D.N.R COLLEGE (AUTONOMOUS), BHIMAVARAM

DEPARTMENT OF COMMERCE

III B.COM(CA) – V SEMESTER

CYBER SECURITY & MALWARE ANALYSIS

R. RADHA RANI

LECTURER IN COMMERCE

1 UNIT

Explain types of Computer Networks.

Computer Network: A computer network is a cluster of computers over a shared communication path that works for the purpose of sharing resources from one computer to another, provided by or located on the network nodes.

Types of Computer Networks

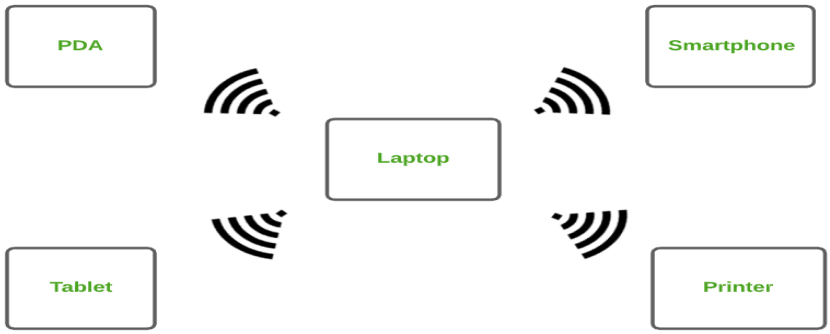
1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Wide Area Network (WAN)
4. Wireless Local Area Network (WLAN)
5. Metropolitan Area Network (MAN)
6. Storage Area Network (SAN)
7. Virtual Private Network (VPN)

These are explained as following below.

1. Personal Area Network (PAN) :

PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centred only to an individual's work space. PAN offers a network range of 10 meters from a person to the device providing communication.

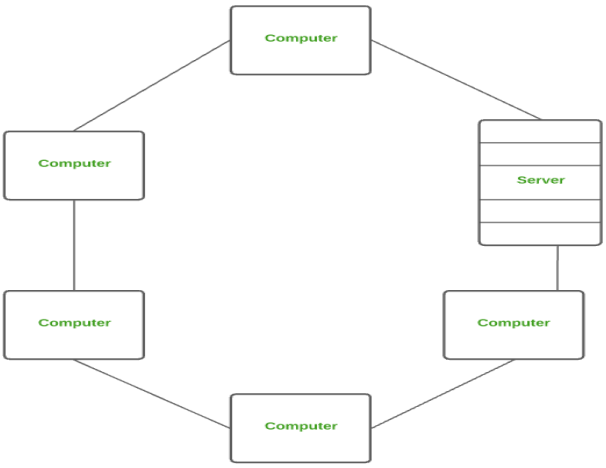
Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.



2. Local Area Network (LAN) :

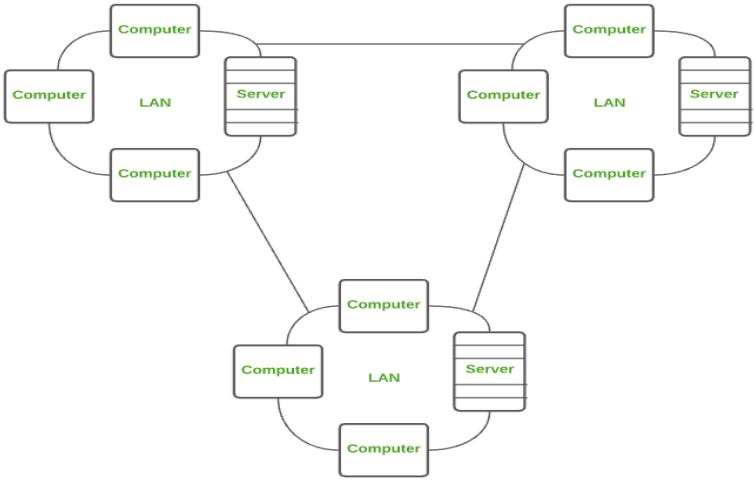
LAN is the most frequently used network. A LAN is a computer network that connects computers together through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi.

Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



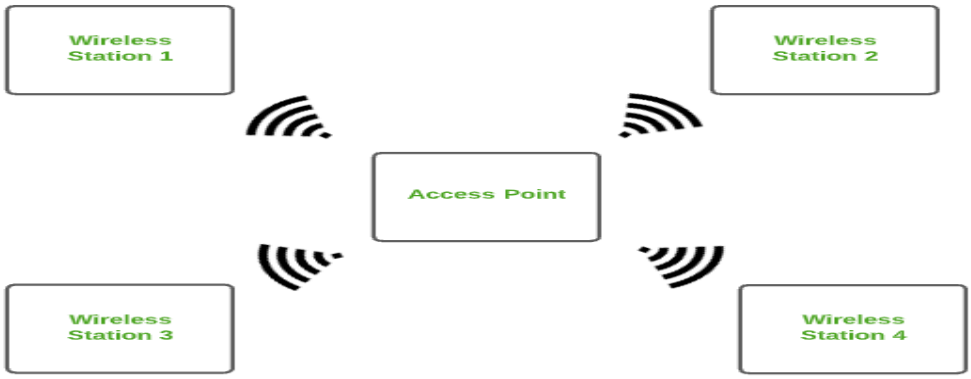
3. Wide Area Network (WAN) :

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other.
The most common example of WAN is the Internet.

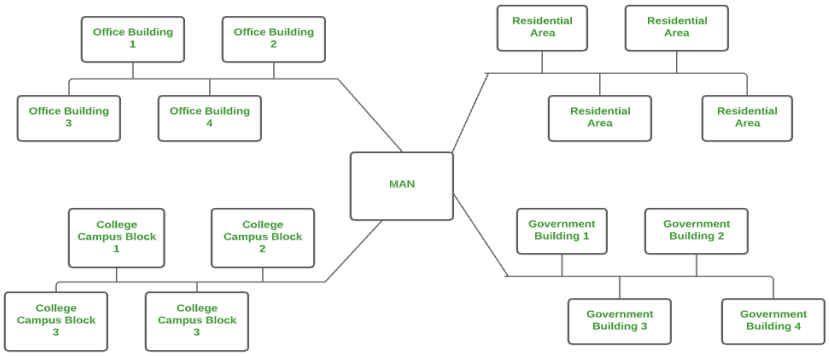


4. Wireless Local Area Network (WLAN) :

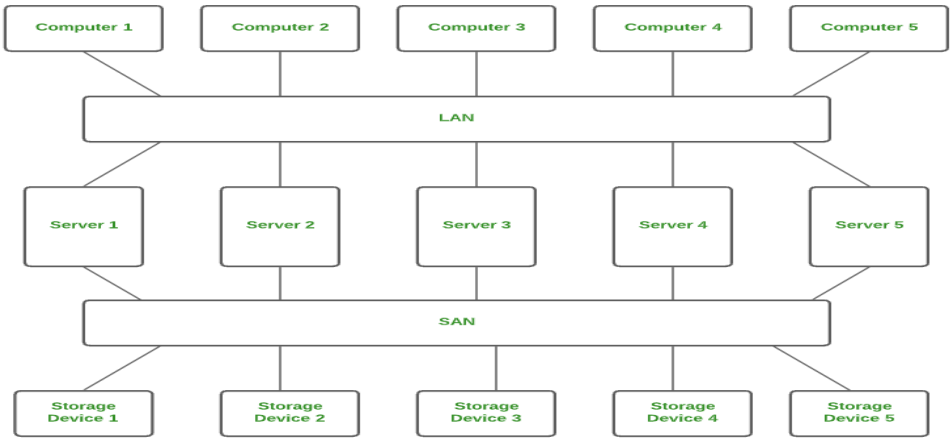
WLAN is a type of computer network that acts as a local area network but makes use of wireless network technology like Wi-Fi. This network doesn't allow devices to communicate over physical cables like in LAN but allows devices to communicate wirelessly.
The most common example of WLAN is Wi-Fi.



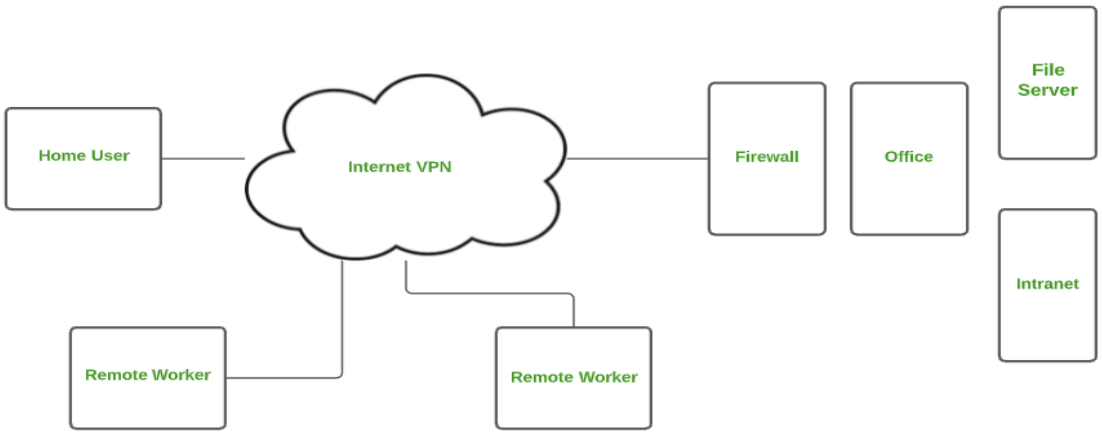
5. Metropolitan Area Network (MAN) :
A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town or metropolitan area.
Examples of MAN are networking in towns, cities, a single large city, large area within multiple buildings, etc.



6. Storage Area Network (SAN) :
SAN is a type of computer network that is high speed and connects groups of storage devices to several servers. This network does not depend on LAN or WAN.. Instead, a SAN moves the storage resources from the network to its own high-powered network. A SAN provides access to block-level data storage.
Examples of SAN are a network of disks accessed by a network of servers.



7.Virtual Private Network (VPN) :
A VPN is a type of computer network that extends a private network across the internet and lets the user send and receive data as if they were connected to a private network even though they are not. Through a virtual point-to-point connection users can access a private network remotely. VPN protects you from malicious sources by operating as a medium that gives you a protected network connection.



What are the Differences Between HTTP and FTP?

FTP-File Transfer Protocol
The term FTP is a short form for File Transfer Protocol. FTP is a type of internet standard that basically allows different devices (computers) to upload as well as download data files on the internet. The FTP sites consist of various types of files (images, video, texts, graphics, etc.).

HTTP- Hyper Text Transfer Protocol
The term HTTP is a short form for HyperText Transfer Protocol. HTTP is basically the backbone of the world wide web (WWW). It is basically an internet standard that assists in the process of transferring various web pages all over the internet.

Difference Between FTP and HTTP
Here is a list of the differences between FTP and HTTP.

Parameters	**FTP**	**HTTP**
Full-Form	The term FTP is a short form for File Transfer Protocol.	The term HTTP is a short form for HyperText Transfer Protocol.
Meaning	FTP refers to the set of rules that basically allows the process of uploading and downloading files from a computer to the internet.	HTTP refers to a set of rules that determines the process of transfer of various web pages over various computers present on the internet.
Support	It provides support for the control connection as well as the data connection.	It provides support for the connection of data.
Use of TCP	It makes use of the TCP. The FTP runs on port 20 and port 21 of TCP.	It also makes use of the TCP. The HTTP runs on port 80 of TCP.

Nature of URLs	The URLs that use the FTP protocol begin with FTP.	The URLs that use the HTTP protocol begin with HTTP.
Requirement of Authentication	It always requires authentication.	The HTTP requires no authentication.
Efficiency of File Transfer	It can easily transfer large files with chunks of data.	It is capable of efficiently transferring various small files.
Maintenance of States	This protocol is not stateless. Thus, it maintains the state.	This protocol is stateless in nature.
Uses	We use FTP for downloading as well as uploading files between a server and a client over the internet.	We use HTTP for providing various web pages from the web browser to the web server.

II UNIT

What is NIST Risk Management Framework(RMF)? Explain the process of risk management.

A Comprehensive, Flexible, Risk-Based Approach:

The NIST Risk Management Framework (RMF) provides a comprehensive, flexible, repeatable, and measurable 7-step process that any organization can use to manage information security and privacy risk for organizations and systems and links to a suite of NIST standards and guidelines to support implementation of risk management programs

The Risk Management Framework:

The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle.
The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.
Managing organizational risk is paramount to effective information security and privacy programs

The following are the steps in risk management process.

Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed

Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

.

2.Write about different security controls and guidance offered by NIST.

The NIST framework:

The NIST framework provides a number of different controls and guidance across multiple security and access control families defined under a baseline of impact. These baselines are separated by:

- **High impact**
- **Medium impact**
- **Low impact**

The controls are as follows:

- **AC (Access control):** Account management and monitoring, enforcing the policy of least privilege principle, and separation of duties.
- **AT (Awareness and training):** Providing awareness and security training to employees, and elevated technical training for more privileged users.
- **AU (Audit and accountability):** Auditing records and content, retaining records, and providing associated analysis and reporting
- **CA (Assessment, authorization and monitoring):** Penetration testing, and monitoring connections to public networks and external systems
- **CM (Configuration management):** Implementing configuration change controls, and setting authorized software policies
- **CP (Contingency planning):** Establishing and testing business continuity strategies, as well as alternate processing and storage sides.
- **IA (Identification and authentication):** Managing credentials and setting up authentication policies and systems in place for users, devices, and services.
- **IP (Individual participation):** Obtaining consent and authorizing privacy policies and practices.
- **IR (Incident response):** Setting up incident response training and setting up associated monitoring and reporting systems.
- **MA (Maintenance):** Having an ongoing system, personnel, and tool maintenance.
- **MP (Media protection):** Securing and protecting media access, use, storage, and transportation.
- **PA (Privacy authorization):** Setting policies for collecting, using, and sharing personally identifiable information(PII)
- **PE (Physical and environmental protection):** Ensuring access to emergency power, securing physical access, and protecting against physical risk and damage.
- **PM (Program management):** Having defined strategies for risk management, insider threats, and scaling architecture.
- **PL (Planning):** Having strategies in place for comprehensive security architecture (such as defense in depth and third-party vendor security)
- **PS (Personnel security):** Screening internal and external personnel, setting up termination and transfer security policies.

- **RA (Risk assessment):** Scanning vulnerabilities, having ongoing privacy impact, and risk assessments.
- **SA (System and services acquisition):** Implementing security across the system development lifecycle, new vendor contracts, and acquisitions.
- **SC (System and communications protection):** Partitioning applications, implementing cryptographic key management, and securing passwords and other sensitive data.
- **SI (System and information integrity):** Implementing system monitoring, alerting systems, and flaw remediation processes.

NIST Compliance

The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cybersecurity as the most reliable global certifying body.

NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness.

It promotes the resilience and protection of critical infrastructure by: Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs Determining the most important activities and critical operations - to focus on securing them Demonstrates the trust-worthiness of organizations who secure critical assets Helps to prioritize investments to maximize the cybersecurity ROI Addresses regulatory and contractual obligations Supports the wider information security program By combining the NIST CSF framework with ISO/IEC 27001 - cybersecurity risk management becomes simplified. It also makes communication easier

throughout the organization and across the supply chains via a common cybersecurity directive laid by NIST.

Final Thoughts As human dependence on technology intensifies, cyber laws in India and across the globe need constant up-gradation and refinements. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security. Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent.

Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyberland - can bring about online safety and resilience.

ROLE OF INTERNATIONAL LAWS

In various countries, areas of the computing and communication industries are regulated by governmental bodies There are specific rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes There are laws governing trade on the Internet, taxation, consumer protection, and advertising There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies Some states limit access to the Internet, by law as well as by technical means.

INTERNATIONAL LAW FOR CYBER CRIME

Cybercrime is "international" that there are ‘no cyber-borders between countries’ The complexity in types and forms of cybercrime increases the difficulty to fight back fighting cybercrime calls for international cooperation Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale

THE INDIAN CYBERSPACE

Indian cyberspace was born in 1975 with the establishment of National Informatics Centre (NIC) with an aim to provide govt with IT solutions. Three networks (NWs) were set up between 1986 and 1988 to connect various agencies of govt. These NWs were, INDONET which connected the IBM mainframe installations that made up India’s computer infrastructure, NICNET (the NIC NW) a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central govt with the state govts and district administrations, the third NW setup was ERNET (the Education and Research Network), to serve the academic and research communities.

New Internet Policy of 1998 paved the way for services from multiple Internet service providers (ISPs) and gave boost to the Internet user base grow from 1.4 million in 1999 to over 150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet

access through mobile phones and tablets. Govt is making a determined push to increase broadband penetration from its present level of about 6%1. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

NATIONAL CYBER SECURITY POLICY

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology. It aims at protecting the public and private infrastructure from cyberattacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

VISION

To build a secure and resilient cyberspace for citizens, business, and government and also to protect anyone from intervening in user's privacy.

MISSION

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, andcooperation.

OBJECTIVE

Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.

3 UNIT

1. Write the Features of OWSAP.(5M)

OWASP

The Open Web Application Security Project, or OWASP, is an international non-profit organization dedicated to web application security. OWASP is a free and open security community project that provides an absolute wealth of knowledge, tools to help anyone involved in the creation, development, testing, implementation and support of a web application to ensure that security is built from the start and that the end product is as secure as possible.

1.OWASP Tools

OWASP tools to help anyone involved in the creation, development, testing, implementation and support of a web application to ensure that security is built from the start and that the end product is as secure as possible.

2.Dedicated to Web application security

OWASP, is an international non-profit organization dedicated to web application security. It ensure that security is built from the start and that the end product is as secure as possible.

3.The OWASP Top 10 regularly-updated report

The OWASP Top 10 is a regularly-updated report outlining security concerns for web application security, focusing on the 10 most critical risks. The report is put together by a team of security experts from all over the world.

4.**Awareness document**

OWASP refers to the Top 10 as an 'awareness document' and they recommend that all companies incorporate the report into their processes in order to minimize and/or mitigate security risks.

5.Provide materials

The materials they offer include documentation, tools, videos, and forums.

6.Focusing on the 10 most critical risks.

Injection
Broken Authentication
Sensitive Data Exposure
XML External Entities (XEE)
Broken Access Control
Security Misconfiguration
Cross-Site Scripting

Insecure Deserialization.
Using Components With Known Vulnerabilities
Insufficient Logging And Monitoring

2.Why OWASP is important?(5M)

Importance of OWASP

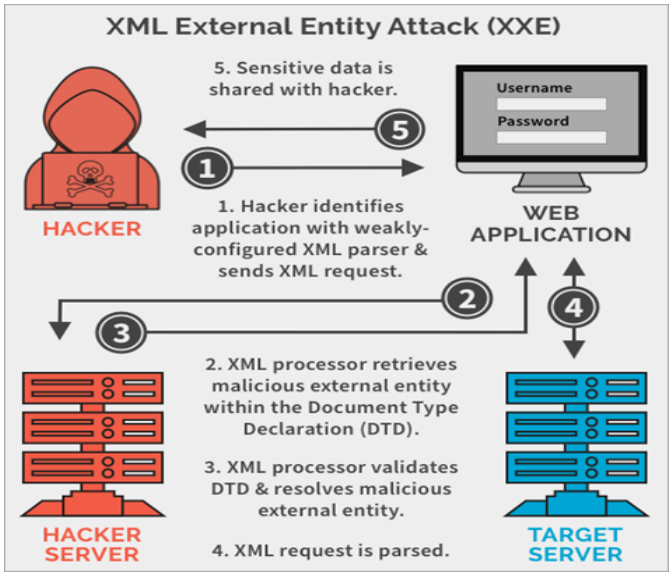
OWASP is a free and open security community project that provides an absolute wealth of knowledge, tools to help anyone involved in the creation, development, testing, implementation and support of a web application to ensure that security is built from the start and that the end product is as secure as possible.

Among the main benefits that OWASP provides to companies and IT professionals, we can highlight the
following:

- helps make applications more armored against cyber attacks;
- helps reduce the rate of errors and operational failures in systems;
- contributes to stronger encryption;
- increases the potential for application success;
- improves the image of the software developer company.

Showing customers that your company actively participates in the community by collaborating with the information will help change the way they see the business and will significantly improve the image of the business in the market.

10. Write about XML External Entities(XXE).(5M)
XML External Entities(XXE).
This is an attack against a web application that parses XML input. This input can reference an external entity, attempting to exploit a vulnerability in the parser. An 'external entity' in this context refers to a storage unit, such as a hard drive. An XML parser can be duped into sending data to an unauthorized external entity, which can pass sensitive data directly to an attacker.
Ways to prevent XEE attacks:-
The best ways to prevent XEE attacks are to have web applications accept a less complex type of data, such as JSON, or at the very least to patch XML parsers and disable the use of external entities in an XML application.
XML or Extensible Markup Language
XML or Extensible Markup Language is a markup language intended to be both human-readable and machine-readable. Due to its complexity and security vulnerabilities, it is now being phased out of use in many web applications.
JavaScript Object Notation (JSON)
JavaScript Object Notation (JSON) is a type of simple, human-readable notation often used to transmit data over the internet. Although it was originally created for JavaScript, JSON is language-agnostic and can be interpreted by many different programming languages.



https://www.softwaretestinghelp.com/owasp-top-10-security-vulnerabilities/

3(a).What is OWSAP? How does its Works.(10M)

OWASP- Open Web Application Security Project

The Open Web Application Security Project, or OWASP, is an international non-profit organization dedicated to web application security. One of OWASP's core principles is that all of their materials be freely available and easily accessible on their website, making it possible for anyone to improve their own web application security.

OWASP Top 10

The OWASP Top 10 is a regularly-updated report outlining security concerns for web application security, focusing on the 10 most critical risks. The report is put together by a team of security experts from all over the world. OWASP refers to the Top 10 as an 'awareness document' and they recommend that all companies incorporate the report into their processes in order to minimize and/or mitigate security risks.

Below are the security risks reported in the OWASP Top 10

1. Injection

Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application. For example, an attacker could enter SQL database code into a form that expects a plaintext username. If that form input is not properly secured, this would result in that SQL code being executed. This is known as an SQL injection attack.

Injection attacks can be prevented by validating and/or sanitizing user-submitted data.

2. Broken Authentication

Vulnerabilities in authentication (login) systems can give attackers access to user accounts and even the ability to compromise an entire system using an admin account. For example, an attacker can take a list containing thousands of known username/password combinations obtained during a data breach and use a script to try all those combinations on a login system to see if there are any that work.

Some strategies to mitigate authentication vulnerabilities are requiring two-factor authentication (2FA) as well as limiting or delaying repeated login attempts using rate limiting.

3. Sensitive Data Exposure

If web applications don't protect sensitive data such as financial information and passwords, attackers can gain access to that data and utilize it for nefarious purposes. One popular method for stealing sensitive information is using an on-path attack.

Data exposure risk can be minimized by encrypting all sensitive data as well as disabling the caching of any sensitive information. Additionally, web application developers should take care to ensure that they are not unnecessarily storing any sensitive data.

XML External Entities (XEE)

This is an attack against a web application that parses XML* input. This input can reference an external entity, attempting to exploit a vulnerability in the parser. An 'external entity' in this context refers to a storage unit, such as a hard drive. An XML parser can be duped into sending data to an unauthorized external entity, which can pass sensitive data directly to an attacker.

The best ways to prevent XEE attacks are to have web applications accept a less complex type of data, such as JSON(Java Script Object Notation), or at the very least to patch XML parsers and disable the use of external entities in an XML application.

XML or Extensible Markup Language is a markup language intended to be both human-readable and machine-readable. Due to its complexity and security vulnerabilities, it is now being phased out of use in many web applications.

5. Broken Access Control

Access control refers a system that controls access to information or functionality. Broken access controls allow attackers to bypass authorization and perform tasks as though they were privileged users such as administrators. For example a web application could allow a user to change which account they are logged in as simply by changing part of a url, without any other verification.

Access controls can be secured by ensuring that a web application uses authorization tokens* and sets tight controls on them.

6. Security Misconfiguration

Security misconfiguration is the most common vulnerability on the list, and is often the result of using default configurations or displaying excessively verbose errors. For instance, an application could show a user overly-descriptive errors which may reveal vulnerabilities in the application.

This can be mitigated by removing any unused features in the code and ensuring that error messages are more general.

7. Cross-Site Scripting

Cross-site scripting vulnerabilities occur when web applications allow users to add custom code into a url path or onto a website that will be seen by other users. This vulnerability can be exploited to run malicious JavaScript code on a victim's browser.

Mitigation strategies for cross-site scripting include escaping untrusted HTTP requests as well as validating and/or sanitizing user-generated content. Using modern web development frameworks like ReactJS and Ruby on Rails also provides some built-in cross-site scripting protection.

8. Insecure Deserialization

This threat targets the many web applications which frequently serialize and deserialize data. Serialization means taking objects from the application code and converting them into a format that can be used for another purpose, such as storing the data to disk or streaming it.

Deserialization is just the opposite: converting serialized data back into objects the application can use. An insecure deserialization exploit is the result of deserializing data from untrusted sources, and can result in serious consequences like DDoS (Distributed Denial of Service attacks) and remote code execution attacks.

While steps can be taken to try and catch attackers, such as monitoring deserialization and implementing type checks, the only sure way to protect against insecure deserialization attacks is to prohibit the deserialization of data from untrusted

9. Using Components With Known Vulnerabilities

Many modern web developers use components such as libraries and frameworks in their web applications. These components are pieces of software that help developers avoid redundant work and provide needed functionality; common example include front-end frameworks like React and smaller libraries that used to add share icons or a/b testing. Some attackers look for vulnerabilities in these components which they can then use to orchestrate attacks.

To minimize the risk of running components with known vulnerabilities, developers should remove unused components from their projects, as well as ensuring that they are receiving components from a trusted source and ensuring they are up to date.

10. Insufficient Logging And Monitoring

Many web applications are not taking enough steps to detect data breaches. The average discovery time for a breach is around 200 days after it has happened. This gives attackers a lot of time to cause damage before there is any response.

OWASP recommends that web developers should implement logging and monitoring as well as incident response plans to ensure that they are made aware of attacks on their applications.

(or)

(b).Write about any 5 types of OWSAP Vulnerabilities.(10M)

Write about the functions of web application firewall(WAF). (10M)

Web application firewall(WAF):

A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. A firewall is a digital security system that checks all incoming and outgoing traffic on a network according to a defined set of rules. A firewall keeps out unauthorized traffic and lets in only communications that are deemed safe, using a set of security rules that you or your network administrator set up.

Protects web applications from attacks

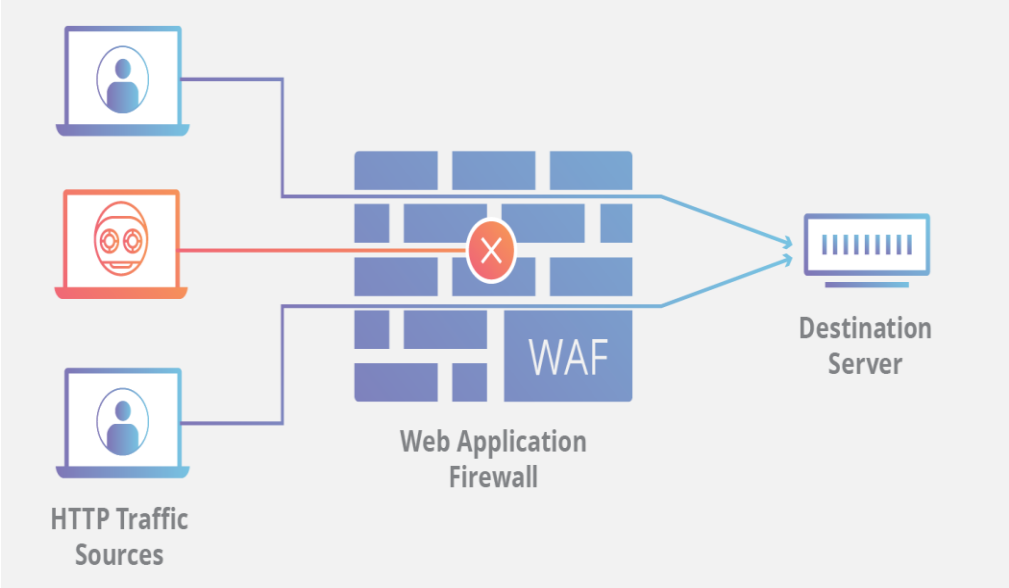
It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors.

A shield is placed between the web application and the Internet.

By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine's identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.

Operates through a set of rules

WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attacks and the rate limiting can be quickly implemented by modifying WAF policies.



Authorization method:

Web Application Firewalls are controlled by specific network administrators who are responsible for defining the firewall rules. Firewall network security is also the authorization method used in many remote access scenarios, such as remote working environments.

Filters data:

A firewall filters data entering your network. It analyzes that data by checking the sender's address, the application the data is meant for, and the contents of the data. By combining these defined data points, a firewall can tell what's harmful and what isn't. Then the firewall opens or closes the network gate accordingly.

Network-based, host-based, and cloud-based WAFs

A WAF can be implemented one of three different ways, each with its own benefits and shortcomings:

- **A network-based WAF:** A network-based WAF is generally hardware-based. Since they are installed locally they minimize delay, but network-based WAFs are the most expensive option and also require the storage and maintenance of physical equipment.
- **A host-based WAF:** A host-based WAF may be fully integrated into an application's software. This solution is less expensive than a network-based WAF and offers more customizability. The downside of a host-based WAF is the consumption of local server resources, implementation complexity, and maintenance costs. These components typically require engineering time, and may be costly.
- **Cloud-based WAFs:** Cloud-based WAFs offer an affordable option that is very easy to implement; they usually offer a turnkey installation that is as simple as a change in DNS to redirect traffic. Cloud-based WAFs also have a minimal upfront cost, as users pay monthly or annually for security as a service. Cloud-based WAFs can also offer a solution that is consistently updated to protect against the newest threats without any additional work or cost on the user's end.

What does a firewall do?(5M)

FIREWALL: A firewall is a digital security system that checks all incoming and outgoing traffic on a network according to a defined set of rules. A firewall keeps out unauthorized traffic and lets in only communications that are deemed safe, using a set of security rules that you or your network administrator set up.

Installed on every Mac and Windows computer:

Software firewalls come installed on every Mac and Windows computer. They can be installed as standalone software or bundled with other cyber security programs. Hardware firewalls are more specific to larger network devices, such as internet routers.

Protect company communications:

To protect company communications, businesses typically use a software firewall on all employee computers along with larger hardware firewalls to protect the entire network. That means that every data request has to go through at least two firewalls.

Authorization method:

Network firewalls are controlled by specific network administrators who are responsible for defining the firewall rules. Firewall network security is also the authorization method used in many remote access scenarios, such as remote working environments.

Filters data:

A firewall filters data entering your network. It analyzes that data by checking the sender's address, the application the data is meant for, and the contents of the data. By combining these

defined data points, a firewall can tell what's harmful and what isn't. Then the firewall opens or closes the network gate accordingly.

Check the traffic:

The primary purpose of a firewall is to check if traffic or an incoming connection meets a predefined set of security standards, which is critical for internet security. A good firewall tool can help you adjust the firewall's settings to your needs.

Discuss about different ways of implementation of Web Application Firewalls .(5M)

Web application firewall(WAF):

A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. A firewall is a digital security system that checks all incoming and outgoing traffic on a network according to a defined set of rules. A firewall keeps out unauthorized traffic and lets in only communications that are deemed safe, using a set of security rules that you or your network administrator set up.

Different ways of Implementation:

Network-based, host-based, and cloud-based WAFs

A WAF can be implemented one of three different ways, each with its own benefits and shortcomings:

- **A network-based WAF:** A network-based WAF is generally hardware-based. Since they are installed locally they minimize delay, but network-based WAFs are the most expensive option and also require the storage and maintenance of physical equipment.
- **A host-based WAF:** A host-based WAF may be fully integrated into an application's software. This solution is less expensive than a network-based WAF and offers more customizability. The downside of a host-based WAF is the consumption of local server resources, implementation complexity, and maintenance costs. These components typically require engineering time, and may be costly.
- **Cloud-based WAFs:** Cloud-based WAFs offer an affordable option that is very easy to implement; they usually offer a turnkey installation that is as simple as a change in DNS to redirect traffic. Cloud-based WAFs also have a minimal upfront cost, as users pay monthly or annually for security as a service. Cloud-based WAFs can also offer a solution that is consistently updated to protect against the newest threats without any additional work or cost on the user's end.

What is Broken authentication? Write the impact of broken authentication.

Broken authentication

Broken authentication is one of the OWASP Top 10 list. Broken authentication is typically caused by poorly implemented authentication and session management functions. Broken authentication attacks aim to take over one or more accounts giving the attacker the same privileges as the attacked user. Authentication is "broken" when attackers are able to compromise passwords, keys or session tokens, user account information, and other details to assume user identities.

Due to poor design and implementation of identity and access controls, the prevalence of broken authentication is widespread. Common risk factors include:

- Predictable login credentials
- User authentication credentials that are not protected when stored

- Session IDs exposed in the URL (e.g., URL rewriting)
- Session IDs vulnerable to session fixation attacks
- Session value that does not time out or get invalidated after logout
- Session IDs that are not rotated after successful login
- Passwords, session IDs, and other credentials sent over unencrypted connections

Impact of Broken Authentication and Session Management

If a hacker successfully logs in by stealing your credentials using any of the above mentioned broken authentication techniques, they can misuse your privileges and impact your company's sustainability.

Cybercriminals can have various intentions of hijacking your web application, such as:

- Stealing critical business data
- Identity theft
- Sending fraud calls or emails.
- Creating malicious software programs for disrupting networks.
- Cyber terrorism
- Cyber stalking
- Selling illegal items on the dark web
- Sharing fake news on social media

In short, hackers can use broken authentication attacks and session hijacking to gain access to the system by forging session data, such as cookies, and stealing login credentials.

Thus, it would be best if you never compromised with your web applications' security.

Broken Authentication Examples

Here are a few examples of broken authentication.

Example 1: Credential Stuffing

Suppose you run a departmental store and sell groceries. To grow your business rapidly, you implement a CRM system that stores critical customer data, such as name, phone number, username, and password.

Hackers make their way inside the CRM system and steal all the data. They then use the same credentials — usernames and passwords — to hack into the central bank's database.

In this case, hackers are trying to successfully log in to the central bank's database by hoping that a handful of consumers must be using the same credentials at both places. Such kinds of broken authentication attacks are called credential stuffing.

Example 2: Application session timeouts aren't set properly.

Suppose you go to a cyber cafe and login your Gmail account. After sending the email, you close the browser tab and return home.

Sometime later, the hacker opens your Gmail account and gains access to your crucial information. It happens because your credentials — username and password — haven't been invalidated adequately during logout.

Thus, if the application session timeouts aren't set properly, hackers can execute a broken authentication attack.

Explain the concept of Injection attack with examples and how can you protect from that attack?

Injection attack

An injection flaw is a vulnerability which allows an attacker to relay malicious code through an application to another system. This can include compromising both backend systems as well as other clients connected to the vulnerable application.

The effects of these attacks include:

- Allowing an attacker to execute operating system calls on a target machine
- Allowing an attacker to compromise backend data stores
- Allowing an attacker to compromise or hijack sessions of other users
- Allowing an attacker to force actions on behalf of other users or services

Many web applications depend on operating system features, external programs, and processing of data queries submitted by users. When a web application passes information from an HTTP request as part of an external request, set up a way to scrub and validate the message. Otherwise an attacker can inject special (meta) characters, malicious commands/code, or command modifiers into the message.

While these attacks are not difficult to attempt, there are an increasing number of tools that scan for these flaws. An attacker can use these techniques to obtain, corrupt, or destroy the contents of your database, compromise backend systems, or attack other users.

Successful injection attacks may completely compromise or destroy a system. It is important to test for and protect against these types of attacks.

Examples

1. **OS Command Injection -** A malicious parameter could modify the actions taken by a system call that normally retrieves the current user's file to access another user's file (e.g., by including path traversal ../ characters as part of a filename request). Additional commands could be tacked on to the end of a parameter that is passed to a shell script to execute an additional shell command (e.g., ; rm –r *) along with the intended command.
2. **SQL Injection -** Is a particularly widespread and dangerous form of injection. To exploit a SQL injection flaw, an attacker needs to find a parameter that the web application passes through to a database interaction. An attacker can then embed malicious SQL commands into the content of the parameter, to trick the web application to forward a malicious query to the database. SQL queries could be modified by adding additional 'constraints' to a where clause (e.g., OR 1=1) to gain access to or modify unauthorized data.
3. **Cross-Site Scripting (XSS) -** A type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.[1] Attacks of this type can hijack user sessions, log keystrokes, or perform malicious actions on behalf of victim users.

How to Protect Yourself

The best way to determine if your applications are vulnerable to injection attacks is to search the source code for all calls to external resources.

Additionally, validate that all user provided input is sanitized and user provided data that is output is properly encoded where applicable.

1. Validate Input
2. Apply Least Privilege

3. Handle Exceptions and Returned Status Codes
4. Investigate Mitigation Techniques for Specific Technologies Your Application Uses
5. Avoid Accessing External Interpreters.

What are the best practices to avoid Components with Known Vulnerabilities?

Best practices to avoid Components with Known Vulnerabilities:

Web applications typically rely on several open-source components, where attacks are mostly orchestrated using components with known vulnerabilities. To mitigate this, the Online Web Application Security Project (OWASP) helps organizations enhance their security posture through educational content, methodologies, conferences, and open-source software projects. The project is maintained by a community of volunteers who provide free and easily accessible material, making it easy for anyone to get involved in web application security.

Some best practices to keep applications secure against known vulnerability attacks include:

OWASP evaluation

Awareness is one of the best approaches to defend an application against known vulnerabilities. Threats are evaluated by OWASP on four criteria: **ease of exploitation, business impact, detectability, and prevalence.**

Enable Software Composition Analysis (SCA)

SCA is a collection of automated processes and tools that enable the codebase to identify open-source software. SCA involves inspecting source code, manifest files, container images, package managers, and more, compiling them into a Bill of Materials that is checked against various reliability databases.

Deploy Web Application Firewalls (WAFs)

WAF monitors and filters traffic enabling developers to protect web applications. Using WAFs, teams can block malicious traffic and prevent data exchange between the application and malicious actors. The firewall can further be configured with custom policies updated regularly to meet each web application's unique needs.

Develop Products using only the necessary features and permissions

Many development teams include open-source frameworks and components to increase the attractiveness or interactivity of their applications. Some of these include fancy features that the application doesn't need yet and require full permissions.

Formalize the patch management process

Organizations should set out a clearly defined patch management and versioning process to keep all components secure and informed by personnel. The security patches procedures should be defined according to the application's data needs.

Enforce Continuous Monitoring

Continuous **testing** and **monitoring** for vulnerabilities is an effective solution to mitigate known vulnerability attacks. Monitoring can be used to inspect the performance and validity of transactions through log and event monitors.

Crashtest Security suite

Crashtest Security's end-to-end vulnerability assessment platform can help organizations keep their web applications and APIs secure from attacks that exploit known vulnerabilities. The testing suite offers various tools to enable full-scale vulnerability scanning and is trusted by several software vendors and organizations globally to deploy safer web applications through vulnerability scanning and assessment.

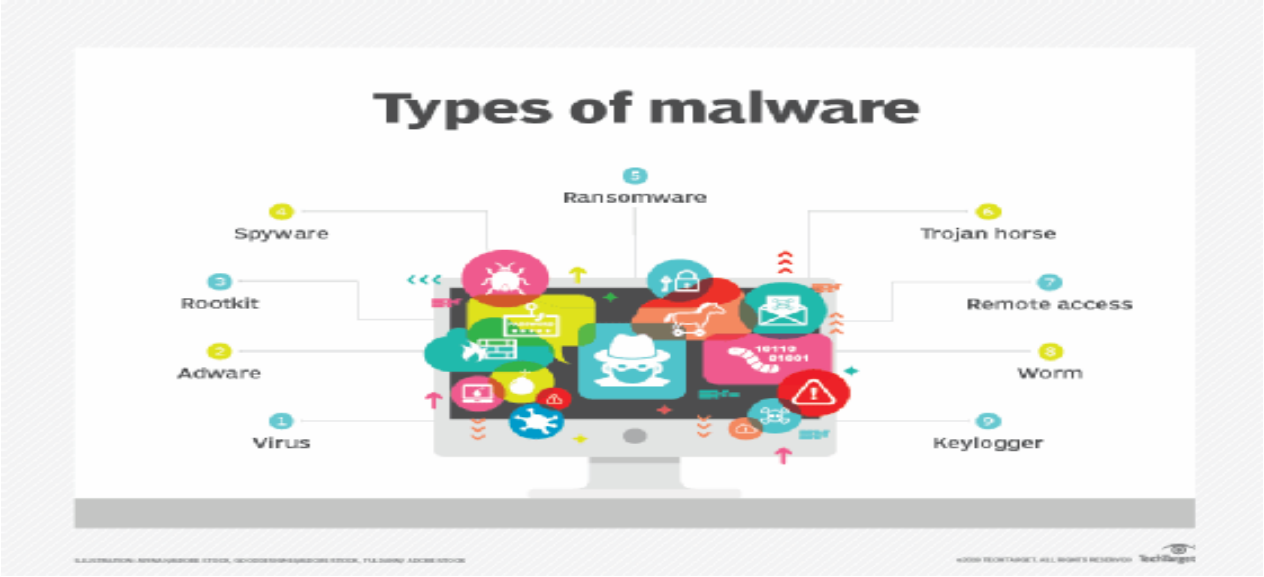
4thunit

4.a)What is Malware? Write about different types of Malwares.

Malware:

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions and monitor end users' computer activity.



Different types of malware have unique traits and characteristics. Types of malware include the following:

1. **A <u>virus</u>** is the most common type of malware that can execute itself and spread by infecting other programs or files.
2. **A <u>worm</u>** can self-replicate without a host program and typically spreads without any interaction from the malware authors.
3. **A <u>Trojan horse</u>** is designed to appear as a legitimate software program to gain access to a system. Once activated following installation, Trojans can execute their malicious functions.
4. **<u>Spyware</u> c**ollects information and data on the device and user, as well as observes the user's activity without their knowledge.
5. **Ransomware** infects a user's system and encrypts its data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
6. **A <u>rootkit</u>** obtains administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system.

7. **A backdoor virus** or remote access Trojan (RAT) secretly creates a backdoor into an infected computer system that enables threat actors to remotely access it without alerting the user or the system's security programs.
8. **Adware** tracks a user's browser and download history with the intent to display pop-up or banner advertisements that lure the user into making a purchase. For example, an advertiser might use cookies to track the web pages a user visits to better target advertising.
9. **Keyloggers**, also called system monitors, track nearly everything a user does on their computer. This includes emails, opened web pages, programs and keystrokes

b)How to detect and prevent malware infections?

Malware:

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions and monitor end users' computer activity.

How to detect malware

Users may be able to detect malware if they observe unusual activity such as a sudden loss of disk space, unusually slow speeds, repeated crashes or freezes, or an increase in unwanted internet activity and pop-up advertisements.

Antivirus and antimalware software may be installed on a device to detect and remove malware. These tools can provide real-time protection or detect and remove malware by executing routine system scans.

Prevention of malware infections

There are several ways users can prevent malware. In the case of protecting a personal computer, users can install antimalware software.

1.Users can prevent malware by practicing safe behavior on their computers or other personal devices. This includes not opening attachments from strange email addresses that may contain malware disguised as a legitimate attachment- such emails may even claim to be from legitimate companies but have unofficial email domains.

2.Users should update their antimalware software regularly, as hackers continually adapt and develop new techniques to breach security software. Security software vendors respond by releasing updates that patch those vulnerabilities. If users neglect to update their software, they may miss out on a patch that leaves them vulnerable to a preventable exploit.

3.In enterprise settings, networks are larger than home networks, and there is more at stake financially. There are proactive steps companies should take to enforce malware protection. Outward-facing precautions include the following:

- Implementing dual approval for business-to-business (B2B) transactions; and
- Implementing second-channel verification for business-to-consumer (B2C) transactions.

Business-facing, internal precautions include the following:

- Implementing offline malware and threat detection to catch malicious software before it spreads;
- Implementing allowlist security policies whenever possible; and

- Implementing strong web browser-level security.

Malwarebytes is an example of an antimalware tool that handles detection and removal of malware. It can remove malware from Windows, macOS, Android and iOS platforms. Malwarebytes can scan a user's registry files, running programs, hard drives and individual files. If detected, malware can then be quarantined and deleted. However, unlike some other tools, users cannot set automatic scanning schedules.

c)What is a Firewall? Explain its key uses.

Firewall

Firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer's entry point which only allows trusted sources, or IP addresses, to enter your network.

Working of Firewall

A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rules.

Key Uses of Firewalls

1. Firewalls can be used in corporate as well as consumer settings.
2. Firewalls can incorporate a security information and event management strategy (SIEM) into cyber security devices concerning modern organizations and are installed at the network perimeter of organizations to guard against external threats as well as insider threats.
3. Firewalls can perform logging and audit functions by identifying patterns and improving rules by updating them to defend the immediate threats.
4. Firewalls can be used for a home network, Digital Subscriber Line (DSL), or cable modem having static IP addresses. Firewalls can easily filter traffic and can signal the user about intrusions.
5. They are also used for antivirus applications.
6. When vendors discover new threats or patches, the firewalls update the rule sets to resolve the vendor issues.
7. In-home devices, we can set the restrictions using Hardware/firmware firewalls
8. It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.
9. Firewalls provide faster response time and can handle more traffic loads.
10. A firewall allows you to easily handle and update the security protocols from a single authorized device.
11. It safeguards your network from phishing attacks.

4.a)**Explain about 5 different types of Firewalls.**

What Is Firewall

Firewalls prevent unauthorized access to networks through software or firmware. By utilizing a set of rules, the firewall examines and blocks incoming and outgoing traffic.

Fencing your property protects your house and keeps trespassers at bay; similarly, firewalls are used to secure a computer network.

Types of Firewalls

A firewall can either be software or hardware. Software firewalls are programs installed on each computer, and they regulate network traffic through applications and port numbers. Meanwhile, hardware firewalls are the equipment established between the gateway and your network. Additionally, you call a firewall delivered by a cloud solution as a cloud firewall.

There are multiple types of firewalls based on their traffic filtering methods, structure, and functionality. A few of the types of firewalls are:

- **Packet Filtering**

A packet filtering firewall controls data flow to and from a network. It allows or blocks the data transfer based on the packet's source address, the destination address of the packet, the application protocols to transfer the data, and so on.

- **Proxy Service Firewall**

This type of firewall protects the network by filtering messages at the application layer. For a specific application, a proxy firewall serves as the gateway from one network to another.

- **Stateful Inspection**

Such a firewall permits or blocks network traffic based on state, port, and protocol. Here, it decides filtering based on administrator-defined rules and context.

- **Next-Generation Firewall**

According to Gartner, Inc.'s definition, the next-generation firewall is a deep-packet inspection firewall that adds application-level inspection, intrusion prevention, and information from outside the firewall to go beyond port/protocol inspection and blocking.

- **Threat-Focused NGFW**

These firewalls provide advanced threat detection and mitigation. With network and endpoint event correlation, they may detect evasive or suspicious behavior.

b)What is Trojan Horse? Explain types of Trojan malware.

Trojan Horse

A Trojan Horse (Trojan) is a type of malware that disguises itself as legitimate code or software. Once inside the network, attackers are able to carry out any action that a legitimate user could perform, such as exporting files, modifying data, deleting files or otherwise altering the contents of the device.

Trojans may be packaged in downloads for games, tools, apps or even software patches. Many Trojan attacks also leverage social engineering tactics, as well as spoofing and phishing, to prompt the desired action in the user.

Types of Trojan Malware

1. **Exploit Trojan:** As the name implies, these Trojans identify and exploit vulnerabilities within software applications in order to gain access to the system.

2. **Downloader Trojan:** This type of malware typically targets infected devices and installs a new version of a malicious program onto the device.
3. **Ransom Trojan:** Like general ransomware, this Trojan malware extorts users in order to restore an infected device and its contents.
4. **Backdoor Trojan:** The attacker uses the malware to set up access points to the network.
5. **Distributed Denial of Service (DDoS) attack Trojan:** Backdoor Trojans can be deployed to multiple devices in order to create a botnet, or zombie network, that can then be used to carry out a DDoS attack. In this type of attack, infected devices can access wireless routers, which can then be used to redirect traffic or flood a network.
6. **Fake AV Trojan:** Disguised as antivirus software, this Trojan is actually ransomware that requires users to pay fees to detect or remove threats. Like the software itself, the issues this program claims to have found are usually fake.
7. **Rootkit Trojan:** This program attempts to hide or obscure an object on the infected computer or device in order to extend the amount of time the program can run undetected on an infected system.
8. **SMS Trojan:** A mobile device attack, this Trojan malware can send and intercept text messages. It can also be used to generate revenue by sending SMS messages to premium-rate numbers.
9. **Banking Trojan or Trojan Banker:** This type of Trojan specifically targets financial accounts. It is designed to steal data related to bank accounts, credit or debit cards or other electronic payment platforms.
10. **Trojan Game Thief:** This program specifically targets online gamers and attempts to access their gaming account credentials.

c) **Explain the Use of Process explorer and process monitor in malware analysis.**

1.Process explorer :

one of the most famous tools it gained was Process Explorer. For Windows operating systems (OS), especially those up to and including Windows 7, Process Explorer is an excellent replacement for Task Manager.

C**learer view**

It offers a much clearer view of what is going on and has a lot more options. Besides the options the regular Task Manager has to offer, there are a few extra ones that are particularly interesting when you suspect your machine to be infected.

The tools in Process Explorer

The tools in Process Explorer offer targeted help such as Fast Search to locate a file quickly or the Kill Process option to shut down a complete process tree with one click. Hitting the space bar pauses the automatic updates so IT can monitor a process closely before it disappears. IT can easily locate files that get locked or lost in the sea of processes in the handle view.

VirusTotal to monitor potential malware

Process Explorer also uses VirusTotal to monitor potential malware from questionable processes. IT can add the VirusTotal column in options, and the column will show all the antivirus sites that flagged a process as a potential virus.

check your running processes

VirusTotal is an online malware repository that allows the general public to analyze files (and URLs) and check if they are found to be malicious by contributing vendors. This is relevant because Process Explorer allows you to check your running processes and loaded DLLs on VirusTotal.

2.Process monitor :

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.

If wanted to know what a process is accessing in terms of files and registry keys and so forth, we need a tool that can monitor those activities. Enter "Process Monitor".

Monitors and captures File system activity

Process monitor is a tool that monitors and captures File system activity, registry activity, network activity, profiling events and processes and threads activity on a particular system by using a kernel driver.

Tool for troubleshooting

It's a powerful tool for troubleshooting and understanding what a process is doing behind the scene and at a lower level and so powerful

Adds an extensive list of enhancements

Adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more.

Unique utility in malware hunting

It is a unique utility for system troubleshooting and malware hunting.

5 Marks

11.a)What are the Objectives of Malware?

Malware:

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware.

Objectives of Malware

1.Malware can infect networks and devices and is designed to harm those devices, networks and/or their users in some way.

2.Depending on the type of malware and its goal, this harm may present itself differently to the user or endpoint. In some cases, the effect malware has is relatively mild and benign, and in others, it can be disastrous.

3.These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions and monitor end users' computer activity.

4. All types of malware are designed to exploit devices at the expense of the user and to the benefit of the hacker who is the person who has designed and/or deployed the malware.

5. Malware that infects devices and networks. For example, malicious programs can be delivered to a system with a USB drive, through popular collaboration tools and by drive-by downloads, which automatically download malicious programs to systems without the user's approval or knowledge.

6.Hackers continually adapt and develop new techniques to breach security software through malwares and steal sensitive data.
7.Provide remote control for an attacker to use an infected machine.
8.Send spam from the infected machine to unsuspecting targets.
9.Investigate the infected user's local network.

b)Explain working of firewall.

Firewall

Firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer's entry point which only allows trusted sources, or IP addresses, to enter your network.

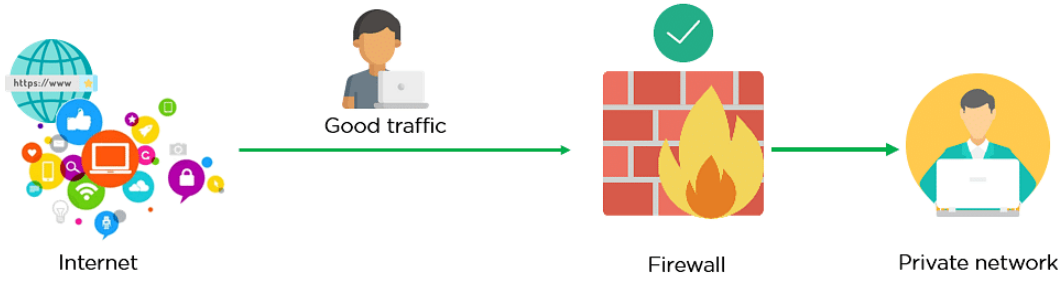
Working of Firewall

A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rules.

These rules are based on several aspects indicated by the packet data, like their source, destination, content, and so on. They block traffic coming from suspicious sources to prevent cyber attacks.

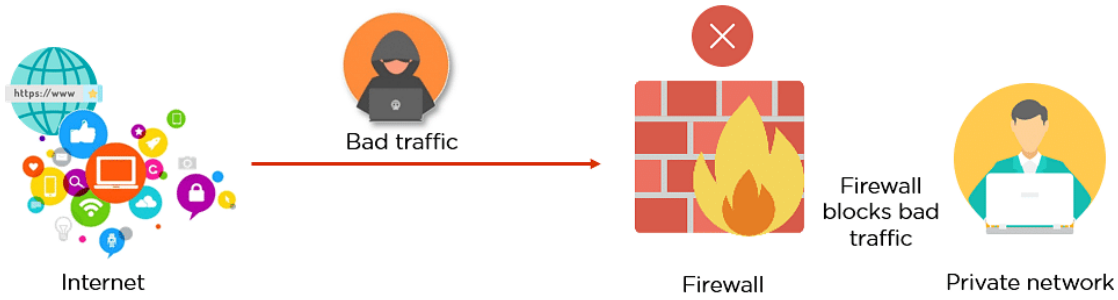
For example, the image depicted below shows how a firewall allows good traffic to pass to the user's private network.

Fig: Firewall allowing Good Traffic



However, in the example below, the firewall blocks malicious traffic from entering the private network, thereby protecting the user's network from being susceptible to a cyberattack.

Fig: Firewall blocking Bad Traffic



c) Discuss about malware responsive plan.

Malware responsive plan: Every organization should create a malware response plan to indentify the vulnerabilities of malware attack and they should plan how to block and how to recover the affected data.

The steps involved in an organization's malware response plan.

12.a) Write the advantages of antivirus software.

Antivirus software. The program protects the computer from viruses, malware, spyware, and other unknown threats and eliminating them before these malicious programs can harm the device's system. An effective antivirus would have developed a list of good and bad files to help distinguish a program as to whether it is harmful or not.

1. Protection from viruses

This is the primary function of an antivirus program. An effective antivirus would have developed a list of good and bad files to help distinguish a program as to whether it is harmful or not.

2. Prevention of phishing attacks

What is antivirus going to do to protect a computer? One of the answers would be that it protects computers from phishing attacks. These attacks are comprised of unauthorized attempts by a third person to access a computer's data to steal or infect it and render it unusable to the owner.

3. Scanning removable devices

An antivirus is capable of quickly scanning any removable device connected to the computer to identify potential threats. It allows the program to run for the computer owner to use, but it prevents the program from accessing the computer's data and other resources.

4. Protection against online threats

With continuous access to the Internet, computer owners have to fight off numerous cyber threats. But a good antivirus can block them from accessing the computer.

5. Firewall protection

What is antivirus good for? It monitors data going in and out of the network system through the Internet, monitors suspicious data, and blocks suspicious data from getting transmitted.

6. Blocking spam sites and ads

Most of the spam ads and viruses infect computers through pop-up ads and other spam sites. These spam attacks aim to steal information from a user's computer, compromising their privacy, or even causing substantial financial losses.

7. Faster computer

One can look for an antivirus program that can perform its job without slowing a computer down. It deletes unwanted folders and files from the computer, improving its performance speed.

8. Protection from identity theft

Spyware attacks are designed to steal personal information from the computer. These can include banking data, social security numbers, passwords, credit card numbers, and other important data.

9. Convenience

It is more convenient to simply run the antivirus than having to waste time trying to locate it, delete it, and restore any data that it has damaged.

b)What is VM ware and how to use VM ware security?

VM ware

Virtualization is a skill that is expected from nearly every employee in the IT industry. To do this, one must know how to use VMware for testing software.

Currently, the cyber security market is fragmented with thousands of vendors contributing to individual components. This is an environment that's ripe for cybercriminals to invade and exploit your system.

More people are working remotely than ever before. IT departments are straining to find the most secure way to integrate systems, share resources, and reduce costs.

VMware may be the solution to those problems. It is a central part of many IT infrastructures. Knowing how to use VMware can improve your company's efficiency and save money.

How to Use VMware Security

1.Companies need stronger security than ever before. More branch offices and remote workers mean more places to breach your IT network.

2.Every company's requirements are different, so make sure your security software service is specific to your needs and not a generic one-size-fits-all.

3.Unify and integrate security into your entire infrastructure from the cloud to the application to the device with VMware.

4.VMware is able to protect every application whether it lives on the cloud or a physical device. Make VMware Your Virtualization Solution

5.Virtualization is a flexible way to increase your hardware capacity and efficiency. It allows you to use the software in a safer, more cost-effective manner.

6.VMware is the most effective virtualization software system on the market.

c) Write about Sand box technology.

Sand box technology:

A sandbox is a system for malware detection that runs a suspicious object in a virtual machine (VM) with a fully-featured OS and detects the object's malicious activity by analyzing its behavior. If the object performs malicious actions in a VM, the sandbox detects it as malware. VMs are isolated from the real business infrastructure.

At the same time, compared to other behavior analysis designs, a sandbox is safer as it doesn't risk running a suspicious object in the real business infrastructure.

Malware detection workflow:

The sandbox receives a request to scan an object (a file or a URL) from another security solution component, with instructions

the OS and the configuration for running the object, the object's execution parameters, other third-party applications installed in the VM, the test time limit, etc.

The tested object is run.

The sandbox collects artifacts throughout the specified time span. If the object interacts with other processes or URLs with known reputations, the sandbox captures this.

The sandbox analyzes artifacts and delivers its verdict to the requesting system

The sandbox adds the object's data to the verdict (ID, features, logs, behavior details), which may help in further analysis without the need for a new request to the sandbox.

If a certain suspicious activity is found during the sample's execution, sandbox also returns detailed description of the activity.

13.a) What are the 5 types of Cyber Security?

b) Discuss about reasons for increasing Cyber attacks in India.

c) Explain the concept of Cyber terrorism.

5.a) Define Cyber Crime? Explain the Legal Perspectives of Cyber Crimes.

a) What are the main categories of Cyber Crime according to Law?

a) Discuss about different types of Cyber Security.

(OR)

b) Discuss about Cyber Crime and Punishments according to Indian IT Act 2000.

b) Explain the Cyber Security Challenges in India.

b) Explain the importance of Cyber Laws

13.a)Define Cyber Crime? Explain the Legal Perspectives of Cyber Crimes.

Cyber: Cyber space includes computers, networks, softwares, data storage devices(such as hard disks, USB disks etc), the internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Cyber Crime:

Any crime with the help of computer and telecommunication technology.

Cybercrime, also called computer crime, **the use of a computer as an instrument to further illegal ends**, such as committing fraud, trafficking intellectual property, stealing identities, or violating privacy.

Techno-savvy environment

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.

Cyber crime and the legal landscape around the world

The computer-generated world of internet is known as cyberspace and the laws prevailing this area are known as Cyber laws and all the users of this space come under the ambit of these laws as it carries a kind of worldwide jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet.

The growth of Electronic Commerce

The growth of Electronic Commerce require effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce. All these governing mechanisms and legal structures come within the domain of Cyber law.

Cyber Laws In India

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

Cyber laws: Information Technology Act 2000- National Cyber Security Policy 2013

Cyber law is important because it touches almost all aspects of transactions and activities and on involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal angles.

Cyber Crime is not defined in Information Technology Act 2000
National Cyber Security Policy 2013
The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cybercrime.

Cyber law encompasses laws relating to:

· Cyber crimes
· Electronic and digital signatures
· Intellectual property
· Data protection and privacy

b) What are the main categories of Cyber Crimes according to Cyber Law?

Cyber Crime:

Any crime with the help of computer and telecommunication technology.
Cybercrime, also called computer crime, **the use of a computer as an instrument to further illegal ends**, such as committing fraud, trafficking intellectual property, stealing identities, or violating privacy.

Cyber Laws In India

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

Cyber laws: Information Technology Act 2000- National Cyber Security Policy 2013

Cyber law is important because it touches almost all aspects of transactions and activities and on involving the internet, World Wide Web and cyberspace.

Major Categories of Cyber Crime: There are three basic categories they are

1.Cybercrimes against persons
2. Cybercrimes against property
3. Cybercrimes against government

1. Against Persons:

Cyber stalking
Impersonation
Loss of Privacy
Transmission of Obscene Material
Harassment with the use of computer

2. Against Property

Unauthorized Computer Trespassing
Computer vandalism
Transmission of harmful programmes
Siphoning of funds from financial institutions

Stealing secret information & data
Copyright

3. Against Government
Hacking of Government websites
Cyber Extortion
Cyber Terrorism
Computer Viruses

Some Other Crimes
Logic Bombs
Spamming
Virus, worms, Trojan Horse
E-Mail Bombing
E-Mail abuse etc.

c)Discuss about different types of Cyber Security.

Cyber security

Cyber security refers to every aspect of protecting an organization and its employees and assets against cyber threats. As cyber attacks become more common and sophisticated and corporate networks grow more complex, a variety of cyber security solutions are required to mitigate corporate cyber risk.

The Different Types of Cybersecurity

Cyber security is a wide field covering several disciplines. It can be divided into seven main pillars:

1. Network Security

Most attacks occur over the network, and network security solutions are designed to identify and block these attacks. These solutions include data and access controls such as Data Loss Prevention (DLP), IAM (Identity Access Management), NAC (Network Access Control), and NGFW (Next-Generation Firewall) application controls to enforce safe web use policies.

Advanced and multi-layered network threat prevention technologies include IPS (Intrusion Prevention System), NGAV (Next-Gen Antivirus), Sandboxing etc.

2. Cloud Security

1. As organizations increasingly adopt cloud computing, securing the cloud becomes a major priority. A cloud security strategy includes cyber security solutions, controls, policies, and services that help to protect an organization's entire cloud deployment (applications, data, infrastructure, etc.) against attack.

3. Endpoint Security

The zero-trust security model prescribes creating micro-segments around data wherever it may be. One way to do that with a mobile workforce is using endpoint security. With endpoint security, companies can secure end-user devices such as desktops and laptops with data and network security controls, advanced threat prevention such as anti-phishing and anti-ransomware, and technologies that provide forensics such as endpoint detection and response (EDR) solutions.

4. Mobile Security

Often overlooked, mobile devices such as tablets and smartphones have access to corporate data, exposing businesses to threats from malicious apps, zero-day, phishing, and IM (Instant Messaging) attacks. Mobile security prevents these attacks and secures the operating systems and devices from rooting and jail breaking. When included with an MDM (Mobile Device Management) solution, this enables enterprises to ensure only compliant mobile devices have access to corporate assets.

5. IoT Security

While using Internet of Things (IoT) devices certainly delivers productivity benefits, it also exposes organizations to new cyber threats. IoT security protects these devices with discovery and classification of the connected devices, auto-segmentation to control network activities, and using IPS as a virtual patch to prevent exploits against vulnerable IoT devices. In some cases, the firmware of the device can also be augmented with small agents to prevent exploits and runtime attacks.

6. Application Security

Web applications, like anything else directly connected to the Internet, are targets for threat actors. Since 2007, OWASP has tracked the top 10 threats to critical web application security flaws such as injection, broken authentication, misconfiguration, and cross-site scripting to name a few.

7. Zero Trust

The traditional security model is perimeter-focused, building walls around an organization's valuable assets like a castle. However, this approach has several issues, such as the potential for insider threats and the rapid dissolution of the network perimeter. As corporate assets move off-premises as part of cloud adoption and remote work, a new approach to security is needed.

2. (OR)

b) Discuss about Cyber Crime and Punishments according to Indian IT Act 2000.

Cyber Laws In India

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

Need For Cyber Law

Cyber offences

Cyber offences are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. Cyber crime usually includes:
Unauthorized access of the computers
Virus/worms attack
Theft of computer system
Denial of attacks
Logic bombs
Trojan attacks
Internet time theft
Web jacking
Email bombing

Offences & Penalties under the Information Technology Act, 2000

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offence or contravention committed outside India

Cybercrime laws are laws that create the offences and penalties for cybercrimes.
Section 66B of the IT Act and Section 411 of IPC deal with the offense of dishonestly receiving stolen computer resources or devices.
Section 66C of the IT Act prescribes punishment for identity theft and states that any person who uses the identity credentials of a person for fraud or in a dishonest manner is liable for **Section 66D** punishment with imprisonment up to 3 years and a fine up to Rupees 3 lacs.

Cheating by personation using a computer resource is punishable under **Section 66D** of the IT Act.

IPC under Section 419, 463, 465, and 468 Similar provisions for these offenses are given under IPC under Section 419, 463, 465, and 468.

The existing laws of India, even with the most compassionate and liberal interpretation could not be interpreted in the light of the emergency cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgement found that it shall not be without major threats and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence, the need for enactment of relevant cyber laws.
None of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email id not “legal” in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for

Cyber law.

Importance of Cyber Laws

We are living in highly digitalized world.

All companies depend upon their computer networks and keep their valuable data in electronic form.

Government forms including income tax returns, company law forms etc are now filled in electronic form.

Consumers are increasingly using credit cards for shopping.

Most people are using email, cell phones and SMS messages for communication.

Even in "non-cyber crime" cases, important evidence is found in computers/ cell phones e.g. in cases of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.

Since it touches all the aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace therefore Cyber law is extremely important.[4]

Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even Dos or DDos) are all technologies and per se not crimes, but falling into the wrong hands with an illicit intent who are out to exploit them or misuse them, they come into the array of cyber-crime and become punishable offences.

Hence, it should be the tenacious efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes. It should be the duty of the three stake holders viz. i) the rulers, regulators, law makers and agents ii) Internet or Network Service Suppliers or banks and other intercessors and iii) the users to take care of information security playing their respective role within the permitted limitations and ensuring obedience with the law of the land.

Written By:- Vinit Verma - K.R. Mangalam University

Cybercrime law includes laws related to computer crimes, internet crimes, information crimes, communications crimes, and technology crimes. While the internet and the digital economy represent a significant opportunity, they're also an enabler for criminal activity. Cybercrime laws are laws that create the offences and penalties for cybercrimes.

Cybercrime describes:

crimes directed at computers, data or information communications technologies (ICTs), and

crimes committed by people using computers or ICT.

Cybercrime is a global problem, which requires a coordinated international response. We help organisations comply with the regulatory requirements that come out of cyber laws.

International cybercrime conventions

African Union Convention on Cyberspace Security and Personal Data Protection

Council of Europe Convention on Cybercrime (also known as the Budapest Convention on Cybercrime)

Model cybercrime law

CW Model Law – Model Law on Computer and Computer-related Crime

SADC Model Law – SADC Model Law on Computer Crime and Cybercrime

HIPCAR – Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbeans (Cybercrime/e-Crimes)
ITU – International Telecommunications Union Cybercrime Legislation Resources – ITU Toolkit for Cybercrime Legislation

India has two laws that recognise the importance of cybersecurity:

The Information Technology Act, 2000, and
specific rules, like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Offences & Penalties under the Information Technology Act, 2000

The introduction of the internet has brought the tremendous changes in our lives. People of all fields are increasingly using the computers to create, transmit and store information in the electronic form instead of the traditional papers, documents. Information stored in electronic forms has many advantages, it is cheaper, easier to store, easier to retrieve and for speedier to connection. Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian Parliament passed the law --- Information Technology Act 2000. The IT Act 2000 has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The increase rate of technology in computers has led to enactment of Information Technology Act 2000. The converting of the paper work into electronic records, the storage of the electronic data, has led tremendous changed the scenario of the country. The Act further amends the Indian Penal Code, 1860, The Evidence Act, 1872, The Banker's Book's Evidence Act, 1891 and The Reserve Bank of India Act, 1934.

Offences:

Cyber offences are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. Cyber crime usually includes:
(a) Unauthorized access of the computers
(b) Data diddling
(c) Virus/worms attack
(d) Theft of computer system
) Denial of attacks
(g) Logic bombs
(h) Trojan attacks
(i) Internet time theft
(j) Web jacking
(k) Email bombing
(l) Salami attacks
(m) Physically damaging computer system.

The offences included in the IT Act 2000 are as follows:

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offence or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.

Section 66F covers a crucial matter which is cyber terrorism and prescribes punishment for the same. It provides the acts which constitute cyber terrorism

ages and disadvantages. Little did the founding fathers know that their creation will be used someday to harm and destroy someone. Today, various dangerous things are happening in cyberspace. Using the web with criminal intent is known as cybercrime. The term “cybercrime” is not defined under any statute in India. But in the wider sense, it could mean, any activity done with criminal intent in cyberspace, where the computer could be a tool as well as the victim. Sometimes, these crimes are committed for generating profits, sometimes it is done to damage software and at other times it is done to ship malware into a system that enters other machines and spreads to the whole network in no time. Cybercrime could involve traditional criminal activities like theft, fraud, mischief, forgery, or defamation which are subject to the Indian Penal Code, 1860; and the new age crimes are subject to the Information Technology Act, 2000.

Cybercrimes can be divided into two categories broadly;

1.Where the computer is used as a weapon. Such crimes are- cyber terrorism, credit card fraud, IPR violations, pornography

2.Where the computer is the target. Such crimes include the use of one computer to damage another one like launching virus, hacking, DOS attacks

There are various types of cybercrimes which are divided into mainly 3 headings based on their target-

1.Cybercrimes against person such as pornography, defamation, harassment via mail, email bombing, cyberstalking, cyber extortion, etc. These are the most important cybercrimes known today and are capable of causing potential harm to humanity.

2.Cybercrimes against property such as cyber vandalism, data theft, transmitting the virus, unauthorized computer trespassing, IPR infringement, credit card frauds, etc

3.Cybercrimes against the government are like cyber terrorism. Cyberspace is misused by

individuals and certain groups to threaten international governments and their citizens by cracking the official governmental or military websites.

Significant Cyber Crimes:-

Cyber extortion- This crime involves an attack or a threat to attack to demand extortion money. One such type is a ransomware attack. Cybercriminals hack into the network of an organization and make any potential data or documents inaccessible until a ransom is paid.

Identity theft- This crime constitutes an attack where an individual trespasses into a computer to extract the personal information of the user like banking details, credit card number, identity card number, personal health details, etc. Such information is bought and sold on the dark web for profits and is often used to commit frauds and making unauthorized transactions.

Cyber espionage- Under this crime, individuals or groups hacks into the system and gather confidential information from the government or any organization. It constitutes every type of attack from destroying the data to modifying it or using system-connected devices like a webcam to spy on an individual or monitoring the email, messages, and other connections.

Software piracy- This is one of the most common cybercrimes today which involves unauthorized use, unlawful copying, or distribution of such copy. This is often done for personal or commercial gain. IPR infringement, counterfeiting, internet piracy are some of its examples.

Exit scam- The digital version of this old scam involves the transfer of virtual currency held in marketplace escrow accounts to the accounts of dark web administrators.

DDoS (Distributed Denial of Service) attacks- This type of attack is performed by using the organization’s protocol and taking advantage of its limits to shut down the server by overwhelming its capacity to respond to communications. These attacks are generally carried out for malicious purposes or committing mischief and sometimes to divert the attention of the targeted network from another attack.

Phishing attacks- This is the technique for acquiring sensitive information like login details, passwords, credit card details, company data, etc. of a user by sending fraudulent messages (mostly emails) that appear to be coming from a trustworthy and reputable source.

Cyber Laws in India:-

"Every action and reaction occurring in the cyberspace has some legal and cyber legal perspectives". The term "cyberlaw" is used to address the legal issues occurring in cyberspace. It is an integration of various laws to deal with and resolve such issues and challenges posed by humanity on the web every day.

As cybercrime is a field still developing towards specialization, there is absolutely no comprehensive law to deal with it, anywhere in the world till date. But Government of India has the Information Technology Act, 2000 in force to regulate the malicious activities on the web that violate the rights of an internet user. At times, one may find that there are provisions of the IPC and IT Act that penalize such activities overlap each other.

Penalties under Cyber Crimes:-

Section 43 and 66 of the IT Act punishes a person committing data theft, transmitting virus into a system, hacking, destroying data, or denying access to the network to an authorized person with maximum imprisonment up to 3 years or a fine of rupees 5 lacs or both. At the same time data theft is also punishable under Section 378 and Section 424 of IPC with maximum imprisonment of 3 years or fine or both; and imprisonment of 2 years or fine or both respectively. Denying access to an authorized person or damaging a computer system is penalized under Section 426 of IPC with imprisonment of up to 3 months or fine or both.

Tampering with computer source documents is a punishable offence under Section 65 of the IT Act. Section 66E provides the punishment for violation of privacy. It states that if any person captures, publishes, or distributes an image of a private area of a person without his/her consent has committed a breach of privacy and is punishable with imprisonment up to 3 years or a fine up to 2 lacs or both.

Section 66F covers a crucial matter which is cyber terrorism and prescribes punishment for the same. It provides the acts which constitute cyber terrorism like denial of access or penetrating through a network or transmitting virus/malware utilizing which he is likely to cause death or injury to any person, which is all done with the purpose to threat the integrity, sovereignty, unity, and security of India or create terror in the minds of its citizen.

Apart from the provisions for punishment, the IT Act also empowers the Central Government to issue directions to block access of any information on an intermediary or computer resource for the public, if it feels necessary in the interest of the State. It can also intercept, decrypt or monitor such information.

Cyber security-types

Cybersecurity challenges in India are as follows:

With India carving a niche for itself in the IT sector, dependence on technology is also increasing. However, there are two things that set India aside from the players in the big leagues, like the United States and China, and that is design and density. With Indians using the internet for all their needs, ranging from shopping to banking, studying to storing data, cyber crimes have also increased in proportion to usage.

Some of the Cybersecurity challenges in India are as follows:

1. Lack of uniformity in devices used for internet access – With varying income groups in India, not everyone can afford expensive phones. In the US, Apple has over 44% market share. However, in India the iPhones with their higher security norms are used by less than 1% of mobile users. The widening gap between the security offered by the high-end iPhone and lower cost mobiles make it almost impossible for legal and technical standards to be set for data protection by the regulators.

2. Lack of national level architecture for Cybersecurity – Critical infrastructure is owned by private sector, and the armed forces have their own firefighting agencies. However there is no national security architecture that unifies the efforts of all these agencies to be able to assess the nature of any threat and tackle them effectively. The Prime Minister's Office has created a position towards this cause but there is a long way to go before India has the necessary structure in place.

3. Lack of separation – Unlike countries or states, in cyberspace there are no boundaries, thus making the armed forces, digital assets of ONGC, banking functions, etc. vulnerable to cyber attacks from anywhere. This could result in security breaches at a national level, causing loss of money, property or lives. To respond to possible threats on the country's most precious resources, there is a need for a technically equipped multi-agency organization that can base its decisions on policy inputs and a sound strategy.

4. Lack of awareness – As there is no National regulatory policy in place for cybersecurity there is a lack of awareness at both company level as well as individual level. Domestic netizens can protect and be protected from the cyber attacks only if there is a guided and supervised legal framework.

Both cybercrime and cybercriminals have developed at a rapid pace, while the law has progressed at best at a snail's pace, and even that is usually only a knee-jerk reaction. Technology, particularly the Internet, has created a seamless, borderless platform for use, abuse, and misuse, with few laws or enforcement mechanisms to prevent, protect, cure, or punish such transgressions.

Cybersecurity is the use of technology, processes, and policies to prevent cyberattacks on systems, networks, programs, devices, and data. Its goal is to limit the risk of cyberattacks and protect systems, networks, and technologies from

unauthorized use.[i] Cybersecurity measures, also known as information technology security (IT), prevent threats to networked systems and applications, whether they come from outside or inside a company or organization.

Cyber Security Challenges:

Cybercrime:

According to Joseph Aghatise,[ii] cybercrime is a crime committed on the Internet using a computer either as a tool or as a targeted victim. It is very difficult to categorize crimes into different groups because many crimes evolve daily. Even in the real world, crimes such as rape, murder, or theft do not necessarily need to be separated. However, in all cybercrimes, both the computer and the person behind it are victims; it just depends on which of the two is the main target. Therefore, the computer can be a target or a tool for simplicity. Hacking, for example, involves attacking the computer's information and other resources. It is important to note that in many cases, there is overlap, and it is impossible to have a perfect classification system.[iii]

Verizon's[iv] 2016 annual report, titled "Data Breach Investigations Report," lists industry-related incidents and security breaches. According to the report, "89 percent of data breaches had a financial or espionage-related purpose."[v] When individuals suffer harm, the impact is felt the most, especially when the hard road of international enforcement is taken. The vastness of cyberspace makes enforcement even more difficult.

According to a report by the Ministry of Electronics and Information Technology (MeitY) submitted to a parliamentary subcommittee, cybercrime and fraud cases increased more than fivefold between 2018 and 2021. According to data from India's Computer Emergency Response Team (Cert-In), the total number of incidents increased from 208,456 in 2018 to 1,402,809 in 2021, so according to these figures, cybercrime in India has increased by 572% in just 3 years.[vi]

Cyber Terrorism:

Social media sites such as Facebook, Twitter, and YouTube have become popular recruiting sites for terrorists. The attacks on Charlie Hebdo[vii] and in Paris[viii] in November 2015 highlighted the effectiveness of social media in reaching recruits from afar.

Soon after the enactment of the IT Act of 2000, errors became apparent, prompting the circulation of draft amendments in 2005 and the introduction of a bill in 2006. After the Mumbai attacks, the IT Act amendments owing to the inclusion of the provision on "Cyber Terrorism" were passed in the parliament without debate or discussion. The Mumbai attacks of 26/11 (2008)[ix] were a major factor in the IT Act amendments of December 2008 receiving a super expedited stamp of approval. Section 66F of the IT Act deals with cyber terrorism in India.

Despite their shortcomings, the regulations in place show an attempt to regulate cybercrime and cyber-terrorism. However, when implemented in the sphere of cyber warfare, the regulations clearly illustrate their limits. Several attacks, such as the Estonia DDOS attack, the Stuxnet attack on Iran, and Ukraine's Power Grid Attack are considered cyber-warfare. The lack of effective punishment against perpetrators indicates the enormous gap in the fight against these types of threats

Cyber money laundering has emerged as the next big problem, especially in the fight against terrorism. For cross-border crime, online payment systems have become the primary payment method. More crucially, they have become the primary means for terrorists to raise funds. Consequently, states cannot overlook the fact that terrorists spread their actions through digital or electronic media. This is a real and present threat that states must address.

Laws related to cyber security in India:
Exclusive cyber laws:
The Information Technology Act of 2000,[x] as amended in 2008, is India's principal cybercrime law. Crimes against the nation predominate among the criminal provisions of the old law and the amended IT law.

The provision for cyber terrorism under section 66F was added in 2008. Section 69 of the IT Act gave the government broad interception and monitoring powers. Sections 69A and 69B were added to tighten these provisions, allowing governments to monitor and collect traffic statistics as well as prevent access to content on the internet.

Another provision that affected the dynamics of governmental monitoring and intermediary compliance was the insertion of intermediary duties and liabilities, specifically section 67C, which imposes penalties on intermediaries who violate government directives. Section 70 applied to "protected systems" such as critical information infrastructure. Sections 70A and 70B were inserted to create a national nodal agency for critical infrastructure protection and to establish the Indian Computer Emergency Response Team (CERT-IN).

Sections 71 to 74 deal with offenses involving "Electronic Signature Certificates," such as misrepresentation to obtain an electronic signature certificate (Section 71), breach of confidentiality (Section 72), and publication of an electronic signature certificate with false details or fraudulent purposes (Section 73). In addition, section 72A was enacted, as the criminal counterpart of section 43A of the IT Act. Breach of confidentiality concerning "personal information" with the intent to cause unlawful loss or benefit is punishable by 3 years in prison and a fine of Rs. 500,000 under the section.

3. **Cyberlaw Provisions In Other Laws:**

4. **The IPC and the Indian Evidence Act were revised to add several clauses after the passage of the IT Act in 2000. Most of these modifications dealt with the admissibility of electronic records and offenses related to them. The provisions from sections 463 to 477A of the IPC, which made forging electronic records a crime, were the most significant amendments. These provisions strongly encourage the prosecution of phishing attacks and a variety of other banking and financial frauds.**

   Apart from the IPC, Intellectual Property legislation also bolsters the provisions of the IT Act for punishing infractions. For example, if the data stolen is proprietary, data theft offenses can be prosecuted under section 63 of the Copyright Act, 1957. Section 65B of the Copyright Act, as well as sections 463 to 468 of the IPC, may be used in the case of a breach of a proprietary right to the software. Cybersquatting and phishing crimes may also come under the Trademarks Act of 1999's criminal prohibitions.

   These offenses would fall under the general category of "cybercrime" if they were committed online or using computer resources; however, the IT Act may not specifically regulate them. Provisions from several statutes may become applicable for prosecution depending on the facts of each case.