoS attack

d) Software Piracy

e) Tabjacking

a) See Topic: CATEGORY OF CYBERCRIME. Long Answer Type Question No. 4(c).

b) See Topic: TOOLS AND METHODS USED IN CYBER CRIME, Long Answer Type Question No. 7.a).

c) See Topic: TOOLS AND METHODS USED IN CYBER CRIME, Long Answer Type Question No. 7.b).

d) See Topic: INTRODUCTION TO CYBERCRIME, Long Answer Type Question No. 6.

e) See Topic: TOOLS AND METHODS USED IN CYBER CRIME, Long Answer Type Question No. 7.c).

QUESTION 2017

Group – A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for any ten of the following:

i) Access to a computer program that bypasses security mechanism is called

✓a) Backdoor — b) Trojan horse

c) Strom Worm — d) None of these

ii) The method in which the Phishes identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data

a) Dragnet — ✓b) Rod and reel

c) Gillnet — d) Lodsterpot

iii) The attacker setup typo and matching domain names of the target and install websites for similar look and feel is

a) Phishing — ✓b) Pharming

c) Backup theft — d) None of these

iv) Sniffing is a technique used for

a) Attacks on computer hardware — b) Attacks on computer software

c) Attacks on operating system — ✓d) Attacks on wireless network

v) Which of the following is India's first cyber law?

a) ITA 1998 — b) ITA 1999

✓c) ITA 2000 — d) ITA 2001

vi) The use of the Internet or other electronic means to stalk or harass an organization is termed

a) Cyberspace — ✓b) Cyber stalking

c) Pornography — d) None of these

vii) What type of attack relies in the trusting nature of employees and the art of deception?

✓a) Social Engineering — b) Fraud

c) Phishing — d) Dumpster Diving

viii) This is a program in which malicious or harmful code is contained inside apparently harmless programming or data

a) War dialer — b) Spam trap

✓c) Trojan horse — d) Email

ix) Vishing is mean for
a) SMS Phishing
✓b) Voice Phishing
c) Phishing
d) All of these

x) In cyber law terminology 'DDoS' means
✓a) Distributed Denial of Service
b) Disc Operating System
c) Distant Operator Service
d) None of these

Group – B

(Short Answer Type Questions)

2. Explain the difference between hackers, Crackers and Phreakers.
See Topic: INTRODUCTION TO CYBERCRIME, Short Answer Type Question No. 4.

3. What is Phishing? What are the different methods of Phishing attack?
See Topic: PHISING AND IDENTITY THEFT, Long Answer Type Question No. 1.a).

4. What is Trojan Horse? What is the difference between Trojan Horse and Backdoors?
See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Short Answer Type Question No. 4.

5. Discuss briefly about proxy server.
See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Short Answer Type Question No. 5.

6. What is SQL injection? How it can be prevented?
See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Short Answer Type Question No. 1.

Group – C

(Long Answer Type Questions)

7. a) Define Cybercrime? Discuss about various types of Cybercrime.
b) Discuss about email spoofing and email spamming
c) What is Reconnaissance in the world of Hacking?
d) What is Salami Attack?
a) See Topic: CATEGORY OF CYBERCRIME, Long Answer Type Question No. 1.
b) See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Long Answer Type Question No. 4.
c) See Topic: CATEGORY OF CYBERCRIME, Short Answer Type Question No. 1.
d) See Topic: CATEGORY OF CYBERCRIME, Short Answer Type Question No. 2.

8. a) Define Cyber stalking. How stalking works?
b) Explain the difference between passive and active attacks.
c) Explain the different attacks launched with attack vector.
d) What is Cyber bullying?
a) See Topic: CATEGORY OF CYBERCRIME, Long Answer Type Question No. 2.
b) See Topic: CATEGORY OF CYBERCRIME, Short Answer Type Question No. 3.
c) See Topic: PHISING AND IDENTITY THEFT, Long Answer Type Question No. 2.

d) See Topic: CATEGORY OF CYBERCRIME, Short Answer Type Question No. 4.

9. a) What is the difference between Staganography and Cryptography?
b) What are the different kinds of attacks on mobile/cell phones? Explain with examples.
c) What is blind SQL injection attack? How can it be prevented?
d) What is forgery?
a) See Topic: CYBERCRIME AND CYBERSECURITY, Short Answer Type Question No. 3.
b) See Topic: CYBERCRIME MOBILE AND WIRELESS DEVICES, Long Answer Type Question No. 1.
c) See Topic: INTRODUCTION TO CYBERCRIME, Long Answer Type Question No. 3.
d) See Topic: INTRODUCTION TO CYBERCRIME, Short Answer Type Question No. 5.

10. a) What is ID theft? What are the techniques of ID theft?
b) What are steps to protect Dos/DDos attack?
c) What is buffer overflow? Discuss about the types of buffer overflow.
d) What is DNS redirection?
a) See Topic: PHISING AND IDENTITY THEFT, Short Answer Type Question No. 2.
b) See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Short Answer Type Question No. 6.
c) See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Long Answer Type Question No. 5.
d) See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Short Answer Type Question No.7.

11. Write the short notes any *three* of the following:
a) Spear Phishing
b) Backdoor
c) Smishing
d) WAP kitting and WAP jacking
e) Dos and DDos
a) See Topic: PHISING AND IDENTITY THEFT, Long Answer Type Question No. 4(b).
b) See Topic: CATEGORY OF CYBERCRIME, Long Answer Type Question No. 4(d).
c) See Topic: PHISING AND IDENTITY THEFT, Long Answer Type Question No. 4(c).
d) See Topic: CYBERCRIME MOBILE AND WIRELESS DEVICES, Long Answer Type Question No. 6(b).
e) See Topic: TOOLS AND METHOD USED IN CYBERCRIME, Long Answer Type Question No. 7.d).

QUESTION 2018

Group – A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for *any ten* of the following:
i) Section 66F of IT Act deals with
a) cyber stalking
b) e-mail bombing
c) child pornography
✓d) cyber terrorism

ii) Skimming means
✓a) stealing ATM PIN information
b) stealing telephonic information
c) stealing identity
d) none of these

iii) What is full form of CERT/CC?
a) Computer Engineering Response Team Co-ordination Center
b) Computer Emergency Record Team Co-ordination Center
✓c) Computer Emergency Response Team Co-ordination Center
d) Computer Engineering Record Team Co-ordination Center

iv) Pharming is used by
a) data hiding
✓b) data alteration
c) hosts file poisoning
d) file overriding

v) Access to a computer program that by passes security mechanism called
✓a) back door
b) Trojan horses
c) storm worm
d) none of these

vi) The tool that acts like an offline browser is
✓a) HT track
b) e-mail traker pro
c) trace route
d) none of these

vii) The name of the virus that will erase all IMEI and IMSI information both from your phone and SIM card is
a) IDI-4
✓b) XALAN
c) SCA
d) MDEF

viii) Which program generates random packets to launch DOS attack?
a) jolt 2
b) targa
✓c) nemesy
d) all of these

ix) Which of the following is the India's first Cyber Law?
✓a) ITA 2000
b) ITA 1999
c) ITA 1998
d) ITA 2001

x) India's first cyber police station is located at
a) Delhi
✓b) Bangalore
c) Chennai
d) Mumbai

xi) LDAP stands for
✓a) Light Weight Directory Access Protocol
b) Light Weight Data Access Protocol
c) Light Weight Domain Access Protocol
d) Light Weight DNS Access Protocol

xii) Changing of raw data is known as
a) salami attack
✓b) data diddling
c) forgery
d) web jacking

Group – B
(Short Answer Type Questions)

2. Define Vishing. State different Vishing techniques.
See Topic: PHISHING & IDENTITY THEFT, Short Answer Type Question No. 1.

3. Describe different types of cyber criminals and explain each one briefly.
See Topic: INTRODUCTION OF CYBERCRIME, Short Answer Type Question No. 2.

4. What is the difference between proxy server and anonymizer?
See Topic: TOOLS AND METHODS USED IN CYBER CRIME, Short Answer Type Question No. 9.

5. What is blind SQL injection? How it can be prevented?
See Topic: INTRODUCTION OF CYBERCRIME, Long Answer Type Question No. 3.

6. Discuss about the impact of IT act amendments on IT Organization.
See Topic: CYBERCRIME & CYBERSECURITY, Short Answer Type Question No. 1.

Group – C
(Long Answer Type Questions)

7. a) Describe the steps to reduce cyber risk.
b) Who are the cyber criminals?
See Topic: CATEGORY OF CYBERCRIME, Long Answer Type Question No. 3.

8. a) What is information? What information should you protect? What are the risks to you information and how much risk can you accept?
b) How can you ensure that you have the best possible understanding of the threat to you business?
c) How do you embed risk management within your computer?
See Topic: CYBERCRIME & CYBERSECURITY, Long Answer Type Question No. 2.

9. a) What would happen to the business if one of your risks becomes a reality?
b) Describe CKC in details.
c) Define Depth of defence (DoD).
d) What is criminal revenue?
a), b) & d) See Topic: CYBERCRIME & CYBERSECURITY, Long Answer Type Question No. 3.
c) See Topic: CATEGORY OF CYBERCRIME, Short Answer Type Question No. 5.

10. a) Differentiate direct and indirect losses for cyber crime.
b) What is the methodology for assessing the impact of IP theft?
c) What is the impact of cyber crime?
a) See Topic: INTRODUCTION OF CYBERCRIME, Long Answer Type Question No. 4.

b) See Topic: CYBERCRIME MOBILE & WIRELESS DEVICES, Long Answer Type Question No. 4.
c) See Topic: CYBERCRIME & CYBERSECURITY, Short Answer Type Question No. 5.

11. a) How easy is it to exploit stolen IP?
b) What do cyber criminal targets?
c) What are the steps to protect your mobile phone from cyber crime?
a) See Topic: CYBERCRIME & CYBERSECURITY, Long Answer Type Question No. 4.
b) See Topic: INTRODUCTION OF CYBERCRIME, Long Answer Type Question No. 5.
c) See Topic: CYBERCRIME MOBILE & WIRELESS DEVICES, Long Answer Type Question No. 5.

12. a) What do you do if you become a victim of phishing and pharming?
b) Define Virus, Worm and Trojan horse.
a) See Topic: PHISHING & IDENTITY THEFT, Long Answer Type Question No. 3.
b) See Topic: TOOLS AND METHODS USED IN CYBER CRIME, Long Answer Type Questions No. 6.

13. What are the probable punishment in the following cases?
a) Publication for fraudulent purpose.
b) Disclosure of information in breach of contract.
c) Publication and transmission of containing sexually explicit act or conduct.
d) Cyber terrorism.
e) Hacking with computer system.
See Topic: CYBERCRIME & CYBERSECURITY, Long Answer Type Question No. 3.