Q.1 Mention different tools used in cyber crime.

Ans:

1. WIRESHARK

Formerly known as Ethereal, Wireshark is open-source network software that can efficiently analyze network protocols and enhance security in real time. Since it is a console-based password auditing and packet sniffer tool, you can use this security software to sniff the network and monitor your network traffic in real time. Security professionals use this efficient software to capture data packets and inspect the features that particular data packets exhibit, which further helps to identify the weaknesses in network security.

2. KALI LINUX

Kali Linux is one of the organizations' most excellent penetration testing tools to scan their IT systems and networks for vulnerabilities. This cybersecurity tool contains around 300 different software used for security auditing. Most of these tools are executable, which simply means that the users can monitor and maintain their network security systems with a single click. The most common characteristic of Kali Linux is that all types of users, from experienced to newbies, can use it to reinforce their security in networking. It does not need any specific set of expertise or degree to function.

3. JOHN THE RIPPER

Professionals use John the Ripper for testing password strength. This tool can quickly look for complex ciphers, encrypted logins, and hash-type passwords and identify weak passwords, which can be a big threat to a protected system. The software can efficiently work with Windows, DOS, OpenVMS systems, and Unix environments.

4. METASPLOIT

Metasploit is one of the best security software that contains various tools for executing penetration testing services. Professionals use this tool to attain varying security goals, such as discovering vulnerabilities in the system, strengthening computer system security, weaving cyber defense strategies, and maintaining complete security assessments. These penetration testing tools can examine different security systems, including web-based apps, servers, networks, and so on. Metasploit can instantly identify all the new security vulnerabilities as soon as they occur, thus maintaining top-notch security all the time.

5. CAIN AND ABEL

It is a password auditing and packet sniffer network security tool used to discover Windows operating system weaknesses. IT experts rely on this software to strengthen security in networking and identify vulnerabilities in the Windows security password. You can use this free tool to discover password flaws and recover them accordingly. ‘Cain and Abel’ contains many functionalities, such as recording VoIP communications, analyzing routing protocols, decoding scrambled passwords, cracking encrypted passwords, etc. Also, this software is highly effective in cryptanalysis. You can consider using this security tool as a good start for all kinds of packet sniffing exercises.

6. TCPDUMP

Tcpdump is one of the most efficient packet sniffer security tools used to monitor and log TCP/IP traffic connected via a network. Since it is a command-based tool, it can efficiently define network security and the packet contents of system traffic.

7. NIKTO

Nikto is open-source security software that detects web vulnerabilities and takes appropriate actions accordingly. The software contains a database that includes around 6400 different threats. Security professionals keep updating this database so that the users may easily identify the new vulnerabilities.

8. FORCEPOINT

Forcepoint is a customizable security tool primarily designed for cloud users. The tool defines network security, restricts users from accessing particular content, and blocks various intrusion attempts. The security admins can customize Forcepoint's SD-Wan to quickly monitor and quickly detect dubious acts in a network and rapidly implement appropriate action. The tool adds an extra level of protection for more critical threats.

9. PAROS PROXY

Paros Proxy is a Java-based security tool that contains a variety of other tools like vulnerability scanners, traffic recorders, web spiders, etc. Professionals use these tools to scan security tests for identifying web vulnerabilities and maintaining network activities in real-time.

10. NMAP

Also known as Network Mapper, Nmap is a free network discovery and security auditing tool professionals use to scan single hosts and large networks. Its key features include detecting unidentified devices and identifying network issues for testing security vulnerabilities.

Q.2 Describe the following term.

Ans: Keylogger:-

Keylogger is a malicious computer program that records everything you type on the keyboard and learns the keystroke pattern including words, characters, symbols and sends all the recorded details to the malicious hackers.

But technically, keyloggers are software. There has been a misconception that Keyloggers are always used for criminal purposes. In reality, Keyloggers have professional and legal usage also.

Imagine an invisible camera kept above your keyboard which records everything you type and sends it to the person who kept it. These are called as Keyloggers.

It can be used by parents who want to monitor their children's activities or Companies that want to monitor their employees from doing malicious activities.

Keyloggers are sometimes enclosed with other malware like trojans, worms or viruses. This stealthy little software can analyze your keystrokes and predict what you are typing on the computer.

Keylogger Infographic Pic: Cybersecuritynews.com

For instance, if you are typing fb.com or facebook.com, obviously the next thing you are going to enter is your credentials. In this way, the keylogger will store the rest of the keystrokes as "username" and "password".

Keyloggers are very hard to detect when you are a normal computer user. They are responsible for lots of password stealing, credit card hijacking and other major malicious activities.

Type of Keyloggers

i) Hardware Keyloggers: Devices that can be attached in our computer which will act as a keylogger and collects information about the specified

target.
ii) Software keyloggers: Probably a malicious program that does not infect your system but still can steal your passwords, account details, etc.

How does Keylogger work?

Just like any other malicious program that sends its reports to the attackers, keyloggers also send information about keystrokes that a victim enters in his/her keyboard to its creator or a remote server or a specified email address.

Keyloggers are hidden so deep that even some antivirus programs can't detect. Professionally designed keyloggers get embedded with the operating system kernel which makes it too difficult to detect by antiviruses. Keyloggers are one of the dangerous and stealthy.

How to Protect From Keyloggers?

- Do not download any attachments from unknown websites.
- Keep your AntiVirus software updated.
- Use Virtual Keyboards which will prevent typing keystrokes.
- Use Two-Factor Authentication Methods on important sites.
- User firewall and password manager

2. Steganography :-

The word **Steganography** is derived from two Greek words- 'stegos' meaning 'to cover' and 'grayfia', meaning 'writing', thus translating to 'covered writing', or 'hidden writing'. **Steganography** is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

How is it different from cryptography?
Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable, or hides the *meaning* of the data, while steganography hides the *existence* of the data.
In layman's terms, cryptography is similar to writing a letter in a secret language: people can read it, but won't understand what it means. However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either knows or figures out your secret language, then your message can easily be read.

If you were to use *steganography* in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter. To those who don't know about the message, it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for, and finds the message hidden in them.
Similarly, if two users exchanged media files over the internet, it would be more difficult to determine whether these files contain hidden messages than if they were communicating using cryptography.

Cryptography is often used to supplement the security offered by steganography. Cryptography algorithms are used to encrypt secret data before embedding it into cover files.

Image Steganography –
As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the **cover image** and the image obtained after steganography is called the **stego image**.

How is it done?
An image is represented as an N*M (in case of greyscale images) or N*M*3 (in case of color images) matrix in memory, with each entry representing the intensity value of a pixel. In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm. The recipient of the image must be aware of the same algorithm in order to know which pixels he or she must select to extract the message.

3. SQL Injection :-

SQL injection is a technique used to exploit user data through web page inputs by injecting SQL commands as statements. Basically, these

statements can be used to manipulate the application's web server by malicious users.

- SQL injection is a code injection technique that might destroy your database.
- SQL injection is one of the most common web hacking techniques.
- SQL injection is the placement of malicious code in SQL statements, via web page input.

Exploitation of SQL Injection in Web Applications

Web servers communicate with database servers anytime they need to retrieve or store user data. SQL statements by the attacker are designed so that they can be executed while the web-server is fetching content from the application server.It compromises the security of a web application.

Impact of SQL Injection

The hacker can retrieve all the user-data present in the database such as user details, credit card information, social security numbers and can also gain access to protected areas like the administrator portal. It is also possible to delete the user data from the tables.
Nowadays, all online shopping applications, bank transactions use back-end database servers. So in-case the hacker is able to exploit SQL injection, the entire server is compromised.

Preventing SQL Injection

- User Authentication: Validating input from the user by pre-defining length, type of input, of the input field and authenticating the user.
- Restricting access privileges of users and defining as to how much amount of data any outsider can access from the database. Basically, user should not be granted permission to access everything in the database.
- Do not use system administrator accounts.

Q.3 Differentiate between DOS attack and DDoS attack.

Ans:

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.

DOS	DDOS
In Dos attack single system targets the victim system.	In DDoS multiple systems attacks the victims system..
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple location.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDoS attack,The volumeBots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in the Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

Q.4 Explain different malicious software Virus , Worms And Torjon Horses.

Ans:

Virus:

Virus is a computer program or software that connect itself to another software or computer program to harm computer system. When the computer program runs attached with virus it perform some action such as deleting a file from the computer system. Virus can't be controlled by remote.

Worms:

Worms is also a computer program like virus but it does not modify the program. It replicate itself more and more to cause slow down the computer system. Worms can be controlled by remote.

Trojan Horse:

Trojan Horse does not replicate itself like virus and worms. It is a hidden piece of code which steal the important information of user. For example, Trojan horse software observe the e-mail ID and password while entering in web browser for logging.

Difference between Virus, Worm and Trojan Horse:

Virus	Worm	Trojan Horse
Virus is a software or computer program that connect itself to another software or computer program to harm computer system.	Worms replicate itself to cause slow down the computer system.	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
Virus replicates itself.	Worms are also replicates itself.	But Trojan horse does not replicate itself.
Virus can't be controlled by remote.	Worms can be controlled by remote.	Like worms, Trojan horse can also be controlled by remote.
Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse.	And spreading rate of Trojan horse is slow in comparison of both virus and worms.
The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.

Viruses are executed via executable files.	Worms are executed via weaknesses in system.	Trojan horse executes through a program and interprets as utility software.

Q.5 differentiate between toxic server ans anonymiser.

Ans:

Q.6 Mention different types of worms and life cycle in cyber security.

Ans:

A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers.[1] It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue.[2] Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on the law of exponential growth, thus controlling and infecting more and more computers in a short time.[3] Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Many worms are designed only to spread, and do not attempt to change the systems they pass through. However, as the Morris worm and Mydoom showed, even these "payload-free" worms can cause major disruption by increasing network traffic and other unintended effects.

Life-Cycle Manager

Some worm writers prefer to run a version of a computer worm for a preset period of time. For instance, the W32/Welchia.A worm "committed suicide" in early 2004, and then the B variant of Welchia was released in late February of 2004 to run for three more months. On the other hand, many worms have bugs

in their life-cycle manager component and continue to run without ever stopping. Furthermore, we often encounter variants of computer worms that were patched by others to give the worm "endless" life.

Consider the statistics collected on an individual Welchia honeypot administered by Frederic Perriot between August 2003 and February 2004, shown in Figure 9.1. The sudden drop of Welchia is related to its life-cycle manager, which triggers the worm's self-killing routine.

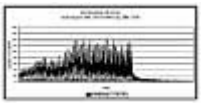


Figure 9.1 The suicide of Welchia worm.

The cumulative number of distinct Welchia attacking systems was around 30,000 when the worm started to kill itself when observed on a particular DSL network (see Figure 9.2).

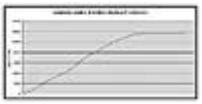


Figure 9.2 The cumulative number of Welchia attackers.

Q.7 what are the features of IT Act 2000.

Ans: In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce (e-commerce) to bring uniformity in the law in different countries.

Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000.

Features of the Information Technology Act, 2000

a. All electronic contracts made through secure electronic channels are legally valid.

b. Legal recognition for digital signatures.

c. Security measures for electronic records and also digital signatures are in place

d. A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized

e. Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.

f. An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court

g. Digital Signatures will use an asymmetric cryptosystem and also a hash function

h. Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.

i. The Act applies to offences or contraventions committed outside India

j. Senior police officers and other officers can enter any public place and search and arrest without warrant

k. Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

Q.8 why IT abdonment act was introduced and what are its feature.

Ans: The IT Amendment Act, 2008 was passed by the Parliament with an intention to curb the growing malady relating to the IT industry. The present

article highlights some of the new/modified provisions relating to Data Protection, Privacy and Cyber Crime and try to analyse how effective these modifications will be to ensure some dynamism in the IT Act.

Whilst the focus of the Information Technology Act, 2000 ("IT Act) was clearly recognition of electronic records and facilitation of E-Commerce, that of the Information Technology (Amendments) Act, 2008[1] ("ITA, 2008") is clearly Cyber Terrorism and to a significant extent, Cyber Crime. A little bit of the background first - the Ministry of Information Technology first posted a draft of proposed amendments to the IT Act in 2005. Thereafter in 2006, the IT Bill was tabled with substantial changes brought about by consensual and plentiful objections to the proposed amendments of 2005. The ITA, 2008, passed with marked haste by the parliament in December 2008 contains a lot of the changes proposed in the IT Bill of 2006 but contains sizeable additions and modifications to it, which appear to be a knee-jerk reaction to the recent spate of terror attacks.

Features:-

- **Incorporation of Electronic Signature:** To go by their aim of making the act ‘technologically neutral, the term ‘digital signature’ has been replaced with ‘electronic signature’, as the latter represents an umbrella term which encompasses many different types of digital marketing, while the former is a specific type of electronic signature.

- **Fight against Cyber-terrorism:** Pursuant to the 26/11 Mumbai Attacks, the amendment has incorporated the concept of cyber terrorism and prescribed hefty punishments for it. The scope of cybercrime under Section 66 is widened with many major additions defining various cybercrimes along with the controversial Section 66A which penalized sending “offensive messages”. Section 66A was later found to be in violation of one’s fundamental right to freedom of speech and expression and thus was struck down.

- **Child Pornography:** Along with reducing the term of imprisonment and increasing the fine for publishing obscene material in electronic form, an array of sections have also been inserted under Section 67, one among which recognizes publishing child pornography as a felonious act.

- **Cyber Cafes:** Cybercrimes like sending obscene e-mails to harass individuals, identity theft, and maliciously acquiring net banking passwords have many at times been taking place at Cyber Cafes. Due to the lack of inclusion of ‘Cyber Cafes’ in the IT Act, they are incapable of being regulated. The 2008 amendment explicitly defines them and includes them under the term ‘intermediaries’, thus allowing several aspects of the Act to be applicable to them. This lead to an great movement of the government that they did IT Act 2000 amendment which became information technology amendment act 2008.

- **Government Interception and Monitoring:** The new amendment allows the government to listen in to your phone calls, read your SMS’s and emails, and monitor the websites you visit without getting a warrant from a magistrate. The same clause under the Telegraph Act was restricted by the condition of public emergency or safety, but the new amendment drops all such restrictions, vastly extending the government’s power.

Q.9 what is digital signature.

Ans: Digital Signature

A digital signature is a mathematical technique which validates the authenticity and integrity of a message, software or digital documents. It allows us to verify the author name, date and time of signatures, and authenticate the message contents. The digital

signature offers far more inherent security and intended to solve the problem of tampering and impersonation (Intentionally copy another person's characteristics) in digital communications.

The computer-based business information authentication interrelates both technology and the law. It also calls for cooperation between the people of different professional backgrounds and areas of expertise. The digital signatures are different from other electronic signatures not only in terms of process and result, but also it makes digital signatures more serviceable for legal purposes. Some electronic signatures that legally recognizable as signatures may not be secure as digital signatures and may lead to uncertainty and disputes.

Application of Digital Signature

The important reason to implement digital signature to communication is:

- Authentication
- Non-repudiation
- Integrity

Authentication

Authentication is a process which verifies the identity of a user who wants to access the system. In the digital signature, authentication helps to authenticate the sources of messages.

Non-repudiation

Non-repudiation means assurance of something that cannot be denied. It ensures that someone to a contract or communication cannot later deny the authenticity of their signature on a document or in a file or the sending of a message that they originated.

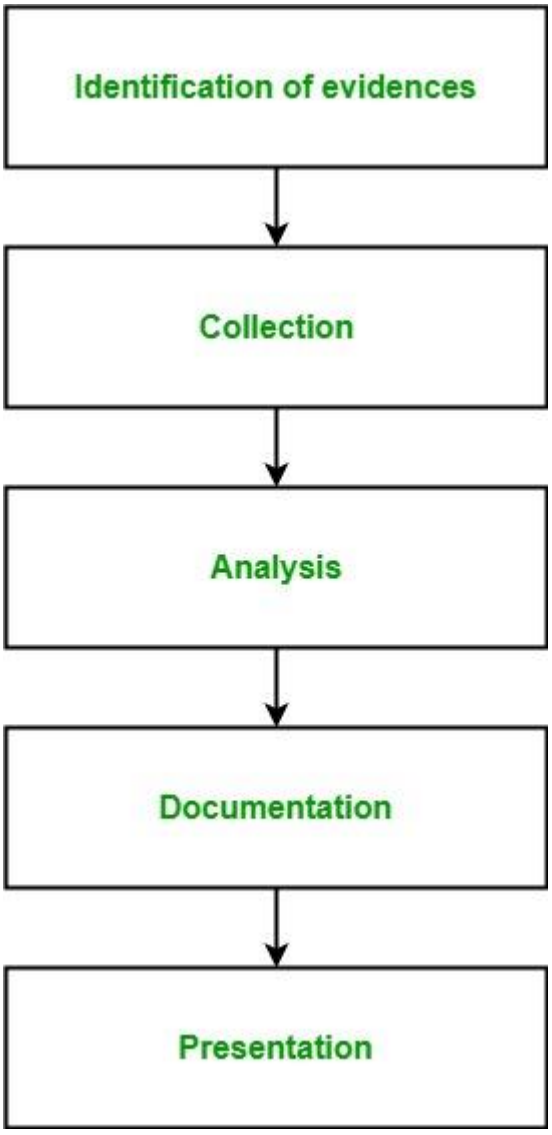
Integrity

Integrity ensures that the message is real, accurate and safeguards from unauthorized user modification during the transmission.

Q.10 draw digital forensic life cycle and explain the process.

Ans: **Digital Forensics** is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital

information in the digital devices related to the computer crimes, as a part of the investigation. In simple words, Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidences. The first computer crimes were recognized in the 1978 Florida computers act and after this, the field of digital forensics grew pretty fast in the late 1980-90's. It includes the area of analysis like storage media, hardware, operating system, network and applications. It consists of 5 steps at high



1. **Identification of evidence:** It includes of identifying evidences related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.

2. **Collection:** It includes preserving the digital evidences identified in the first step so that they doesn't degrade to vanish with time. Preserving the digital evidences is very important and crucial.

3. **Analysis:** It includes analyzing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.

4. **Documentation:** It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.

5. **Presentation:** It includes the presentation of all the digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

Branches of Digital Forensics:

- **Media forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of audio, video and image evidences during the investigation process.

- **Cyber forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a cyber crime.

- **Mobile forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime committed through a mobile device like mobile phones, GPS device, tablet, laptop.

- **Software forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime related to softwares only.