Cyber Security
IMP Questions with solution

1.What is Vulnerability? Give small example

A vulnerability in cybersecurity is a weakness in a host or system, such as a missed software update or system misconfiguration, that can be exploited by cybercriminals to compromise an IT resource and advance the attack path.

Identifying cyber vulnerabilities is one of the most important steps organizations can take to improve and strengthen their overall cybersecurity posture.

Example : Unsecured APIs

Another common security vulnerability is unsecured application programming interfaces (APIs). APIs provide a digital interface that enables applications or components of applications to communicate with each other over the internet or via a private network.

APIs are one of the few organizational assets with a public IP address. If not properly and adequately secured, they can become an easy target for attackers to breach.

As with misconfigurations, securing APIs is a process prone to human error. While rarely malicious, IT teams may simply be unaware of the unique security risk this asset possesses and rely on standard security controls. Conducting a security awareness training to educate teams on security best practices specific to the cloud — such as how to store secrets, how to rotate keys and how to practice good IT hygiene during software development — is critical in the cloud, just as in a traditional environment.

2.Write short note on Nmap and Netcat

Nmap is an open-source utility for network discovery. Network Mapper is a security auditing and network scanning independent tool developed by Gordon Lyon. It is used by network administrators to detect the devices currently running on the system and the port number by which the devices are connected.

Many systems and network administrators are used for managing network inventory, service upgrade schedules, monitoring hosts and service uptime.

Working of Nmap

Nmap is convenient during penetration testing of networked systems. Nmap provides the network details, and also helps to determine the security flaws present in the system. Nmap is platform-independent and runs on popular operating systems such as Linux, Windows and Mac.

Nmap is a useful tool for network scanning and auditing purposes.

- It can search for hosts connected to the Network.
- It can search for free ports on the target host.
- It detects all services running on the host with the help of operating system.
- It also detects any flaws or potential vulnerabilities in networked systems.

It is effortless to work with the Nmap. With the release of a new graphical user interface called GenMap User, it performs many tasks such as saving and comparing scan results, scanning the results in a database, and visualize the network system topology graphically, etc.

NETCAT

Netcat is a networking utility with the help of TCP/IP protocol which reads and writes data across network connections. Netcat is built as a secure back-end tool and can be used to send files from a client to a server and back directly with other programmes and scripts.

At the same time, it's a network debugging and exploration platform rich in features that can define network parameters while also creating a tunnel connection to a remote host.

Although Netcat can do many things, its primary objective and most desirable features are as follows −

- To build a connection from the server to the client, create an initial socket.
- If linked, a second socket will be created automatically by Netcat to transmit files from the server to the client and vice versa.

The capabilities of Netcat are as follows −

- Capability of using any local source port
- Port-scanning capabilities
- Having Slow send mode
- Outbound or inbound and TCP or UDP connections from any port or to any port
- Full DNS forward and reverse checking
- Loose source routing

3.What is OpenVas? Write advantage and disadvantage of OpenVas.

The Open Vulnerability Assessment System, known more commonly as OpenVAS, is a suite of tools that work together to run tests against client computers using a database of known exploits and weaknesses. The goal is to learn about how well your servers are guarded against known attack vectors.

Advanatages

- Open-source and Free of Cost:

The best aspect of OpenVAS is that it is open-source and free of cost, and at the same time competent to the paid assessment systems that are present in the industry.

- Useful for Small Businesses

Most small businesses prefer OpenVAS because it is a cost-free product and is notable in the testing tools industry. Also, if you are still deciding to go for vulnerability assessment tool and yet not sure about it, you can give your thoughts a chance by try using OpenVAS without risking your investment.

Disadvantages

OpenVAS covers less CVEs and test cases for testing and assessment as compared to Nessus which covers approximately double of what OpenVAS covers. In short, OpenVAS would discover less vulnerability

4.Write benefits of Metasploit

Metasploit: It is an open-source project which offers the public resources to develop codes and research security vulnerabilities. It permits the network administrators for breaking their network to recognize security threats and also document which vulnerability requires to be defined first.

Let's discuss some advantages of Metasploit.

1. Open-source

   It is actively developed and open-source is the most important reason why we prefer Metasploit. Several other paid tools exist to carry out the penetration testing process. However, Metasploit permits users for adding their custom modules and accessing its code. The Metasploit Pro version is chargeable, although, for the sake of gaining, the community edition is preferred mostly.

2. Easy naming convention and support to test large networks

   Metasploit is easy-to-use. However, here this feature defines the easy naming conventions of many commands. Metasploit facilitates ease while building a large penetration test of a network. For example, suppose we have to test any network having 200 systems. Rather than testing all the systems one-by-one, Metasploit can test the whole range automatically.

   With parameters like Classless Inter-Domain Routine (short for CIDR) and subnet values, Metasploit can test every system to exploit the susceptibility. However, in any manual exploitation method, we may need to define the exploits onto 200 systems manually. Therefore, Metasploit is saving a large amount of energy and time.

3. GUI Environment

Metasploit provides third-party instances and friendly GUI like Armitage. These types of interfaces can ease the projects of penetration testing by facilitating services like functions on a button click, vulnerability management over the fly, and easy-to-shift workspaces.

4. Cleaner exits

Metasploit is liable to make a cleaner exit through a system. It is an important aspect if we know that this service will not immediately reboot. Also, it gives a lot of functions for post-exploitation like persistence which could support to maintain access to a server permanently.

5. Explain Following terms: 1. Datapipe 2. Fpipe

Datapipe : Datapipe is a Unix-based port redirection tool written by Todd Vierling. It uses standard system and network libraries, which enable it to run on the alphabet of Unix platforms. Datapipe is not exploit code. It is not a buffer overflow or a cross-site scripting attack.

Fpipe:FPipe is a source port forwarder/Redirector. It can Create a TCP or UDP stream with a source port of your choice. This is useful for getting past firewalls that allow traffic with source ports of say 23, to Connect with internal servers

6.Describe Network Sniffers with suitable example.

Sniffing is the technique used to monitor and record all data packets continuously that go through a network. Network/system administrators employ sniffers to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets carrying sensitive passwords and account information. Sniffers are implemented as hardware or software in the system. A hostile intruder can gather and analyse all network traffic by using a packet sniffer in promiscuous mode on a network.

A packet sniffer is another term for a network sniffer. Because every packet of data is sniffed through the network to avoid network-related issues, it's called a packet sniffer. The packet sniffer tool is implemented to investigate cybercrime, hackers, and data theft. It can be employed for both ethical and unethical reasons.

Network Sniffing can be either Active or Passive.

Active Sniffing

Active Sniffing involves sniffing in the switch. A switch is a network device that provides a connection between two points. The switch controls the flow of data between its ports by continuously checking the MAC address on each port, ensuring that data is sent to the correct destination. Sniffers actively spike traffic into the LAN to monitor communication between targets and enable traffic sniffing. Active sniffing is done in a variety of ways.

Passive Sniffing

The attacker does not interact with the target in this sniffing. They connect to the network and collect packets sent and received by the network and the packets sent and received between two devices. This sniffing is done through the hub. An attacker uses their PC to connect to the hub. The attacker only needs a LAN account.

Types of Network Sniffers

Following are the different types of Network Sniffers −

- Mac sniffers − Sniffers are used to sniff data relevant to the MAC address filter.
- Protocol sniffer − It sniffs the data on the network for network protocols.
- LAN sniffer − This type of device is primarily employed in internal systems or networks, and it can inspect an entire range of IP addresses.
- IP sniffers − Sniff all data relevant to a specific IP filter. It records the data packets for analysis and diagnosis. IP sniffers capture network traffic and log the information, generally delivered in a human-readable format for analysis. They may be used by network administrators and hackers of all stripes to assess the current condition of a network, identify network vulnerabilities, and evaluate network performance.
- ARP sniffers − Rather than sending packets to the host only and passed to the network administrator, packets are sent to the ARP caches of both network hosts in this sniffing. It also allows attackers to map IP addresses to MAC addresses, carrying out packet spoofing and other vulnerabilities or poisoning attacks.
- Password sniffers − It is a technique for extracting information from network traffic to harvest passwords. Hackers used to target sessions to steal credentials and other information. Websites that don't have an

SSL protocol encryption to protect themselves are vulnerable to attack and exploitation.

Use of Network Sniffers

Hackers primarily employ network sniffers to gather information on passwords and other sensitive information. The sniffer decodes data in packets travelling from source to destination, between client and server, or between organisations. They functioned as middlemen and employed a packet injection attack to grab the data. For example, a network sniffer can track down someone using too much bandwidth at a university or company by monitoring network traffic. They are also used to detect security vulnerabilities in our system.

Today, however, black hat hacking is a widespread application for them. In the wrong hands, network sniffing tools can allow anyone with little to no hacking expertise to monitor network traffic across unsecured WiFi networks to steal passwords and other sensitive data. This reason can give network sniffing tools a bad name, yet network sniffers have many valid purposes.

How Does Sniffing Work?

With the software's assistance for sniffing data packets, the Network sniffing tool intercepts and logs the network traffic. This software allows you to access information from a whole network or just a segment of one.

As we all know, networks are used to send packets of data. The data can be large, and transmitting it all in one packet places a load on the network, compromising the data's integrity. As a result, once a data file is sent, it is usually broken down into small parts and sent to the intended location.

The destination address, number of packets, reassembly order, and source address are all included in the data packet. The data packet's footers and headers were erased after it arrived at its destination. A filter on the network can delete packets that are not addressed to the same network.

Following the receipt of network data, the following steps are taken −

- Individual packets (sections of network data) or their contents are recorded.
- Software only saves the header segment of data packets to save space.
- The user can access and evaluate the information when the network data has been decoded and formatted.
- Packet sniffers examine network communication failures, troubleshoot network connections, and reconstruct whole datastreams meant for other computers.
- Some network sniffing applications retrieve passwords, PINs, and other confidential information.

7.Types of cyber crimes

The following are considered to be types of cyber-crimes:

Child pornography or child sexually abusive material (CSAM):

In its simplest sense, child sexual abuse materials (CSAMs) include any material containing sexual images in any form, wherein both the child being exploited or abused may be seen. There is a provision in Section 67(B) of the Information

Technology Act which states that the publication or transmission of material depicting children in sexually explicit acts in an electronic form is punishable.

Cyberbullying:

A cyberbully is someone who harasses or bullies others using electronic devices like computers, mobile phones, laptops, etc. Cyberbullying refers to bullying conducted through the use of digital technology. The use of social media, messaging platforms, gaming platforms, and mobile devices may be involved. Oftentimes, this involves repeated behaviour that is intended to scare, anger, or shame those being targeted.

Cyberstalking:

Cyberstalking is the act of harassing or stalking another person online using the internet and other technologies. Cyberstalking is done through texts, emails, social media posts, and other forms and is often persistent, methodical, and deliberate.

Cyber grooming:

The phenomenon of cyber grooming involves a person building a relationship with a teenager and having a strategy of luring, teasing, or even putting pressure on them to perform a sexual act.

Online job fraud:

An online job fraud scheme involves misleading people who require a job by promising them a better job with higher wages while giving them false hope. On March 21, 2022, the Reserve Bank of India (RBI) alerted people not to fall prey to job scams. By this, the RBI has explained the way in which online job fraud is perpetrated, as well as precautions the common man should take when applying for any job opportunity, whether in India or abroad.

Online sextortion:

The act of online sextortion occurs when the cybercriminal threatens any individual to publish sensitive and private material on an electronic medium. These criminals threaten in order to get a sexual image, sexual favour, or money from such individuals.

Phishing:

Fraud involving phishing is when an email appears to be from a legitimate source but contains a malicious attachment that is designed to steal personal information from the user such as their ID, IPIN, Card number, expiration date, CVV, etc. and then selling the information on the dark web.

Vishing:

In vishing, victims' confidential information is stolen by using their phones. Cybercriminals use sophisticated social engineering tactics to get victims to divulge private information and access personal accounts. In the same way as phishing and smishing, vishing convincingly fools victims into thinking that they are being polite by responding to the call. Callers can often pretend that they are from the government, tax department, police department, or victim's bank..

Smishing:

As the name suggests, smishing is a fraud that uses text messages via mobile phones to trick its victims into calling a fake phone number, visiting a fraudulent website or downloading malicious software that resides on the victim's computer.

Credit card fraud or debit card fraud:

In credit card (or debit card) fraud, unauthorized purchases or withdrawals from another's card are made to gain access to their funds. When unauthorized purchases or withdrawals of cash are made from a customer's account, they are considered credit/debit card fraud. Fraudulent activity occurs when a criminal gains access to the cardholder's debit/credit number, or personal identification number (PIN). Your information can be obtained by unscrupulous employees or hackers.

Impersonation and identity theft:

A person is impersonated or exposed to identity theft when they make fraudulent use of an electronic signature, a password, or any other unique identifier on another person's behalf.

Prevention of cyber crimes

As per the recommendations of the International Maritime Organization (IMO), the cyber-attack risk must be approached using the following framework:

- The first step is to define the roles and responsibilities of the personnel responsible for cyber risk management.
- The second step is to identify the systems, assets, data, or capabilities that will put the operation at stake if disrupted.

- To protect against a potential cyber event and to maintain continuity of operations, it is important to implement risk-control processes and contingency plans.
- It is also important to develop and implement measures to detect a cyber-attack as quickly as possible.
- Preparation and implementation of plans to restore critical systems for continued operations by providing resilience.
- Finally, identify and implement measures to be taken to backup and restore any affected systems.

The following can be the strategies can be used to prevent cyber crime:

Analyze your risk exposure:

In order to adequately prepare for a cyber attack, you must assess the threat and give due consideration. Companies should consider the following:

- They should consider all areas where they are susceptible to cyberattacks and any operational vulnerabilities resulting from them.
- A vulnerability assessment of all systems is necessary to identify those that are critical to the business, to understand the potential exposures each has, and to assess the impact of any cyber-attack on business continuity.
- IT systems and operational technology systems should be checked by businesses.

Preventive measures:

It is recommended that businesses adopt national or international technical standards that provide a high level of protection. These general prevention measures are recommended for companies that currently lack the necessary technical or financial capabilities. The following is the list of preventive measures:

- Applying multiple layers of defence, beginning with physical security, followed by management policies and procedures, firewalls and network architecture, computer policies, account management, security updates and finally antivirus applications.
- Implementing a principle of least privilege, which restricts information and access to only those set of people who needs to know that particular information.
- Implementing network-hardening measures, assuring patch management is sufficient and is proactively reviewed.
- Securing critical systems by utilizing technology such as protocol-aware filtering and segregation.
- Ensuring that removable devices are encrypted and that any USB used with any other device is tested for viruses.
- Furthermore, in order to prevent the negative impact of a cyberattack from further escalating and restoring business operations, it is important to develop business continuity plans, identify key personnel, and implement processes.
- Additionally, organising frequent training and awareness sessions for all employees can also help.
- Compliance audits of third-party service providers will also be beneficial.

List Brute Force Tools with brief explanation and describe how to
Prevent Brute Force Password Hacking?
What is the need of cyber law in India?/Illustrate the aim and objective of Indian IT ACT 2000.

9.Cyber crime laws in India

In terms of cybersecurity, there are five main types of laws that must be followed. Cyber laws are becoming increasingly important in countries such as India which have extremely extensive internet use. There are strict laws that govern the use of cyberspace and supervise the use of information, software, electronic commerce, and financial transactions in the digital environment. India's cyber laws have helped to enable electronic commerce and electronic governance to flourish in India by safeguarding maximum connectivity and minimizing security concerns. This has also made digital media accessible in a wider range of applications and enhanced its scope and effectiveness.

Information Technology Act, 2000 (IT Act):

Overview of the Act:

It is the first cyberlaw to be approved by the Indian Parliament. The Act defines the following as its object:

"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 methods of communication and storage of information, to facilitate

electronic filing of documents with the Government agencies and further 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 and for matters connected therewith or incidental thereto."

However, as cyber-attacks become dangerous, along with the tendency of humans to misunderstand technology, several amendments are being made to the legislation. It highlights the grievous penalties and sanctions that have been enacted by the Parliament of India as a means to protect the e-governance, e-banking, and e-commerce sectors. It is important to note that the IT Act's scope has now been broadened to include all the latest communication devices.

The Act states that an acceptance of a contract may be expressed electronically unless otherwise agreed and that the same shall have legal validity and be enforceable. In addition, the Act is intended to achieve its objectives of promoting and developing an environment conducive to the implementation of electronic commerce.

The important provisions of the Act

The IT Act is prominent in the entire Indian legal framework, as it directs the whole investigation process for governing cyber crimes. Following are the appropriate sections:

- Section 43: This section of the IT Act applies to individuals who indulge in cyber crimes such as damaging the computers of the victim, without taking the due permission of the victim. In such a situation, if a computer is damaged without the owner's consent, the owner is fully entitled to a refund for the complete damage.

In *Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others (2018)*, Rajesh Aggarwal of Maharashtra's IT department (representative in the present case) ordered Punjab National Bank to pay Rs 45 lakh to Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. In this case, a fraudster transferred Rs 80.10 lakh from Matharu's account at PNB, Pune after the latter answered a phishing email. Since the complainant responded to the phishing mail, the complainant was asked to share the liability. However, the bank was found negligent because there were no security checks conducted against fraudulent accounts opened to defraud the Complainant.

- Section 66: Applies to any conduct described in Section 43 that is dishonest or fraudulent. There can be up to three years of imprisonment in such instances, or a fine of up to Rs. 5 lakh.

In *Kumar v. Whiteley (1991)*, during the course of the investigation, the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added, and changed files. As a result of investigations, Kumar had been logging on to a BSNL broadband Internet connection as if he was an authorized legitimate user and modifying computer databases pertaining to broadband Internet user accounts of subscribers. On the basis of an anonymous complaint, the CBI registered a cyber crime case against Kumar and conducted investigations after finding unauthorized use of broadband Internet on Kumar's computer. Kumar's wrongful act also caused the subscribers to incur a loss of Rs 38,248. N G Arun Kumar was sentenced by the Additional Chief Metropolitan Magistrate. The magistrate ordered him to undergo a rigorous year of imprisonment with a fine of Rs 5,000 under Sections 420 of IPC and 66 of the IT Act.

- Section 66B: This section describes the penalties for fraudulently receiving stolen communication devices or computers, and confirms a possible three-year prison sentence. Depending on the severity, a fine of up to Rs. 1 lakh may also be imposed.
- Section 66C: The focus of this section is digital signatures, password hacking, and other forms of identity theft. Thi section imposes imprisonment upto 3 years along with one lakh rupees as a fine.
- Section 66D: This section involves cheating by personation using computer Resources. Punishment if found guilty can be imprisonment of up to three years and/or up-to Rs 1 lakh fine.
- Section 66E: Taking pictures of private areas, publishing or transmitting them without a person’s consent is punishable under this section. Penalties, if found guilty, can be imprisonment of up to three years and/or up-to Rs 2 lakh fine.
- Section 66F: Acts of cyber terrorism. An individual convicted of a crime can face imprisonment of up to life. An example: When a threat email was sent to the Bombay Stock Exchange and the National Stock Exchange, which challenged the security forces to prevent a terror attack planned on these institutions. The criminal was apprehended and charged under Section 66F of the IT Act.
- Section 67: This involves electronically publishing obscenities. If convicted, the prison term is up to five years and the fine is up to Rs 10 lakh.

Positive and negative aspects of the IT Act

This legislation contains the following benefits:

- Several companies are now able to conduct e-commerce without any fear because of the presence of this Act. Until recently, the development of electronic commerce in our country was hindered primarily due to a lack of legal infrastructure to govern commercial transactions online.
- Digital signatures are now able to be used by corporations to conduct online transactions. Digital signatures are officially recognized and sanctioned by the Act.
- Additionally, the Act also paves the way for corporate entities to also act as Certification Authorities for the issuance of Digital Signature Certificates under the Act. There are no distinctions in the Act as to what legal entity may be designated as a Certifying Authority, provided the government's standards are followed.
- Furthermore, the Act permits the companies to electronically file any of their documents with any office, authority, body or agency owned or controlled by the appropriate government by using the electronic form prescribed by that government.
- It also provides information on the security concerns that are so crucial to the success of the use of electronic transactions. As part of the Act, the term secure digital signatures were defined and approved, which are required to have been submitted to a system of a security procedure. Therefore, it can be assumed that digital signatures are now secured and will play a huge part in the economy. Digital signatures can help conduct a secure online trade.

It is common for companies to have their systems and information hacked. However, the IT Act changed the landscape completely. A statutory remedy is now being provided to corporate entities in the event that anyone breaches their computer systems or network and damages or copies data. Damages are charged to anyone who uses a computer, computer system or computer network without the permission of the owner or other person in charge.

However, the said Act has a few problems:

- Section 66A is considered to be in accordance with Article 19(2) of the Constitution of India since it does not define the terms ‘offensive’ and ‘menacing’. It did not specify whether or not these terms involved defamation, public order, incitement or morality. As such, these terms are open to interpretation.
- Considering how vulnerable the internet is, the Act has not addressed issues such as privacy and content regulation, which are essential.
- A domain name is not included in the scope of the Act. The law does not include any definition of domain names, nor does it state what the rights and liabilities of domain name owners are.
- The Act doesn’t make any provision for the intellectual property rights of domain name proprietors. In the said law, important issues pertaining to copyright, trademark, and patent have not been addressed, therefore creating many loopholes.

Indian Penal Code, 1860 (IPC):

If the IT Act is not sufficient to cover specific cyber crimes, law enforcement agencies can apply the following IPC sections:

- Section 292: The purpose of this section was to address the sale of obscene materials, however, in this digital age, it has evolved to deal with various cyber crimes as well. A manner in which obscene material or sexually explicit acts or exploits of children are published or transmitted electronically is also governed by this provision. The penalty for such acts is imprisonment and fines up to 2 years and Rs. 2000, respectively. The punishment for any of the above crimes may be up to five years of imprisonment and a fine of up to Rs. 5000 for repeat (second-time) offenders.
- Section 354C: In this provision, cyber crime is defined as taking or publishing pictures of private parts or actions of a woman without her consent. In this section, voyeurism is discussed exclusively since it includes watching a woman's sexual actions as a crime. In the absence of the essential elements of this section, Section 292 of the IPC and Section 66E of the IT Act are broad enough to include offences of an equivalent nature. Depending on the offence, first-time offenders can face up to 3 years in prison, and second-time offenders can serve up to 7 years in prison.
- Section 354D: Stalking, including physical and cyberstalking, is described and punished in this chapter. The tracking of a woman through electronic means, the internet, or email or the attempt to contact her despite her disinterest amounts to cyber-stalking. This offence is punished by imprisonment of up to 3 years for the first offence and up to 5 years for the second offence, along with a fine in both cases.

A victim in the case *Kalandi Charan Lenka v. the State of Odisha(2017)* has received a series of obscene messages from an unknown number that has damaged her reputation. The accused also sent emails to the victim and created a fake account on Facebook containing morphed images of her. The High Court, therefore, found the accused prima facie guilty of cyberstalking on various charges under the IT Act and Section 354D of IPC.

- Section 379: The punishment involved under this section, for theft, can be up to three years in addition to the fine. The IPC Section comes into play in part because many cyber crimes involve hijacked electronic devices, stolen data, or stolen computers.
- Section 420: This section talks about cheating and dishonestly inducing delivery of property. Seven-year imprisonment in addition to a fine is imposed under this section on cybercriminals doing crimes like creating fake websites and cyber frauds. In this section of the IPC, crimes related to password theft for fraud or the creation of fraudulent websites are involved.
- Section 463: This section involves falsifying documents or records electronically. Spoofing emails is punishable by up to 7 years in prison and/or a fine under this section.
- Section 465: This provision typically deals with the punishment for forgery. Under this section, offences such as the spoofing of email and the preparation of false documents in cyberspace are dealt with and punished with imprisonment ranging up to two years, or both. In *Anil Kumar Srivastava v. Addl Director, MHFW (2005)*, the petitioner had forged signed the signature of the AD and had then filed a case that made false allegations against the same individual. Due to the fact that the petitioner

also attempted to pass it off as a genuine document, the Court held that the petitioner was liable under Sections 465 and 471 of the IPC.

- Section 468: Fraud committed with the intention of cheating may result in a seven-year prison sentence and a fine. This section also punishes email spoofing.

Furthermore, there are many more sections of the IT Act and the Indian Penal Code, which pertain to cyber crimes, in addition to the laws listed above.

Even though there are laws against cyber crime in place, the rate of cyber crime is still rising drastically. It has been reported that cyber crime in India increased by 11.8% in the year 2020, which accounted for reporting around only 50,000 cases. Cyber crime is one of the toughest crimes for the Police to solve due to many challenges they face including underreporting, the jurisdiction of crime, public unawareness and the increasing costs of investigation due to technology.

Certain offences may end up being bailable under the IPC but not under the IT Act and vice versa or maybe compoundable under the IPC but not under the IT Act and vice versa due to the overlap between the provisions of the IPC and the IT Act. For example, if the conduct involves hacking or data theft, offences under sections 43 and 66 of the IT Act are bailable and compoundable, whereas offences under Section 378 of the IPC are not bailable and offences under Section 425 of the IPC are not compoundable. Additionally, if the offence was the receipt of stolen property, the offence under section 66B of the IT Act was bailable while the offence under Section 411 of the IPC was not. In the same manner, in respect of the offence of identity theft and cheating by personation, the offences are compoundable and bailable under sections 66C and 66D of the IT Act, whereas the offences under Sections 463, 465, and 468 of the IPC are not compoundable and the offences under sections 468 and 420 of the IPC are not bailable.

In *Gagan Harsh Sharma v. The State of Maharashtra (2018),* the Bombay High Court addressed the issue of non-bailable and non-compoundable offences under sections 408 and 420 of the IPC in conflict with those under Sections 43, 65, and 66 of the IT Act that is bailable and compoundable.

Information Technology Rules (IT Rules):

There are several aspects of the collection, transmission, and processing of data that are covered by the IT Rules, including the following:

- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: According to these rules, entities holding individuals' sensitive personal information must maintain certain security standards that are specified.
- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021: To maintain the safety online of users' data, these rules govern the role of intermediaries, including social media intermediaries, to prevent the transmission of harmful content on the internet.
- The Information Technology (Guidelines for Cyber Cafe) Rules, 2011: According to these guidelines, cybercafés must register with an appropriate agency and maintain a record of users' identities and their internet usage.

- The Information Technology (Electronic Service Delivery) Rules, 2011: Basically, these regulations give the government the authority to specify the delivery of certain services, such as applications, certificates, and licenses, by electronic means.
- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the CERT-In Rules): There are several ways in which the CERT-In rules provide for the working of CERT-In. In accordance with rule 12 of the CERT-In rules, a 24-hour Incident response helpdesk must be operational at all times. Individuals, organisations and companies can report cybersecurity incidents to Cert-In if they are experiencing a cybersecurity Incident. The Rules provide an Annexure listing certain Incidents that must be reported to Cert-In immediately.

Another requirement under Rule 12 is that service providers, intermediaries, data centres, and corporate bodies inform CERT-In within a reasonable timeframe of cybersecurity incidents. As a result of the Cert-In website, Cybersecurity Incidents can be reported in various formats and methods, as well as information on vulnerability reporting, and incident response procedures. In addition to reporting cybersecurity incidents to CERT-In in accordance with its rules, Rule 3(1)(I) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 also requires that all intermediaries shall disclose information about cybersecurity incidents to CERT-In.

Companies Act, 2013:

A majority of the corporate stakeholders consider the Companies Act of 2013 to be the most pertinent legal obligation to properly manage daily operations. This Act enshrines in law all the techno-legal requirements that need to be met, implementing the law as a challenge to the companies that are not compliant. As part of the Companies Act 2013, the SFIO (Serious Fraud Investigation Office) is entrusted with powers to investigate and prosecute serious frauds committed by Indian companies and their directors.

As a result of the Companies Inspection, Investment, and Inquiry Rules, 2014 notification, the SFIOs have become even more proactive and serious in regard to this. By ensuring proper coverage of all the regulatory compliances, the legislature ensured that every aspect of cyber forensics, e-discovery, and cybersecurity diligence is adequately covered. Moreover, the Companies (Management and Administration) Rules, 2014 prescribe a strict set of guidelines that confirm the cybersecurity obligations and responsibilities of corporate directors and senior management.

Cybersecurity Framework (NCFS):

As the most credible global certification body, the National Institute of Standards and Technology (NIST) has approved the Cybersecurity Framework (NCFS) as a framework for harmonizing the cybersecurity approach. To manage cyber-related risks responsibly, the NIST Cybersecurity Framework includes guidelines, standards, and best practices. According to this framework, flexibility and affordability are of prime importance. Moreover, it aims at fostering resilience and protecting critical infrastructure by implementing the following measures:

- A better understanding, management, and reduction of the risks associated with cybersecurity.
- Prevent data loss, misuse, and restoration costs.
- Determine the most critical activities and operations that must be secured.
- Provides evidence of the trustworthiness of organizations that protect critical assets.
- Optimize the cybersecurity return on investment (ROI) by prioritizing investments.
- Responds to regulatory and contractual requirements
- Assists in the wider information security program.

Using the NIST CSF framework in conjunction with ISO/IEC 27001 simplifies the process of managing cybersecurity risk. Moreover, NIST's cybersecurity directive also allows for easier collaboration in the organization as well as across the supply chain, allowing for more effective communication.

10.Describe DOS and DDOS attack with suitable example.

Denial-of-service attacks

A denial-of-service attack, or DoS attack, is any attack that aims to prevent access to a service for legitimate users. That service might be a website, an email account, a network, or a device. The attack can target any potential users of the service, or one user in particular. For example, a DoS attack could target one person's device to prevent them from accessing the internet, or it could target a website to deny access to all of its visitors.

Attackers can use DoS attacks to make companies lose business, or hold companies to ransom by threatening attack. They might also use DoS attacks to distract their victim from other types of attacks, for example, as a cover to break into a server and steal sensitive data. Sometimes this form of attack has political motivations, for example, the hacker collective Anonymous uses DoS and DDoS attacks to take down government and corporate websites that they disagree with.

There are lots of different ways of conducting a DoS attack, but broadly, they fall into two types:

- Sending illegitimate data (teardrop attack)
- Flooding the victim with data (flooding attack)

In a teardrop attack, the attacker sends data to the victim that the victim doesn't know how to process. It spends so long or so many resources trying to interpret the data that the service slows down or stops. For example, the attacker might send large data packets, broken down into fragments to be reassembled by the victim. The attacker might change how the packet is broken down so that the victim doesn't know how to reassemble it.

In a flooding attack, the attacker floods the victim with so many messages that it overwhelms them. The service slows down or stops for legitimate users, because it cannot handle so many simultaneous demands.

DoS attacks are difficult to defend against. One technique to defend against flooding is to rate limit users, which means only allowing individuals to send a certain number of requests per minute. However, the distributed denial-of-service attack helps attackers to get round this defence.

Distributed denial-of-service attacks

In a distributed denial-of-service (or DDoS) attack, the attacker carries out a DoS attack using several computers. These computers are often infected bots, which we discussed in the previous step.

Controlling lots of computers at the same time allows an attacker to send a greater number of messages, which increases the chances of their DoS attack being effective. Also, the bots that the attacker controls could be located anywhere in the world and would all have separate IP addresses. This means that protections like rate limiting won’t stop the attack.

In a standard DoS attack, if the victim can identify the attacker, they might be able to block their messages. However, when the attacker is made up of lots of different computers, the victim might not be able to tell the difference between the bots and the legitimate users. Sometimes websites just receive a high quantity of traffic because lots of people want to use their service, and it can be extremely difficult to tell when this is happening and when a DDoS attack is taking place. In addition, even if the victim is able to identify a few bots, they can’t stop the attack unless they can identify all of them.

11.What is Virus and Warms?/Explain Virus and Worms, Trojan Horses and Backdoors.

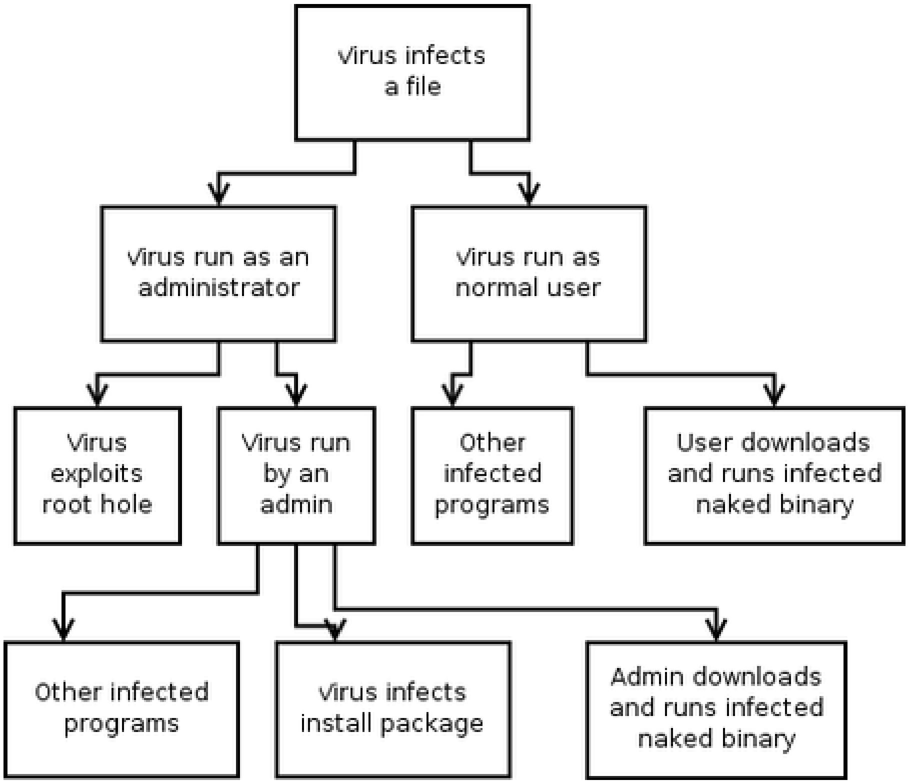
Malicious Software

Malicious Software is also commonly referred to as Malware. According to Bruce Schneier, "Malicious Software includes computer viruses, worms, and trojan horses". Other experts include spyware, dishonest adware, crimeware, rootkits, and other unwanted software. Bots and botnets will also be presented as they have also become a more common threat to computer security.

What is it? Malicious Software or malware is software designed to infiltrate a computer system without the owner's informed consent.

What does it do? Depending on the variety of malware, "it can hijack your browser, redirect your search attempts, serve up nasty pop-up ads, track what web sites you visit, and generally screw things up". The bottom line is malware can cost you or your organization time, money, resources, privacy, and security.

Computer Viruses


Virus infects a file
Virus run as an administrator
Virus run as normal user
Virus exploits root hole
Virus run by an admin
Other infected programs
User downloads and runs infected naked binary
Other infected programs
Virus infects install package
Admin downloads and runs infected naked binary

What is it? A Computer virus "is a program that can infect other programs by modeling them to include a possibly evolved copy of itself. It can spread throughout a computer system or network. Every program that gets infected may also act as a virus and thus the infection grows".

What does it do? "A properly engineered virus can have a devastating effect, disrupting productivity and doing billions of dollars in damages". Viruses can cause any number of symptoms ranging from slowing down the computer to ultimately crashing it.

Viruses have been around since virtually computers have been in existence, dating back to 1949. The term virus dates back to 1984 and is credited to Kenneth Thompson. The term computer virus is often used synonymously for all forms of malware, although each form of malware discussed on this page has a different function.

Worms

What is it? Computer worms are independent programs that copy themselves and reproduce at a rapid pace, usually over a computer network. "The programs on individual computers are described as the segments of worms. The segments in a worm remain in communication with each other, should one segment fail, the remaining pieces must find another free computer, initialize it, and add it to the worm. As segments(computers) join and then leave the program, the worm itself seems to move through the network".

What does it do? It is similar to a computer virus because it magnifies the damage it does by spreading rapidly, and can include malicious instructions that cause damage or annoyance. "Unlike a virus, which attaches itself to a host program, a worm keeps its independence and usually doesn't modify other programs". Worms can infect your email, delete computer files, lock you out of your computer, and even steal your information.

Trojan Horses

What is it? A Trojan horse (computing) is a code fragment that hides inside a program and performs a disguised function. It takes its name from the classical mythology tale of the hollow wooden horse made by Odysseus wherein soldiers hid and then launched their attack during the Trojan War.

What does it do? A Trojan horse hides inside a independent program that performs a useful task. Along with that function, it performs some other unauthorized operation. "Once a Trojan horse is activated, it can access files, folders, or your entire system. Commonly, Trojans create a "backdoor", which can be used to send your personal information to another location". Some Trojans may open up the possibility of someone accessing your machine, while others may monitor your Internet connection and grab your email addresses and access passwords. One common and annoying function is the annoying unwanted pop-up messages that seemingly arise from nowhere.

Spyware

What is it? Spyware refers to programs that use your Internet connection to send information from your personal computer to some other computer, normally without your knowledge or permission.

What does it do? On the Internet (where it is sometimes called a spybot or tracking software), "spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Different strains of spyware perform different functions. Some might also hijack your browser to take you to an unexpected site, cause your computer to dial expensive 900 numbers, replace the Home page setting in your browser with another site, or serve you personal ads, even when you're offline."

Adware

What is it? Adware is short for Advertising Supported software. The legal type of adware is a way for shareware authors to make money from a product, other than by selling it to the users. But since this page is about Malicious Software, dishonest adware is what is explained more fully. Dishonest adware is an aggressive form of unwanted software that evolved from legal adware. Adware then began exhibiting spyware and malware characteristics. Dishonest adware writers began to design their programs so that they would reinstall automatically if removed, sometimes using different file names. As Adware has matured it has become smarter. Historically, as fast as the clean-up experts have worked out how to fight malware, those behind it have fought back with new tricks.

What does it do? It generates advertisements such as pop-up windows or hotlinks on Web pages that are not part of a page's code. "Adware may add links to your favorites and your desktop. It can hijack your home page and search engine, create tool bars that appear out of nowhere, and generate unwanted pop-up windows".

Crimeware

What is it? Crimeware is any software tool used in cybercrime. Crimeware is software that is:

- used in the commission of the criminal act
- not generally regarded as a desirable software or hardware application
- not involuntarily enabling the crime

Like cybercrime itself, the term crimeware covers a wide range of different malicious, or potentially malicious software.

What does it do? Because the definition above states just about any software could be used in a manner that would deem is crimeware, examples of how a software program can be used as crimeware follows. For example, child predators often use various IM clients to converse with their intended victims. Another example would be FTP sites are sometimes set up to facilitate the distribution of pirated software.

Rootkits

What is it? Rootkits are mechanisms and techniques whereby malware, including viruses, spyware, and trojans, attempt to hide their presence from spyware blockers, antivirus, and system management utilities. A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network.

What does it do? Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

Bots & Botnets

What are bots and botnets? A bot is a type of malware which allows an attacker to gain complete control over the affected computer. Computers that are infected with a 'bot' are generally referred to as 'zombies'. There are literally tens of thousands of computers on the Internet which are infected with some type of 'bot' and whose users don't even realize it. A botnet is the network of computers that have been infected by a particular bot software. The term "botnet" is short for "robot network".

What does a botnet do? Computers that have been caught up in a botnet have been effectively taken over, and can be used to perform almost any task by the person or persons who control the botnet. Botnets are controlled by criminals whose motives include selling products, operating financial scams and crippling websites through coordinated attacks.

An interesting fact is that while it is possible for Mac or Linux systems to become victim to botnets, the vast majority of botnets are Windows PC based.

12.Why Keyloggers are a threat? How cyber criminals use Keyloggers?

Keyloggers can be incredibly accurate, which makes them especially dangerous. Many keyloggers go undetected for long periods of time, recording activity on the keyboard and giving the cybercriminal a more intimate look into the victim’s online accounts.

Keyloggers are so dangerous because they’re difficult to detect and very effective at what they do. If you’re reusing passwords, a keylogger will quickly pick up on that, exposing the login credentials to multiple accounts.

A simple keylogger can store information from a single login or multiple sites and accounts, depending on the software. The bottom line? Keyloggers are dangerous, effective, and often hard to detect—which makes them a serious threat to businesses, individuals, and governments.

How do keyloggers work?

So, how does a keylogger work, anyway? Keyloggers require an entry point to the device where it will record keystrokes. There are plenty of ways to get the keylogger onto a device whether via hardware or software. Hardware almost always requires a person to install, so it’s more likely that the keylogger was brought in by an insider.

Most keyloggers, however, are delivered via software. Software downloaded from the web or untrusted sources makes for an easy entry point for all kinds of malware. Many keyloggers have rootkit capabilities, which means they’re far more difficult to detect and remove