Assignment -3

1. *Describe the key differences between intrusion detection systems (IDS) and intrusion prevention systems (IPS).*

An intrusion detection system is a monitoring solution that spots suspicious network incidents and sends out alerts to incident responders or security operations center (SOC) analysts. These alerts enable security personnel to investigate the detected issues and execute the appropriate countermeasures to address them before significant damage occurs.

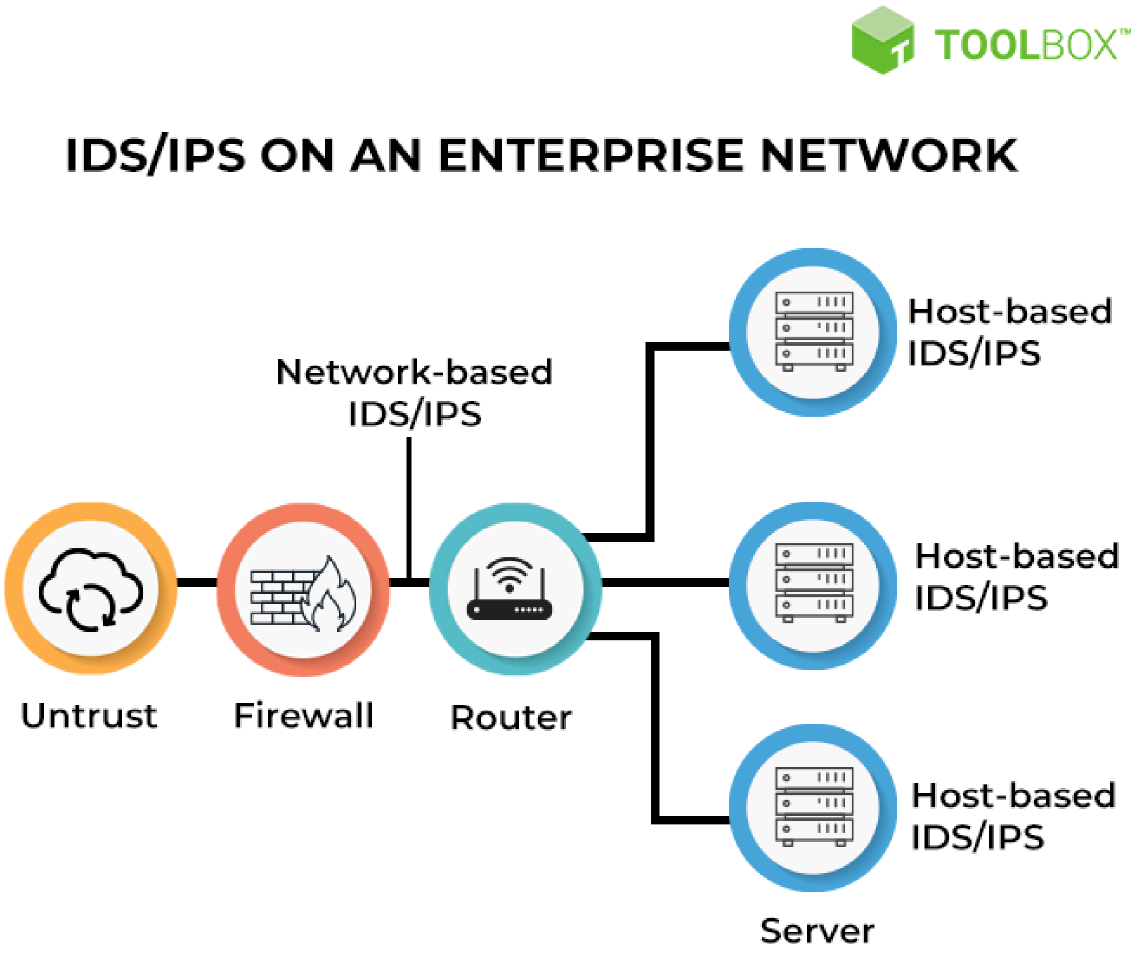
Two main network deployment locations exist for IDS—host-based IDS (HIDS) and network-based IDS (NIDS). HIDS is deployed at the endpoint level and protects individual endpoints from threats, while NIDS solutions monitor and protect entire enterprise networks.

Apart from its deployment location, IDS also differs in terms of the methodology used for identifying potential intrusions. Signature-based IDS leverages fingerprinting to identify known threats, such as malware. Once malicious traffic is identified, its signature is captured and added to the database. Each signature in this database is compared against network traffic in real time to detect new threats. This type of IDS is capable of detecting known threats rapidly and accurately.

False positives are extremely rare as alerts are only sent out once a known threat is detected. However, signature-based IDS solutions cannot detect unknown threats and would be helpless in the face of zero-day vulnerabilities.

On the other hand, anomaly-based IDS operates by creating a ‘normal’ network behavior model. All future network activity is compared against this behavior model, and network anomalies are highlighted as potential threats, with alerts being sent out to security personnel. This type of IDS is capable of detecting zero-day threats. However, both false positives and false negatives are possible here.

Finally, hybrid IDS uses signature-based and anomaly-based threat detection to detect cyberattacks with precision and speed.



What Is an Intrusion Prevention System (IPS)?

Intrusion prevention systems (IPS) perform intrusion detection and then go one step ahead and stop any detected threats.

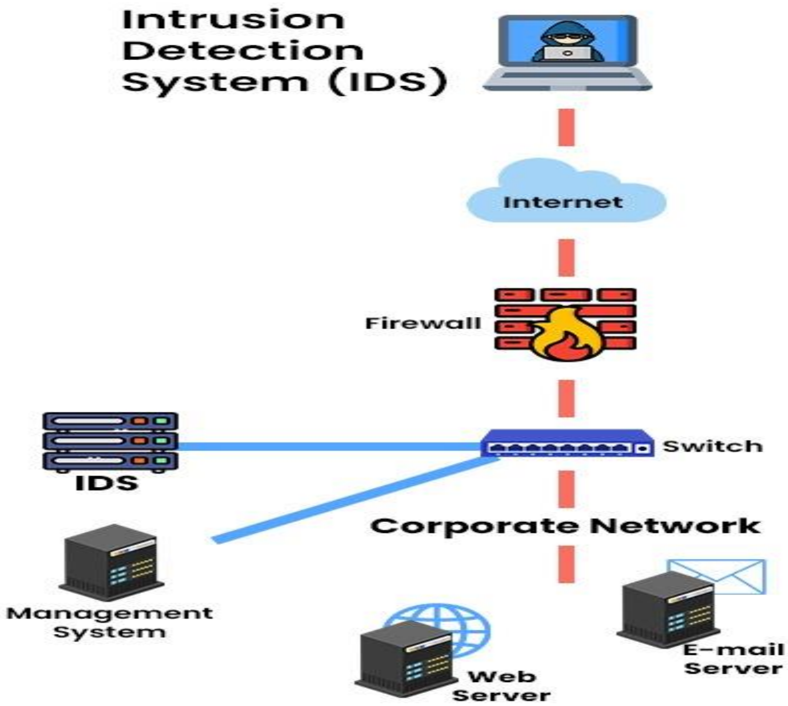
An intrusion prevention system is a network security hardware or software

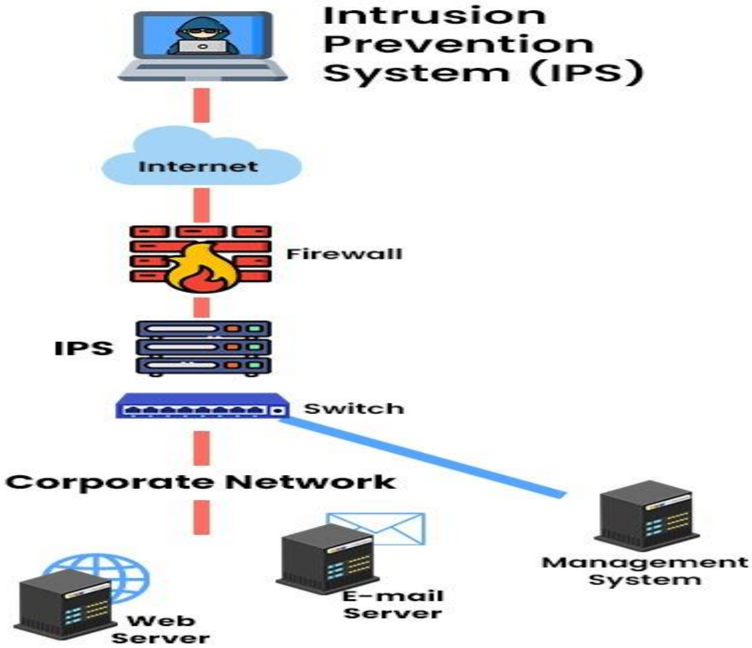
that continuously observes network behavior for threats, just like an intrusion detection system. However, IPS goes one step ahead of IDS and automatically takes the appropriate action to thwart the detected threats, including measures such as reporting, blocking traffic from a particular source, dropping packets, or resetting the connection. Some IPS solutions can also be configured to use a ‘honeypot’ (a decoy that contains dummy data) to misdirect attackers and divert them from their original targets that contain accurate data.

IPS is a critical component of modern-day enterprise security. This is because the organizational networks of 2022 have numerous access points and process high data volumes, thus making manually monitoring traffic and responding to threats an imposing task. Additionally, the increased popularity of cloud platforms means enterprises are operating in highly connected environments. While this has various benefits, it presents a vast attack surface and increases vulnerability if the cloud platform is not adequately secured.

As the threats faced by enterprise systems grow in number and become more sophisticated, automated security solutions such as IPS have become more vital than ever before. This network security solution allows businesses to counter threats in near real-time without stretching security teams’ capabilities. It does so by scanning high volumes of traffic without hampering network performance. Many security providers club IPS with unified threat management (UTM) or next-generation firewall (NGFW) solutions.

IPS solutions are placed within flowing network traffic, between the point of origin and the destination. IPS might use any one of the multiple available techniques to identify threats. For instance, signature-based IPS compares network activity against the signatures of previously detected threats. While this method can easily deflect previously spotted attacks, it’s often unable to recognize newly emerged threats.


Intrusion Detection System (IDS)
Internet
Firewall
Switch
IDS
Corporate Network
Management System
Web Server
E-mail Server


Intrusion Prevention System (IPS)
Internet
Firewall
IPS
Switch
Corporate Network
Management System
E-mail Server
Web Server

Difference between IDS and IPS

The basic difference between IDS and IPS .

Factors	**Intrusion Detection System (IDS)**	**Intrusion Prevention System (IPS)**
Function	IDS only alerts the network administrator when it detects an intrusion.	IPS actively blocks or drops the malicious packets before they reach the target.
Placement	IDS is usually placed outside the network perimeter, such as behind a firewall or a router.	IPS is usually placed inside the network perimeter, such as between a firewall and a switch.
System Type	Passive as it only monitors and then notifies the administrator.	Active as it monitor as well automatically defends the network.
Anomaly Response	Sends a notification to the user or log	Drops or modifies malicious packets
Performance	Low impact on the network speed as it only detects the intrusion.	High impact on network speed as it has to analyze and modify or block traffic in real time.

2. Design a hypothetical network architecture for a medium-sized enterprise and outline how you would integrate both intrusion detection and prevention mechanisms. Consider factors such as placement of sensors, types of detection techniques (e.g., signature-based, anomaly-based),and strategies for blocking or mitigating identified threats

Detection Method of IDS

1. Signature-based intrusion detection

Signature-based intrusion detection aims to identify potential threats by comparing network traffic and log data with existing attack patterns. These patterns are called sequences (hence the name) and may contain sequences of bytes called malicious instruction sequences. Signature-based detection allows you to identify and identify known attacks.

2. Anomaly-based intrusion detection

It is designed to detect unknown attacks, such as new malware and instantly adapt to them using machine learning. Machine learning techniques enable intrusion detection systems (IDS) to build a base of trust (called a trust model) and then compare the new behavior with the trust model. False positives can occur when using a weak IDS, as previously unknown but legitimate communications can be misidentified as malicious.

Network Architectures As with a network-based IDPS, a separate management network or the organization’s standard networks can be used for NBA component communications. If sensors that collect network flow data from other devices are used, the entire NBA solution can be logically separated from the standard networks. Figure 6-1 shows an example of an NBA network architecture

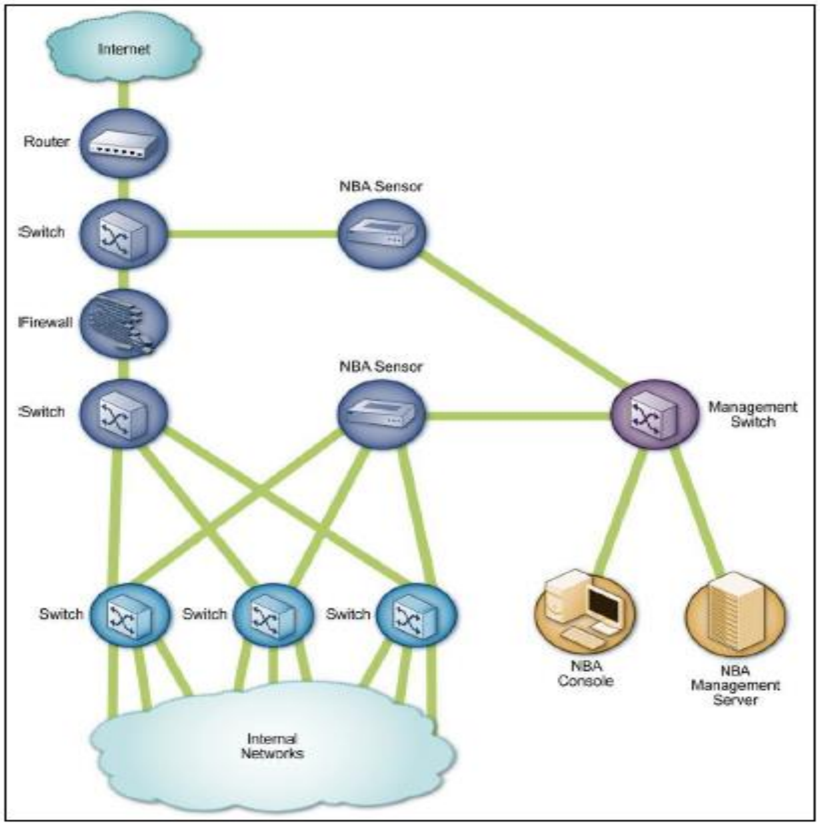


FIG : EXAMPLE OF NBA SENSOR ARCHITECTURE

Sensor Locations

In addition to choosing the appropriate network for the components, administrators also need to decide where the sensors should be located. Most NBA sensors can be deployed in passive mode only, using the same connection methods (e.g., network tap, switch spanning port) as network-based IDPSs. Passive sensors that are performing direct network monitoring should be placed so that they can monitor key network locations, such as the divisions between networks, and key network segments, such as demilitarized zone (DMZ) subnets. Inline sensors are typically intended for network perimeter use, so they would be deployed in close proximity to the perimeter firewalls, often between the firewall and the Internet border router to limit incoming attacks that could overwhelm the firewall.

3.Analyze the impact of social engineering attacks on individuals and organizations, considering factors such as financial losses, reputational damage, and compromised data security.

Ans: Effects of Cybercrime on Different Entities

Cybercrime is a growing threat to individuals in the digital age. With the increasing sophistication of cyberattacks, individuals are becoming more vulnerable to financial loss, identity theft, emotional trauma, and damage to their reputations.

1] On Individuals

- **Financial loss or loss of income :** One of the most common effects of cybercrime on individuals is financial loss. Cybercriminals often use various methods such as phishing, hacking, and malware to gain access to an individual's financial information, such as credit card numbers, bank account details, and passwords. This can result in the loss of money through unauthorized transactions, which can be difficult to recover.
- **Identity theft:** Identity theft is another significant consequence of cybercrime for individuals. Cybercriminals can use stolen personal information such as social security numbers, driver's license numbers, and dates of birth to open new accounts, take out loans, and commit other types of fraud in an individual's name. This can result in financial loss and significant legal and administrative headaches in recovering the individual's identity.
- **Emotional trauma:** In addition to financial loss and identity theft, cybercrime can cause emotional trauma. Victims of cybercrime often feel violated and vulnerable, leading to fear and anxiety. This can have a long-lasting impact on an individual's mental health, especially if they feel isolated and unable to seek help.
- **Loss of reputation:** Lastly, cybercrime can cause damage to an individual's reputation. Cybercriminals can use stolen information to post embarrassing or damaging content online, leading to a loss of credibility and trust. The

effects of reputational damage can be especially damaging in professional settings, leading to job loss or difficulty finding employment.

2] On Businesses

- **Financial loss:** Cybercrime can have devastating financial consequences for businesses, particularly small and medium-sized enterprises. A successful cyberattack can result in the loss of funds, intellectual property, and customer data, which can be costly to recover. In some cases, businesses may even be forced to shut down due to the financial impact of cybercrime.
- **Damage to reputation:** Cybercrime can cause irreparable damage to a business's reputation. A successful cyberattack can expose sensitive customer data, undermining trust and confidence in a business's ability to protect its customers' information. This can lead to losing loyal customers, decreasing revenue, and reducing market share.
- **Legal repercussions:** Businesses can face significant legal repercussions as a result of cybercrime. Data breaches can result in legal action, fines, and penalties, particularly in heavily regulated industries like healthcare and finance.
- **Loss of intellectual property:** Cybercriminals can target businesses to steal intellectual property, such as trade secrets and patents. The loss of intellectual property can be a significant blow to businesses, particularly those that rely on innovation and research to remain competitive. It can further lead to decreased revenues, lost opportunities, and reduced market share, potentially affecting the long-term sustainability of the business.

3] On Society

- **Economic impact:** Cybercrime can have a significant impact on the economy. It can result in financial losses for individuals, businesses, and governments. The cost of repairing damage to systems, recovering lost data, and preventing future attacks can be substantial. It can also impact consumer confidence in online transactions, decreasing business sales and revenue. Additionally, cybercrime can result in the loss of intellectual property, negatively affecting industry innovation and competitiveness.

- **National security concerns:** Cybercrime can pose a serious threat to national security. Attacks on government and military networks can compromise sensitive information and disrupt operations. Cybercriminals can also use technology to engage in espionage, stealing state secrets, and disrupt critical infrastructure, such as power grids and transportation systems. Additionally, cybercrime can be used for political and ideological purposes, leading to social and political unrest.
- **Impact on healthcare and public safety:** Cybercrime can have a significant impact on healthcare and public safety. Attacks on healthcare systems can compromise sensitive patient data and disrupt medical services, which can have life-threatening consequences. Additionally, attacks on critical infrastructure, such as emergency response systems and transportation networks, can put public safety at risk. Cybercriminals can also use technology to commit identity theft, which can financially harm individuals.
- **Increase in cyberbullying and harassment:** Cybercrime can lead to an increase in cyberbullying and harassment. Cybercriminals can use technology to target individuals and groups, spreading malicious content and harassing messages. This can result in emotional and psychological harm and damage to reputations and relationships. Cyberbullying and harassment can also hurt mental health, leading to depression and anxiety. Additionally, cybercrime can spread misinformation, which can have serious social and political consequences.
- **Social media manipulation :** A social media manipulation is a form of cybercrime involving using social media platforms to influence, deceive, or manipulate individuals or groups for political, financial, or personal gain. This can take many forms, including spreading false information, creating fake profiles or personas, and using bots or automated accounts to amplify messages.

The effect of social media manipulation on society can be significant, as it can undermine the integrity of democratic processes, promote extremist ideologies, and erode public trust in institutions and information sources.

Hence knowing prevention strategies is important.

Prevention and Mitigation Strategies

Prevention and mitigation strategies are essential in protecting individuals, businesses, and society from the negative impacts of cybercrime. Cybersecurity threats are becoming increasingly sophisticated and prevalent. There are various measures that individuals, businesses, and governments can take to prevent and mitigate the impact of cybercrime, as follows:

1] Cyber security measures for individuals:

Individuals can take several measures to ensure protection from cybercrime, including:

- Create strong passwords and use two-factor authentication
- Keeping software and operating systems up-to-date with the latest security patches
- Avoid using public Wi-Fi networks and a Virtual Private Network (VPN)
- Being cautious of suspicious emails and messages, especially those containing links or attachments
- Backing up important data regularly
- Educating themselves about cybersecurity threats and best practices

2] Cyber security measures for businesses:

Businesses can take several measures to ensure protection from cybercrime, including:

- Conducting regular security risk assessments
- Implementing access controls and monitoring for suspicious activity
- Providing cyber security training for employees
- Implementing strong passwords, two-factor authentication, and encryption for sensitive data
- Implementing a robust backup and disaster recovery plan
- Regularly updating software and hardware systems

3] Government initiatives and policies:

Governments can implement initiatives and policies to protect citizens from cybercrime, including:

- Establishing cyber security standards and regulations for businesses and organizations
- Providing resources and training for individuals and businesses on cyber security best practices
- Investing in research and development of new cybersecurity technologies and tools
- Enforcing penalties for cybercrime and holding perpetrators accountable
- Sharing threat intelligence and collaborating with international partners to combat cybercrime globally.

4] Investing in creator insurance:

Investing in creator insurance can provide content creators with financial protection and peace of mind. The top benefits are:

- Creator insurance protects content creators from financial loss due to legal disputes or other risks.
- It covers legal fees, damages, and other costs associated with legal claims, such as copyright infringement, defamation, or privacy violations.
- Creator insurance can also protect intellectual property and cover injuries or damage to property or equipment.
- It provides peace of mind and allows creators to focus on their work without worrying about potential financial losses or legal disputes.

4.Compare and contrast the characteristics of malware and ransom ware attacks, including their methods of propagation, objectives, and potential consequences for victims. Evaluate the effectiveness of proactive measures such as regular software updates, antivirus software, and user awareness training in preventing and mitigating the impact of these types of cyber threats.

Ans:

What is Malware?

Malware, short for malicious software, is a broad term encompassing any software designed to harm or exploit computing systems and networks. The different types of malware are vast and varied, each with distinct methods of infiltration and varying impacts.

The most common variations include:

- **Viruses:** These are malicious programs that replicate themselves and spread to other computers, usually attaching themselves to various programs and executing code when a user launches one of those infected programs.
- **Worms:** Worms are similar to viruses in their self-replicating nature, but they can spread without user action. They typically exploit vulnerabilities or weaknesses in operating systems or software to spread across networks.
- **Trojans:** Named after the Greek myth, Trojans appear to be harmless or useful software, but they carry a hidden harmful function. They do not self-replicate but can enable cybercriminals to spy on you, steal sensitive information, or gain backdoor access to your system.
- **Ransom ware:** This type of malware encrypts user’s files and demands a ransom to restore access. Some variants may also threaten to publish the victim’s data unless the ransom is paid.
- **Spyware:** This type of malware covertly collects information about a user’s computer activities, often including keystrokes, emails, web browsing history, and even login credentials, without the user’s consent or knowledge.
- **Adware:** While not always seriously harmful, adware can be annoying and intrusive. It displays unwanted advertisements and can also come bundled with spyware that tracks your activities to tailor ads to you.

- **Root kits:** These are designed to gain administrative level control over a computer system without being detected. They are usually associated with other forms of malware that can use the root kit's functionality to carry out malicious actions.
- **Botnets:** A botnet is a network of infected computers that work together under the control of an attacker. Each individual machine under a botnet's control is referred to as a 'bot'. Botnets are typically used for DDoS attacks, stealing data, sending spam, or allowing the attacker access to the device and its connection

What is Ransomware?

Ransomware is a specific form of malware—in other words, all ransomware is malware, but not all malware is ransomware. It can be one of the most destructive forms of malware, posing a unique and potent threat to individuals, organizations, and businesses alike. It operates by encrypting files and holding them for ransom, often in hard-to-trace cryptocurrency like Bitcoin.

Ransomware infiltrates systems in numerous ways:

- **Phishing Emails:** Ransomware often enters systems via phishing emails. These deceptive messages are cleverly designed to appear legitimate, often masquerading as communications from trusted entities. The unsuspecting user is tricked into opening an infected file or link, thereby downloading the ransomware.
- **Exploit Kits:** These tools are designed to find and take advantage of software vulnerabilities. They are frequently used to spread ransomware by injecting malicious code into insecure websites. If a user visits the compromised website with an outdated or vulnerable application, the ransomware is silently downloaded.
- **Malvertising:** This is a technique that involves injecting malicious code into legitimate online advertising networks. The ads then redirect users to malicious websites which host exploit kits, subsequently leading to a ransomware infection.

- **RDP Attacks:** Remote Desktop Protocol (RDP) is a popular tool among IT professionals. However, unsecured RDP ports can be exploited by cybercriminals to gain access to systems and deploy ransomware.

Malware vs. Ransomware: What are the Differences?

Understanding the difference between malware and ransomware is critical for implementing effective cybersecurity measures.

There are five primary differences between ransomware vs. malware:

1. **Purpose:** The primary difference lies in the purpose of each software. General malware encompasses any malicious software intended to cause damage, steal data, or gain unauthorized access. On the other hand, ransomware, a subset of malware, has a specific goal: to encrypt data and demand a ransom in return for its release.
2. **Impact:** While all malware can cause harm, the impacts vary greatly. Some malware might slow down your system or display unwanted ads, while others can steal sensitive data. Ransomware, however, has a particularly disruptive impact by locking users out of their own files or systems.
3. **Payload Delivery:** Both malware and ransomware use similar delivery methods like phishing emails and exploiting software vulnerabilities. However, some types of malware, like worms, can self-replicate and spread across a network without any user interaction—a feature not typically seen in ransomware.
4. **Recovery:** Generally, the process of recovering from a malware infection involves identifying and removing the malicious software and then restoring the system or affected files from a backup. However, in the case of a ransomware attack, recovery can be much more complex and potentially costly. Unless you have a recent, unaffected backup, the encrypted data may be irretrievable without the decryption key—often only offered in return for the demanded ransom.
5. **Threat Awareness:** Traditional malware often operates covertly, subtly causing damage over time without the user’s knowledge. In contrast, ransomware immediately announces its presence with a ransom note once it

infiltrates a system, aiming to create a sense of urgency and prompt swift action from victims.

	Malware	Ransomware
Goal	Any malicious code designed to perform a variety of unauthorized actions, including damaging digital resources, stealing data and disrupting IT services.	Malicious code specifically designed to lock victims out of their own systems until they make ransom payments. Can also involve extortion, in which attackers exfiltrate data and threaten to publish it online.
Delivery	Delivered in many ways, including via email, USB drives, network worms, Trojans and malicious websites.	Primarily delivered via targeted phishing attacks, RDP attacks or exploited software vulnerabilities.
Removal	Some types of malware can be stopped or removed by antivirus software.	Hard to remove once an infection has occurred and the system has been locked or encrypted.
Motive	Motives for malware vary, ranging from idle criminal mischief to financial gain to nation-state espionage.	The motive in a ransomware attack is financial gain. As such, ransomware qualifies as serious criminal activity.

	Malware	Ransomware
Technical effects	Range from mild performance degradation on a single device to total destruction of an enterprise network.	Often brings all digital activity to a halt until users pay the ransom, restore the system from backup or rebuild the system from scratch.

5.How has the IT Act of 2000, along with its subsequent amendments, shaped the legal landscape for addressing cyber-crime and offenses in India? Discuss the key provisions of the Act related to cyber-security and examine their effectiveness in prosecuting cyber-criminals and protecting individuals and organizations from cyber threats.

Ans: Information Technology Act, 2000 (IT Act):

Overview of the Act:

It is the first cyber law 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, ebanking, 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.

Cybercrimes can be basically divided into four major categories:

1. Cyber Crimes against persons. Cyber crimes committed against persons include various crimes like transmission of childpornography, cyber porn, harassment of a person using a computer such as through e-mail, fake escrow scams. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cyber crimes known today. The potential harm of such a crime to humanity can hardly be explained. Cyber-harassment is a distinct Cyber crime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Different types of harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cyber crimes. Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a Cyber crime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen.

   There are certain offences which affect the personality of individuals can be defined as:

2. Harassment via E-Mails: This is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter, Orkut etc. increasing day by day.

3. Cyber-Stalking: It is expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

4. Defamation: It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

5. Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.

6. Cracking: It is act of breaking into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

7. E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it‟s origin to be different from which actually it originates.

8. SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of

another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual. Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim‟s bank account. There is always unauthorized use of ATM cards in this type of cyber crimes.

9. Cheating & Fraud: It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

10. Child Pornography: In this cyber crime defaulters create, distribute, or access materials that sexually exploit underage children. Assault by Threat: It refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

11. Hacking and Data Theft: Sections 43 and 66 of the IT Act penalise a number of activities ranging from hacking into a computer network, data theft, introducing and spreading viruses through computer networks, damaging computers or computer networks or computer programmes, disrupting any computer or computer system or computer network, denying an authorised person access to a computer or computer network, damaging or destroying information residing in a computer etc. The maximum punishment for the above offences is imprisonment of up to 3 (three) years or a fine or Rs. 5,00,000 (Rupees five lac) or both.

12. Section 378 of the IPC relating to "theft" of movable property will apply to the theft of any data, online or otherwise, since section 22 of the IPC states that the words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth. The maximum punishment for theft under section 378 of the IPC is imprisonment of up to 3 (three) years or a fine or both. It may be argued that the word "corporeal" which means 'physical' or 'material' would exclude digital properties from the ambit of the aforesaid section 378 of the IPC. The counter argument would be that the drafters intended to cover properties of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

13. Section 424 of the IPC states that "whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description1 for a term which may extend to 2 (two) years, or with fine, or with both." This aforementioned section will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 (two) years or a fine or both.

-----------*0000*---------