SCHOOL OF CONTINUING AND DISTANCE EDUCATION

JAWAHARLAL NEHRU TECHNOLOGICALUNIVERSITY - HYDERABAD

Kukatpally, Hyderabad – 500 085, Telangana, India.

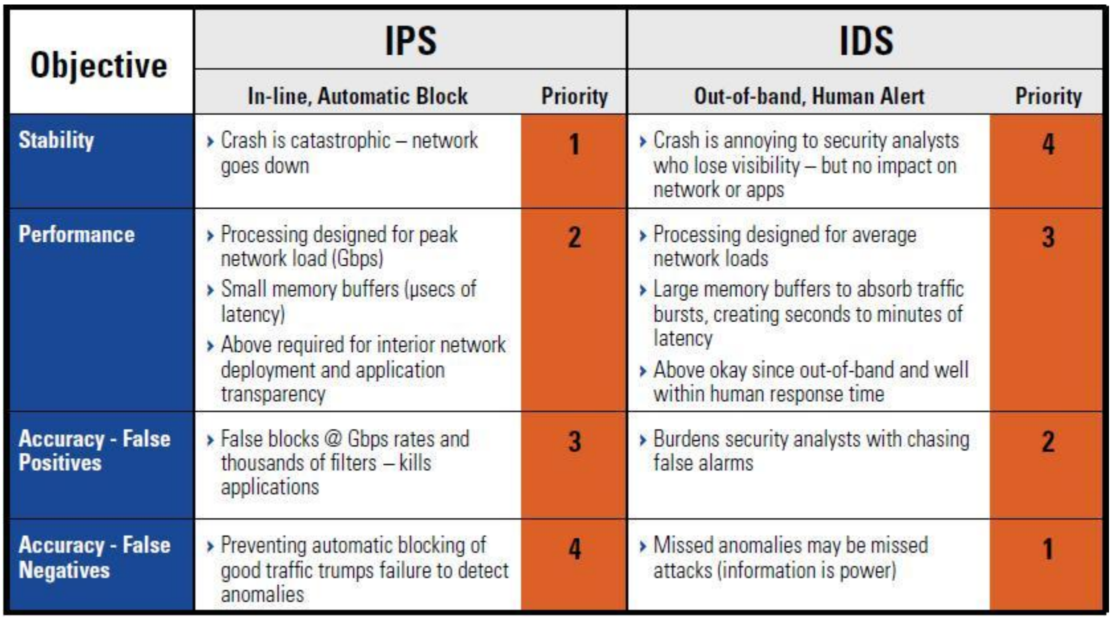
SIX MONTH ONLINE CERTIFICATE COURSES – 2023

CYBER SECURITY - ASSIGNMENT - 03

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

Ans: IDS and IPS are originally developed for addressing requirements of lacking in most firewalls. IDS are basically used to detecting the threats or intrusions in network segment. But IPS is focused on identifying those threats or intrusions for blocking or dropping their activities.

The best example of security gate in term of difference of IDS and IPS is, An IDS works like a patrol car within the border, monitoring activities and looking for abnormal situations. But an IPS operates like a security guard at the gate of allowing and denying access based on credentials and some predefined rule set, or policy. No matter how strong the security at the gate is, the patrols continue to operate in a system that provides its own checks.



Objective	IPS		IDS	
	In-line, Automatic Block	Priority	Out-of-band, Human Alert	Priority
Stability	› Crash is catastrophic – network goes down	1	› Crash is annoying to security analysts who lose visibility – but no impact on network or apps	4
Performance	› Processing designed for peak network load (Gbps) › Small memory buffers (μsecs of latency) › Above required for interior network deployment and application transparency	2	› Processing designed for average network loads › Large memory buffers to absorb traffic bursts, creating seconds to minutes of latency › Above okay since out-of-band and well within human response time	3
Accuracy - False Positives	› False blocks @ Gbps rates and thousands of filters – kills applications	3	› Burdens security analysts with chasing false alarms	2
Accuracy - False Negatives	› Preventing automatic blocking of good traffic trumps failure to detect anomalies	4	› Missed anomalies may be missed attacks (information is power)	1

Differences of IDS and IPS are categorized in four objectives as :

Network Stability & Performance:

The IDS are deployed out of band in network means it passes all network traffic to this system but not through in between devices, the processing capability is matching with average network load. The latency between capture and reporting can range from a few seconds to minutes, but also it also depends on human response time. The IDS are a logging device, the large memory buffers to absorb traffic bursts & average network loads.

The IPS are deployed in-line in network means, it passes through in between the devices and which works in peak network load with large memory buffers to absorb traffic bursts is unacceptable. The latency is in microseconds which give the faster application response time with higher processing capacity.

Accuracy- False Positives:

There are three basic rules to find accuracy with false positives in IDS and IPS:

- The IDS has minimizes false positives but an IPS have no false positives. This changes dramatically the writing and testing of the alert filters.

- The IDS false positive alerts on an intrusion that it can be or cannot be – succeed, but IPS false positive blocks legitimate traffic.

- The anomaly filters cannot be used for blocking.

Accuracy- False Negatives:

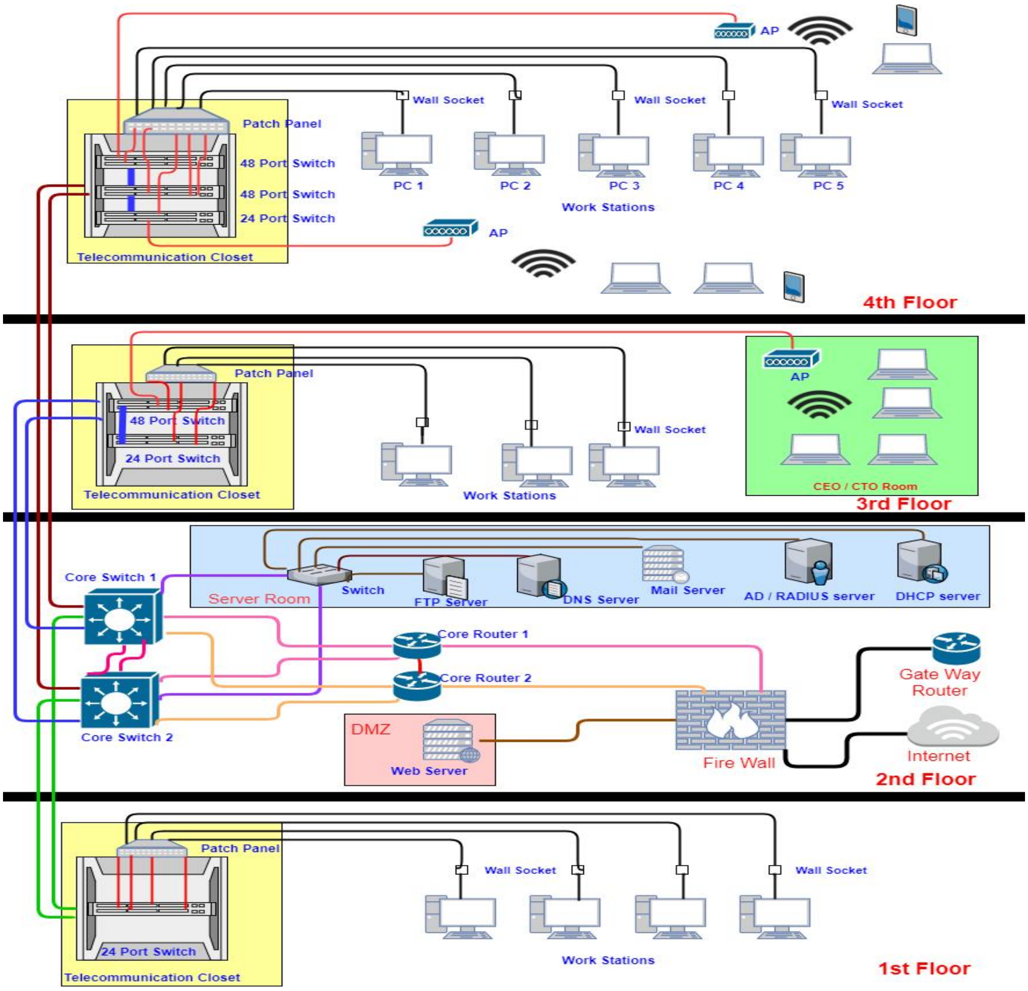
The accuracy of false negatives is simply a missed attack. The goal of this type of system is based on coverage of high priority attacks. The IDS may become overwhelmed with traffic beyond its capacity, dropping packets needed to detect the attack and an IPS is overwhelming the device causes traffic to be blocked or dropped preventing the attack from succeeding to detect anomalies.

Data log analysis:

The IDS and IPS devices are gives a comprehensive logs and data collection, its without actionable alerts, the data gathered from these devices and sensors throughout the network can be used for event correlation and network forensics in a post-attack scenario. This type of data is critical for analysis during and after attacks and can help for organization with both incident response and compliance audits.

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.

Ans:



Network Protocols used in this Network Design

Routing

1. **Static Routing** – Static routes are configured on gateway/core routers of each branches and in main site, to route the traffic from inside network to another branch network. As the next hop (IP of each branch network) is known this can be used. Since this is a **small network using static routes are simple and easy**. It's secure because no any routing advertisements are exchanged between neighbors and computing resources are conserved because no routing algorithm or update mechanisms required.
2. **Default routing** – This is configured on core routers to route the traffic from inside network to ISP router for unknown traffic (towards internet)
3. **Inter VLAN routing** – Core routers are configured to route the traffic between different VLAN in the network. The traffic will reach the core routers from core switch which are connected by trunk link. All VLAN networks will be shown as directly connected routes in routing table (sub interfaces are used)

DHCP (Dynamic Host Configuration Protocol)

DHCP service is installed in the DHCP server which resides in server room. IP address pool for different VLAN will be created in DHCP server. So DHCP server dynamically assign the IP address to the hosts in the network. Static IP address that will be used with in the VLAN can be removed from the IP address pool (excluded address) in DHCP server. Main advantage of using this protocol is **reliable IP address configuration to hosts** (reduce configuration errors caused by manual IP assignment), and **reduced network administration** (centralized management)

STP (Spanning Tree Protocol)

The redundant link connection is provided between the switches in each floor to the 2 core switches located in 2nd floor. Also redundant link is added between 2 core routers and 2 core switches as well as between server room switch and 2 core switches. The purpose of having an extra link is that, if one link goes down still the network components can communicate with each using the redundant link. So, there will be **less down time in the network**. But there is a concern of adding an extra link between network switches is that, it will create a broadcast storm (loop). To avoid this problem, STP protocol is used with in switches in this network. So, at a time one active link will be present and another link will be in blocked mode. Once the active link fails, the redundant link come into active mode from blocked mode.

Signature vs. anomaly-based intrusion detection systems

Signature-based and anomaly-based are the two main methods of detecting threats that intrusion detection systems use to alert network administrators of signs of a threat.

Signature-based detection is typically best used for identifying known threats. It operates by using a pre-programmed list of known threats and their indicators of compromise (IOCs). An IOC might be a specific behavior that generally precedes a malicious network attack, file hashes, malicious domains, known byte sequences, or even the content of email subject headings. As a signature-based IDS monitors the packets traversing the network, it compares these packets to the database of known IOCs or attack signatures to flag any suspicious behavior.

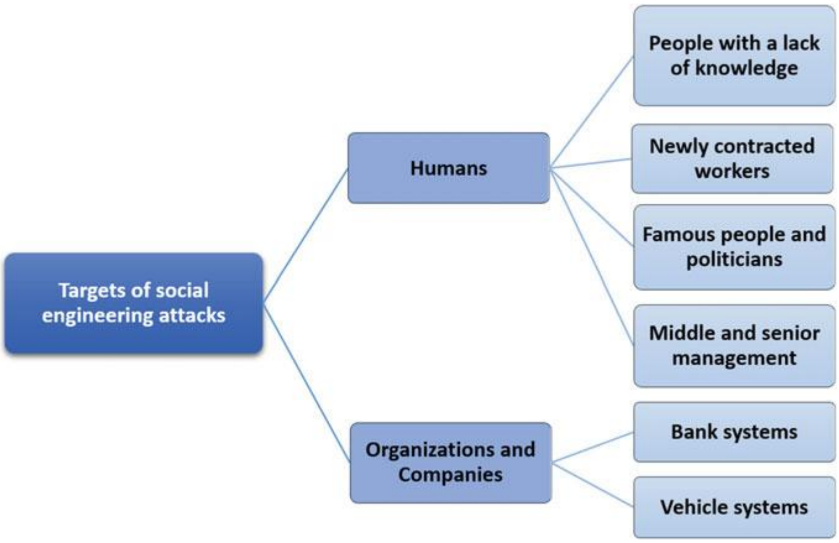
On the other hand, anomaly-based intrusion detection systems can alert you to suspicious behavior that is unknown. Instead of searching for known threats, an anomaly-based detection system utilizes machine learning to train the detection system to recognize a normalized baseline. The baseline represents how the system normally behaves, and then all network activity is compared to that baseline. Rather than searching for known IOCs, anomaly-based IDS simply identifies any out-of-the-ordinary behavior to trigger alerts.

With an anomaly-based IDS, anything that does not align with the existing normalized baseline—such as a user trying to log in outside of standard business hours, new devices being added to a network without authorization, or a flood of new IP addresses trying to establish a connection with a network—will raise a potential flag for concern. The disadvantage here is that many non-malicious behaviors will get flagged simply for being atypical. The increased likelihood for false positives with anomaly-based intrusion detection can require additional time and resources to investigate all the alerts to potential threats.

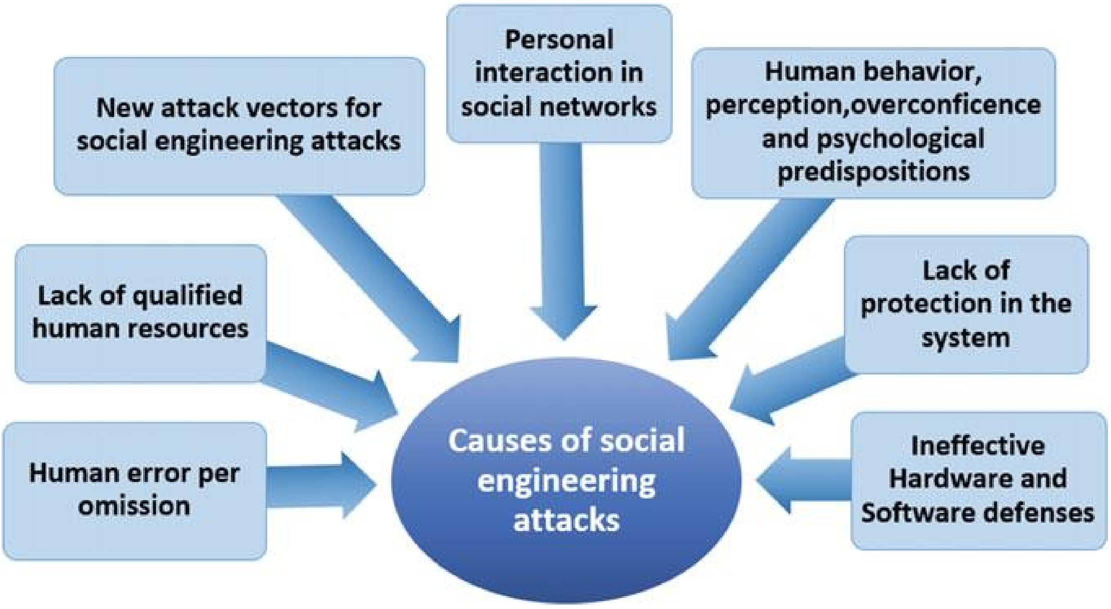
At the same time, this potential disadvantage is also what makes anomaly-based intrusion detection able to detect zero-day exploits signature-based detection cannot. Signature-based detection is limited to a list of known, existing threats. On the other hand, it also has a high processing speed and greater accuracy for known attacks. These two detection methods have advantages and disadvantages that generally complement each other well, and are often used best in tandem.

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:

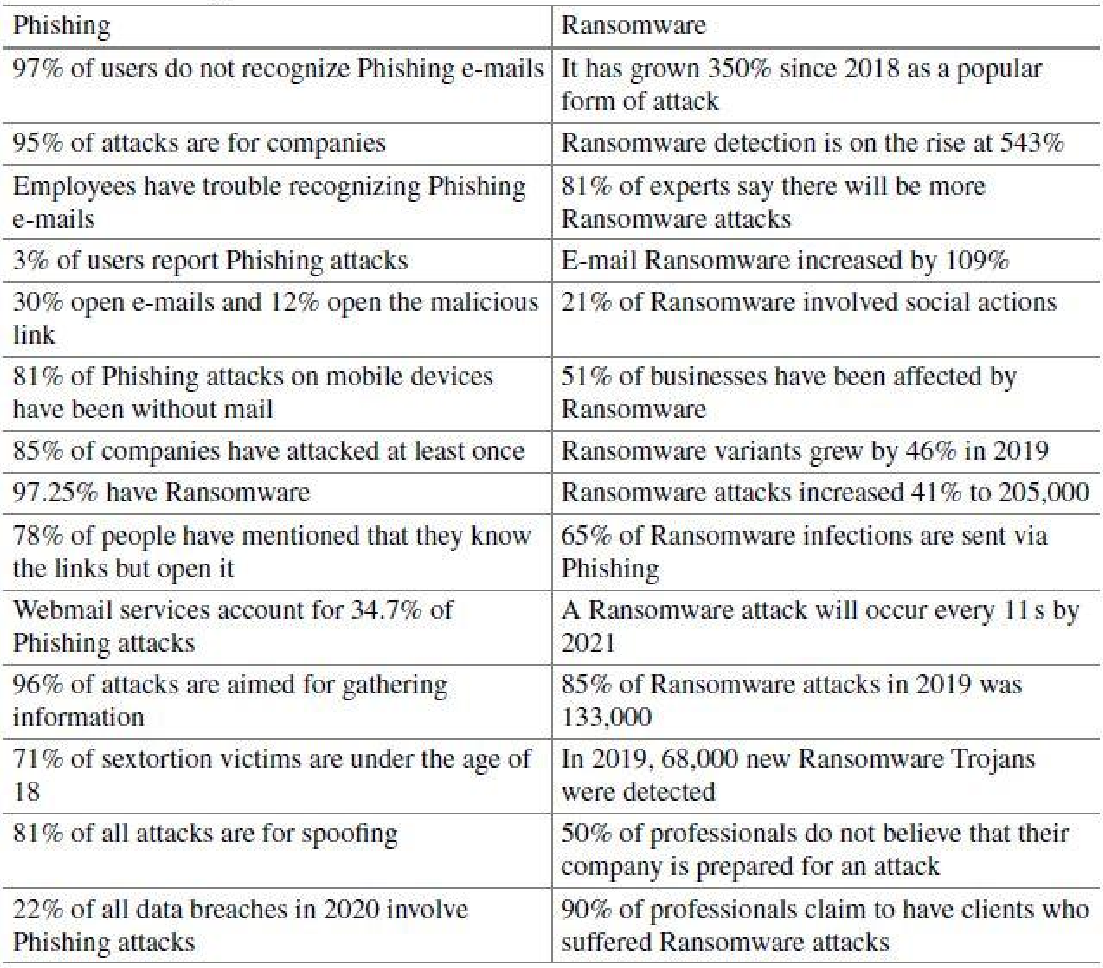

Targets of social engineering attacks
Humans
Organizations and Companies
People with a lack of knowledge
Newly contracted workers
Famous people and politicians
Middle and senior management
Bank systems
Vehicle systems

Primary targets of social engineering attacks


New attack vectors for social engineering attacks
Personal interaction in social networks
Human behavior, perception,overconficence and psychological predispositions
Lack of qualified human resources
Lack of protection in the system
Human error per omission
Causes of social engineering attacks
Ineffective Hardware and Software defenses

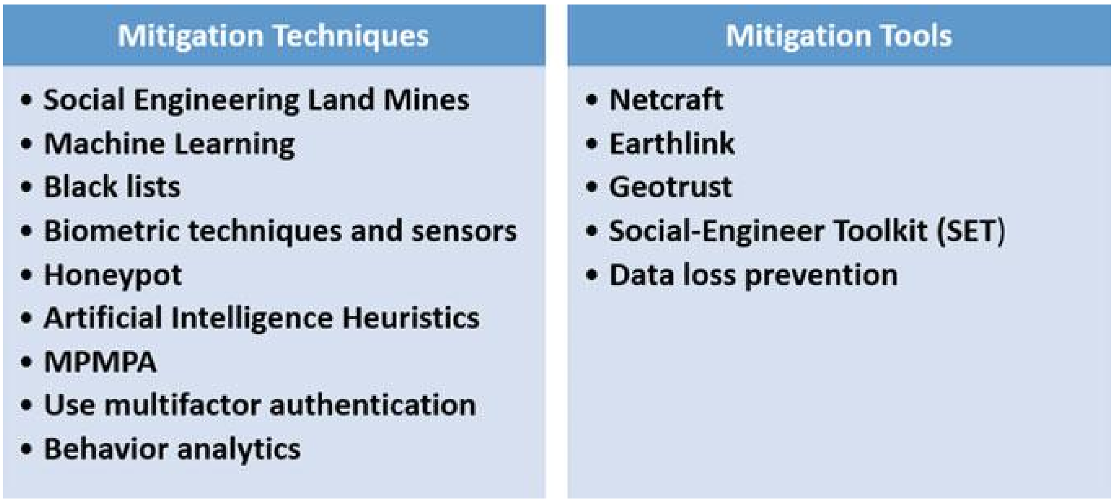
Causes of social engineering attacks

Table 3.1 Phishing versus Ransomware statistics



Phishing	Ransomware
97% of users do not recognize Phishing e-mails	It has grown 350% since 2018 as a popular form of attack
95% of attacks are for companies	Ransomware detection is on the rise at 543%
Employees have trouble recognizing Phishing e-mails	81% of experts say there will be more Ransomware attacks
3% of users report Phishing attacks	E-mail Ransomware increased by 109%
30% open e-mails and 12% open the malicious link	21% of Ransomware involved social actions
81% of Phishing attacks on mobile devices have been without mail	51% of businesses have been affected by Ransomware
85% of companies have attacked at least once	Ransomware variants grew by 46% in 2019
97.25% have Ransomware	Ransomware attacks increased 41% to 205,000
78% of people have mentioned that they know the links but open it	65% of Ransomware infections are sent via Phishing
Webmail services account for 34.7% of Phishing attacks	A Ransomware attack will occur every 11 s by 2021
96% of attacks are aimed for gathering information	85% of Ransomware attacks in 2019 was 133,000
71% of sextortion victims are under the age of 18	In 2019, 68,000 new Ransomware Trojans were detected
81% of all attacks are for spoofing	50% of professionals do not believe that their company is prepared for an attack
22% of all data breaches in 2020 involve Phishing attacks	90% of professionals claim to have clients who suffered Ransomware attacks

Most prominent techniques and tools to mitigate SE attacks



Mitigation Techniques

- Social Engineering Land Mines
- Machine Learning
- Black lists
- Biometric techniques and sensors
- Honeypot
- Artificial Intelligence Heuristics
- MPMPA
- Use multifactor authentication
- Behavior analytics

Mitigation Tools

- Netcraft
- Earthlink
- Geotrust
- Social-Engineer Toolkit (SET)
- Data loss prevention

This field requires responsibility and technological awareness.Within the main findings concerning the impacts of SE attacks, we realized that they are focused on organizations, financial entities, and vehicles' issues, mostly related to human omissions. Social networks and e-mails are the primary sources from which attacks occur, including Phishing and Ransomware as the most common. Among the most used techniques, we encountered artificial intelligence, machine learning, social engineering mining, and, to a lesser size, techniques which allow technicians to analyze human behavior.

4.Compare and contrast the characteristics of malware and ransomware 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: Currently, malware and ransomware-based detection systems have utilized static and dynamic analysis methodologies to collect information on generalized malware and ransomware behavior. Static analysis methods have focused on anti-malware systems to check files against known and common "malicious" signatures. Static analysis methods may have limitations as new or obfuscated files may not be detected, as a signature may not exist. . . As malware continues to evolve and becomes more pervasive, static analysis methods have become less effective, and security researchers have shifted their focus to dynamic detection methods to better prevent malware attacks.

However, a real-time system would be more effective in a production environment, if it is able to detect and differentiate malware and ransomware from benign applications. Security professionals and anti-malware services will need to react to ransomware differently relative to other malicious attacks. It is necessary to distinguish ransomware from other malicious attacks to prevent disruption in business systems and stifle revenue streams.

Ransomware can be classified into the following four categories:

Scareware: a pop-up message is received stating that a malware infection is discovered and that to remove it, a certain amount needs to be paid. If no action is taken, popups will continue to be bombarded, but no harm to files is done.

Screen lockers: also known as non-encrypting ransomware, on starting up the system, a full-size window will appear with a logo from a government agency stating an illegal activity has been detected on the device and demands some amount. The user is not allowed to perform any work by locking the screen or flooding the device with pop-ups.

Encrypting ransomware: also known as cryptoransomware, files are encrypted and taken out of the system. Payment is demanded in order to decrypt and redeliver.

Mobile ransomware - affects mobile devices via malicious apps or drive-by downloads. A message appears that due to some illegal activity, the device is locked and can be unlocked after paying a penalty. Due to the provision of automated cloud data backups, encryption of data does not benefit attackers.

Preventive measures and incident response:

Ransomware attack starts by gaining access to the system, followed by Reconnaissance, in which Attackers identify files containing important data and additional credentials to move laterally throughout the network. After this, in the Activation phase, the Encryption process starts. Deletion of backups and disabling of system restore features is done in this phase. Lastly, a ransom note is left in the system often via a .txt file or through a pop-up message. It contains information to pay the ransom demand.

Protective measures to avoid attacks include:

It includes defence-in-depth by using layers of defence; secure email gateways to provide security from targeted attack; secure web gateways to scan and identify malicious traffic; monitoring tools for server and network to detect anomalies; maintaining proper and tested backups of sensitive data and system images on other devices disconnected from the network; applying the latest and tested patches; providing regular security awareness training and drills for users and implementing network protection policies such as least privilege, zero-trust architecture, segmentation of the network, etc.

Steps for responding to a ransomware

It is reported that 51% of organizations do not have a prescribed ransomware policy. The human error turned out to be the primary cause of data breaches in more than

50% of cases. A tested Business Continuity Plan helps to avoid major operational disruption, without which it becomes tedious to analyze the harm made to the system and then restoration of the affected network.

The following steps can be taken to minimize damage and quickly return to business as usual in case of ransomware attack.

- Isolate the infected device from the network to contain the infection.

- Disconnect all suspiciously behaving devices from the network to stop the spread of infection.

- Assess the damages by preparing a complete list of all affected systems and devices.

- Identify the entry point by checking for any alerts from any active monitoring platform and identify the ransomware by scanning encrypted files and ransom note.

- Reporting the ransomware attack to authorities is needed as per the rules of law enforcement agencies.

If backup is available, restore the systems from a backup. Otherwise, try for decryption options available online.

- In case of unavailability of backups and a decryption key, start 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: The Act defines various offences related to breach of data and privacy of an individual and provides punishment or penalties for them. It also talks about intermediaries and regulates the power of social media. With the advancement of technology and e-commerce, there has been a tremendous increase in cyber crimes and offences related to data and authentic information. Even the data related to the security and integrity of the country was not safe, and so the government decided to regulate the activities of social media and data stored therein. The article gives the objectives and features of the Act and provides various offences and their punishments as given in the Act.

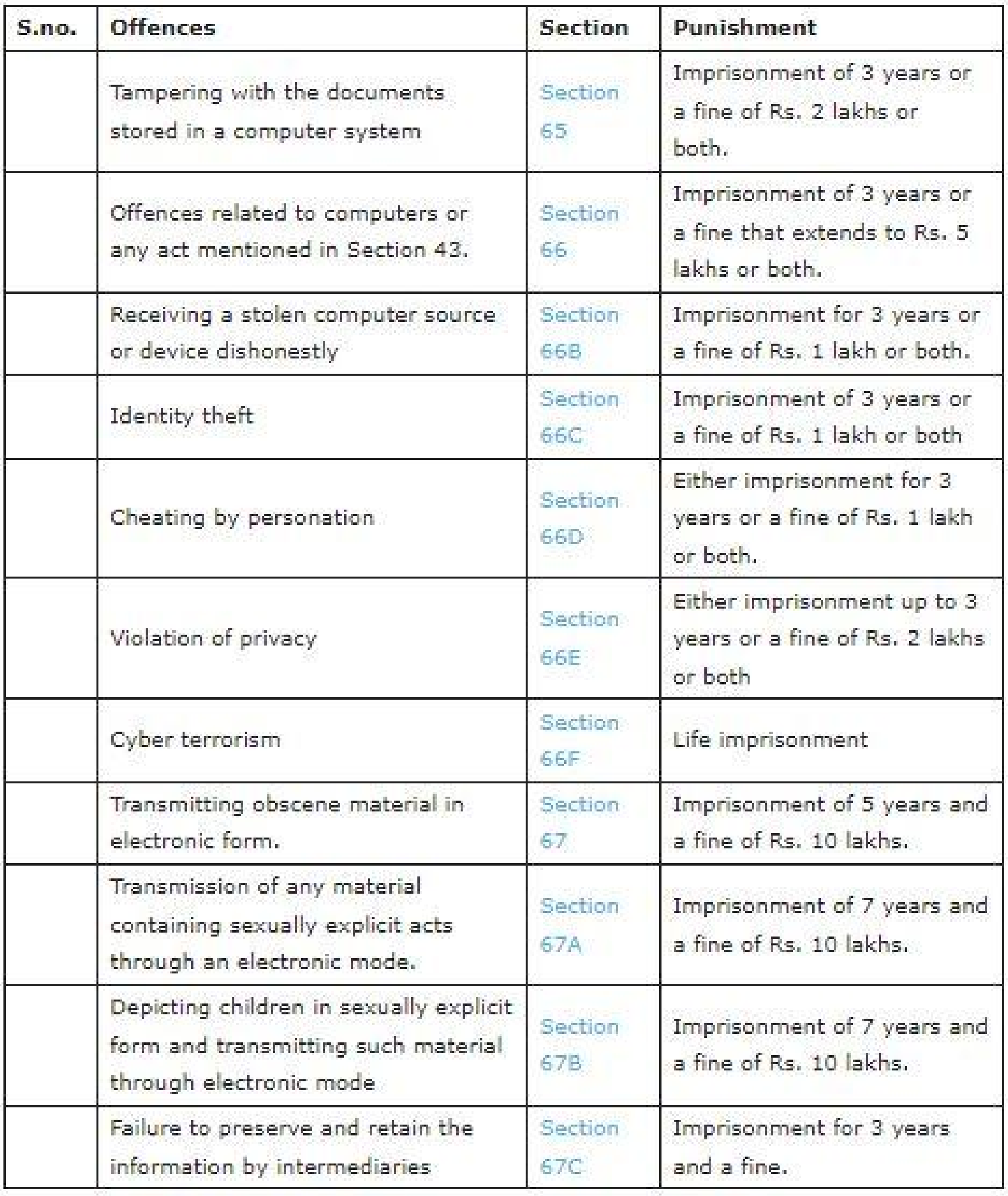
Schedule of Information Technology Act, 2000;

The Act is divided into 13 chapters, 90 sections and 2 schedules.

The features of the Act:

- The Act is based on the Model Law on e-commerce adopted by UNCITRAL.
- It has extra-territorial jurisdiction.
- It defines various terminologies used in the Act like cyber cafes, computer systems, digital signatures, electronic records, data, asymmetric cryptosystems, etc under Section 2(1).
- It protects all the transactions and contracts made through electronic means and says that all such contracts are valid. (Section 10A)
- It also gives recognition to digital signatures and provides methods of authentication.
- It contains provisions related to the appointment of the Controller and its powers.
- It recognises foreign certifying authorities (Section 19).
- It also provides various penalties in case a computer system is damaged by anyone other than the owner of the system.
- The Act also provides provisions for an Appellate Tribunal to be established under the Act. All the appeals from the decisions of the Controller or other Adjudicating officers lie to the Appellate tribunal.
- Further, an appeal from the tribunal lies with the High Court.
- The Act describes various offences related to data and defines their punishment.
- It provides circumstances where the intermediaries are not held liable even if the privacy of data is breached.
- A cyber regulation advisory committee is set up under the Act to advise the Central Government on all matters related to e-commerce or digital signatures.

Offences and their punishments under Information Technology Act, 2000



S.no.	Offences	Section	Punishment
	Tampering with the documents stored in a computer system	Section 65	Imprisonment of 3 years or a fine of Rs. 2 lakhs or both.
	Offences related to computers or any act mentioned in Section 43.	Section 66	Imprisonment of 3 years or a fine that extends to Rs. 5 lakhs or both.
	Receiving a stolen computer source or device dishonestly	Section 66B	Imprisonment for 3 years or a fine of Rs. 1 lakh or both.
	Identity theft	Section 66C	Imprisonment of 3 years or a fine of Rs. 1 lakh or both
	Cheating by personation	Section 66D	Either imprisonment for 3 years or a fine of Rs. 1 lakh or both.
	Violation of privacy	Section 66E	Either imprisonment up to 3 years or a fine of Rs. 2 lakhs or both
	Cyber terrorism	Section 66F	Life imprisonment
	Transmitting obscene material in electronic form.	Section 67	Imprisonment of 5 years and a fine of Rs. 10 lakhs.
	Transmission of any material containing sexually explicit acts through an electronic mode.	Section 67A	Imprisonment of 7 years and a fine of Rs. 10 lakhs.
	Depicting children in sexually explicit form and transmitting such material through electronic mode	Section 67B	Imprisonment of 7 years and a fine of Rs. 10 lakhs.
	Failure to preserve and retain the information by intermediaries	Section 67C	Imprisonment for 3 years and a fine.

Shreya Singhal v. Union of India (2015)

Facts

In this case, 2 girls were arrested for posting comments online on the issue of shutdown in Mumbai after the death of a political leader of Shiv Sena. They were charged under Section 66A for posting the offensive comments in electronic form. As a result, the constitutional validity of the Section was challenged in the Supreme Court stating that it infringes upon Article 19 of the Constitution.

Issue

Whether Section 66A is constitutionally valid or not?

Judgment

The Court, in this case, observed that the language of the Section is ambiguous and vague, which violates the freedom of speech and expression of the citizens. It then struck down the entire Section on the ground that it was violative of Article 19 of the Constitution. It opined that the Section empowered police officers to arrest any person whom they think has posted or messaged anything offensive. Since the word 'offensive' was not defined anywhere in the Act, they interpreted it differently in each case. This amounted to an abuse of power by the police and a threat to peace and harmony.

M/S Gujarat Petrosynthese Ltd and Rajendra Prasad Yadav v. Union of India (2014)

Facts

In this case, the petitioners demanded the appointment of a chairperson to the Cyber Appellate Tribunal so that cases can be disposed of quickly and someone can keep a check on the workings of CAT. The respondents submitted that a chairperson would be appointed soon.

Issue

Appointment of the chairperson of CAT.

Judgment

The Court ordered the appointment of the chairperson and must see this as a matter of urgency and take into account Section 53 of the Act.

Christian Louboutin SAS v. Nakul Bajaj and Ors (2018)

Facts

In this case, a suit was filed by a shoe company to seek an order of injunction against the defendants for using its trademarks and logo.

Issue

Whether the protection of "safe harbour" under Section 79 of the Act be applied in this case?

Judgment

The Court in this case observed that the defendant was not an intermediary as their website was a platform for the supply of various products. It used third-party information and promoted vendors in order to attract consumers for them. The Court held that e-commerce platforms are different from the intermediaries and the rights granted to them in Section 79 of the Act. It ordered the intermediaries to work with due diligence and not infringe the rights of the trademark owner. They must take steps to recognise the authenticity and genuineness of the products while dealing with any merchant or dealer.

The Court added that if the intermediaries act negligently regarding IPR and indulge in any sort of abetment or incitement of unlawful or illegal activity, they will be exempted from the protection of safe harbour under Section 79 of the Act. Any active participation in e-commerce would also lead to the same. It also referred to the intermediaries guidelines, which state that no intermediary must violate any intellectual property rights of anyone while displaying any content on its website.