1)

Intrusion Detection System (IDS):

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

Intrusion Prevention System (IPS):

- Protection Against Known and Unknown Threats: An IPS can block known threats and also detect and block unknown threats that haven't been seen before.
- Real-Time Protection: An IPS can detect and block malicious traffic in real-time, preventing attacks from doing any damage.
- Compliance Requirements: Many industries have regulations that require the use of an IPS to protect sensitive information and prevent data breaches.
- Cost-Effective: An IPS is a cost-effective way to protect your network compared to the cost of dealing with the aftermath of a security breach.
- Increased Network Visibility: An IPS provides increased network visibility, allowing you to see what's happening on your network and identify potential security risks.

The main difference between Intrusion Prevention System (IPS) with Intrusion Detection Systems (IDS) are:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
3. IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

2)

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.

- **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

Host Intrusion Detection System (HIDS): Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the

previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.
- **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

3)

1. Understanding Social Engineering Attacks

Social engineering attacks involve manipulating individuals into revealing sensitive information or performing actions that compromise the security of a network or system. Cybercriminals often rely on social engineering tactics because they exploit the weakest link in any organization's cybersecurity posture: the human factor.

2. Common Social Engineering Tactics

Some of the most prevalent social engineering tactics used by cybercriminals include:

- Phishing: Cybercriminals send deceptive emails or messages that appear to be from a legitimate source, tricking recipients into clicking on malicious links, opening infected attachments, or revealing sensitive information.
- Pretexting: Attackers create a fabricated scenario or impersonate a trusted individual to convince targets to share sensitive data or grant access to systems.
- Baiting: Cybercriminals lure victims with enticing offers, such as free software or hardware, which contain malicious code or lead to compromised websites.
- Tailgating: Attackers gain physical access to restricted areas by following authorized personnel, exploiting their trust and bypassing security measures.

3. The Impact of Social Engineering Attacks on Small Businesses

Social engineering attacks can have severe consequences for small businesses, including:

- Data breaches: Successful social engineering attacks may lead to unauthorized access to sensitive data, such as customer information, intellectual property, or financial records.

- Financial loss: Cybercriminals may use social engineering tactics to gain access to bank accounts, credit cards, or other financial resources, resulting in significant losses for the business.

- Reputational damage: Data breaches or other security incidents stemming from social engineering attacks can harm a small business's reputation, potentially leading to lost customers, partners, or revenue.

- Legal and regulatory repercussions: Small businesses that suffer data breaches or other security incidents due to social engineering attacks may face legal penalties or regulatory fines, especially if sensitive customer data is compromised.

4. Protecting Your Small Business from Social Engineering Attacks

To safeguard your small business against social engineering attacks, consider implementing the following strategies:

- Employee training: Educate your employees about social engineering tactics and provide regular training on how to recognize and respond to potential attacks.

- Establish clear policies and procedures: Develop policies and procedures for handling sensitive information, verifying the identity of individuals requesting access to data or systems, and reporting suspected social engineering attempts.

- Multi-factor authentication: Implement multi-factor authentication (MFA) for accessing sensitive systems and information, adding an extra layer of protection against social engineering attacks.

- Regular communication and awareness campaigns: Maintain open lines of communication with your employees about emerging social engineering threats and reinforce the importance of following security best practices.

- Incident response planning: Develop a robust incident response plan that outlines the steps your organization will take in the event of a social engineering attack, including reporting, containment, and recovery measures.

5. The Future of Social Engineering Attacks and Cybersecurity

As technology continues to advance and cybercriminals become increasingly sophisticated, small businesses must remain vigilant in protecting themselves from social engineering attacks. By staying informed about emerging threats, training employees, and implementing robust security measures, small businesses can minimize the risks associated with social engineering attacks and maintain a strong cybersecurity posture.

In conclusion, the cybersecurity risks associated with social engineering attacks are significant, with cybercriminals exploiting human psychology and trust to compromise small businesses

4)

Malware is one of the greatest security threats enterprises face. Security departments must actively monitor networks to catch and contain malware before it can cause extensive damage. With malware, however, prevention is key. But to prevent an attack, it is critical to first understand what malware is, along with the most common types of malware.

Attackers use malware, short for malicious software, to intentionally harm and infect devices and networks. The umbrella term encompasses many subcategories, including the following:

1. Viruses.
2. Worms.
3. Ransomware.
4. Bots.
5. Trojan horses.
6. Keyloggers.
7. Rootkits.
8. Spyware.
9. Fileless malware.
10. Cryptojacking.
11. Wiper malware.
12. Adware.

1). Viruses

A computer virus infects devices and replicates itself across systems. Viruses require human intervention to propagate. Once users download the malicious code onto their devices -- often delivered via malicious advertisements or phishing emails -- the virus spreads throughout their systems. Viruses can modify computer functions and applications; copy, delete and exfiltrate data; encrypt data to perform ransomware attacks; and carry out DDoS attacks.

The Zeus virus, first detected in 2006, is still used by threat actors today. Attackers use it to create botnets and as a banking Trojan to steal victims' financial data. Zeus's creators released the malware's source code in 2011, enabling threat actors to create updated and more threatening versions of the original virus.

2. Worms

A computer worm self-replicates and infects other computers without human intervention. This malware inserts itself in devices via security vulnerabilities or malicious links or files. Once inside, worms look for networked devices to attack. Worms often go unnoticed by users, usually disguised as legitimate work files.

WannaCry, also a form of ransomware, is one of the most well-known worms. The malware took advantage of the EternalBlue vulnerability in outdated versions of Windows' Server Message Block protocol. In its first year, the worm spread to 150 countries. The next year, it infected nearly 5 million devices.

3. Ransomware

Ransomware locks or encrypts files or devices and forces victims to pay a ransom in exchange for reentry. While ransomware and malware are often used synonymously, ransomware is a specific form of malware.

Common types of ransomware include the following:

- **Locker ransomware** completely locks users out of their devices.
- **Crypto ransomware** encrypts all or some files on a device.
- **Extortionware** involves attackers stealing data and threatening to publish it unless a ransom is paid.
- **Double extortion ransomware** encrypts and exports users' files. This way, attackers can potentially receive payments from the ransom and/or the selling of the stolen data.
- **Triple extortion ransomware** adds a third layer to a double extortion attack, for example, a DDoS attack, to demand a potentially third payment.

- Ransomware as a service, also known as RaaS, enables affiliates or customers to rent ransomware. In this subscription model, the ransomware developer receives a percentage of each ransom paid.

Well-known ransomware variants include REvil, WannaCry and DarkSide, the strain used in the Colonial Pipeline attack.

Data backups were long the go-to defense against ransomware. With a proper backup, victims could restore their files from a known-good version. With the rise of extortionware, however, organizations must follow other measures to protect their assets from ransomware, such as deploying advanced protection technologies and antimalware.

Cyber hygiene practices that prevent malware attacks include the following:

- Patch and update software.
- Use firewalls and security software, such as antimalware and antivirus.
- Follow email security best practices.
- Deploy email security gateways.
- Avoid clicking links and downloading attachments.
- Implement strong access control.
- Require multifactor authentication.
- Use the principle of least privilege.
- Adopt a zero-trust security strategy.
- Monitor for abnormal or suspicious activity.

5)

Digital Signature under the IT Act, 2000 Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3. Electronic Signature Electronic signature has also been dealt with under Section 3A of the IT Act, 2000. A subscriber can authenticate any electronic record by such electronic signature or electronic authentication technique which

is considered reliable and may be specified in the Second Schedule. An Amendment to the IT Act in 2008 introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures. E-Governance E-governance or Electronic Governance is dealt with under Sections 4 to 10A of the IT Act, 2000. It provides for legal recognition of electronic records and Electronic signature and also provides for legal recognition of contracts formed through electronic means. Filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. Controller of Certifying Authorities (CCA) The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users. The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. Penalties and Offences Cyber Crime Brief Description Relevant Section in IT Act Punishments Cyber Stalking Stealthily following a person, tracking his internet chats. 43, 65, 66 3 years, or with fine up to 2 lakh Cyber Pornography including child pornography Publishing Obscene in Electronic Form involving children 67, 67 (2) 10 years and with fine may extends to 10 lakh Intellectual Property Crimes Source Code Tampering, piracy, copyright infringement etc. 65 3 years, or with fine up to 2 lakh Cyber Terrorism Protection against cyber terrorism 69 Imprisonment for a term, may extend to 7 years Cyber Hacking Destruction, deletion, alteration, etc in a computer resources 66 3 years, or with fine up to 2 lakh Phishing Bank Financial Frauds in Electronic Banking 43, 65, 66 3 years, or with fine up to 2 lakh