Different types of Cyber Attacks

Types of Cyber attacks :

It is an attempt to breach the information system of an individual or organization.

1. **Malware:** Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.
2. **Phishing:** Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email.
3. **Man-in-the-middle attack:** Man-in-the-middle (MitM) attacks(eavesdropping attacks) occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal.
4. **Denial-of-service attack(DDOS):** A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack.
5. **SQL injection:** A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.
6. **Zero-day exploit:** A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.
7. **DNS Tunneling:** DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic over port 53. It sends HTTP and other protocol traffic over DNS.They can be used to disguise outbound traffic as DNS, concealing data that is typically shared through an internet connection.

Define Monolithic and Micron Services.

MONOLITHIC :

A monolithic application is built as a single unified unit that is self-contained and independent from other applications. A monolithic architecture is a singular, large computing network with one code base that couples all of the business concerns together.

MICRO SERVICES :

microservices architecture is a collection of smaller, independently deployable services.These services have their own business logic and database with a specific goal. Updating, testing, deployment, and scaling occur within each service.

Difference between REST(Representational State Transfer) and SOAP(Simple Object Access Protocol)

REST was designed specifically for working with components such as media components, files, or even objects on a particular hardware device. Any web service that is defined on the principles of REST can be called a RestFul web service(GET, POST, PUT and DELETE).

The main idea behind designing SOAP was to ensure that programs built on different platforms and programming languages could exchange data in an easy manner. It is used in bank transactions.

- SOAP is a protocol whereas REST is an architectural pattern.
- SOAP uses service interfaces to expose its functionality to client applications while REST uses Uniform Service locators to access to the components on the hardware device.
- SOAP needs more bandwidth for its usage whereas REST doesn’t need much bandwidth.

Study different types of Manual Testing and prepare small description about each manual testing types

Manual software testing is when human testers check the quality of a new application without using automation tools or scripting. The purpose is to identify bugs or defects, ensure the product is error-free, and check it conforms to specified functional requirements. Compares the behavior of a software application with the expected behavior which was defined in the initial phases of the software development life cycle (SDLC).

Acceptance Testing: User Acceptance Testing (UAT) is performed by the client or end-user, to confirm that the software meets the agreed requirements. Sometimes called pre-production testing, it takes place during the final phase before releasing the product to market. UAT is an example of functional testing and types of acceptance testing include Alpha and Beta .

Black Box Testing: (behavioral testing) this method aims to analyze an application's functionality from the end-user's perspective. The internal code structure is not visible during testing (hence the name "Black Box"), so testers are only aware of the inputs and expected outputs of the software.

Integration Testing: Integration Testing is the process of testing an application with two or more integrating components. It is performed once the individual components have been unit-tested, and aims to identify problems with the interfaces and the interactions between them. The two main methods are the Bottom-Up Approach and Top-Down Approach .

System Testing : (end-to-end testing)System Testing means testing the system as a whole, once all its components have been unit-tested and integrated. It checks that the complete application works as intended, by comparing it against the original requirements.

Unit Testing: (module testing or component testing) This is when the individual units or components of an application's source code are tested, to make sure each function performs as expected. It is usually carried out by developers rather than engineers, as it requires detailed knowledge of the internal program design and code.

White Box Testing: (transparent box testing or structural testing) this is a method of testing the internal structures or workings of an application. It is performed by the developer, who checks the software's internal codes before passing it to a test engineer.The main focus of White Box Testing is on strengthening security and improving the software's design and usability.

A combination of Black Box and White Box testing is known as Gray Box Testing.