**Assignment – 1 and 2**

1. **Different types of cyber attacks**
2. Malware

Malware is a type of application that can perform a variety of malicious tasks. Some strains of malware are designed to create persistent access to a network, some are designed to spy on the user in order to obtain credentials or other valuable data, while some are simply designed to cause disruption. Some forms of malware are designed to extort the victim in some way. Perhaps the most notable form of malware is ransomware – a program designed to encrypt the victim’s files and then ask them to pay a ransom in order to get the decryption key.

1. Phishing

A Phishing attack is where the attacker tries to trick an unsuspecting victim into handing over valuable information, such as passwords, credit card details, intellectual property, and so on. Phishing attacks often arrive in the form of an email pretending to be from a legitimate organization, such as your bank, the tax department, or some other trusted entity. Phishing is probably the most common form of cyber-attack, largely because it is easy to carry out, and surprisingly effective.

1. Man-in-the-middle attack (MITM)

A man-in-the-middle attack (MITM) is where an attacker intercepts the communication between two parties in an attempt to spy on the victims, steal personal information or credentials, or perhaps alter the conversation in some way. MITM attacks are less common these days as most email and chat systems use end-to-end encryption which prevents third-party’s from tampering with the data that is transmitted across the network, regardless of whether the network is secure or not.

1. Distributed Denial-of-Service (DDoS) attack

A DDoS attack is where an attacker essentially floods a target server with traffic in an attempt to disrupt, and perhaps even bring down the target. However, unlike traditional denial-of-service attacks, which most sophisticated firewalls can detect and respond to, a DDoS attack is able to leverage multiple compromised devices in order to bombard the target with traffic.

1. SQL injection

SQL injection is a type of attack which is specific to SQL databases. SQL databases use SQL statements to query the data, and these statements are typically executed via an HTML form on a webpage. If the database permissions haven’t been set properly, the attacker may be able to exploit the HTML form to execute queries that will create, read, modify or delete the data stored in the database.

1. Zero-day exploit

A zero-day exploit is where cyber-criminals learn of a vulnerability that has been discovered in certain widely-used software applications and operating systems, and then target organizations who are using that software in order to exploit the vulnerability before a fix becomes available.

1. DNS Tunnelling

DNS tunneling is a sophisticated attack vector that is designed to provide attackers with persistent access to a given target. Since many organizations fail to monitor DNS traffic for malicious activity, attackers are able to insert or “tunnel” malware into DNS queries (DNS requests sent from the client to the server). The malware is used to create a persistent communication channel that most firewalls are unable to detect.

1. Business Email Compromise (BEC)

A BEC attack is where the attacker targets specific individuals, usually an employee who has the ability to authorize financial transactions, in order to trick them into transferring money into an account controlled by the attacker. BEC attacks usually involve planning and research in order to be effective. For example, any information about the target organization’s executives, employees, customers, business partners, and potential business partners, will help the attacker convince the employee into handing over the funds. BEC attacks are one of the most financially damaging forms of cyber-attack.

1. Cryptojacking

Cryptojacking is where cybercriminals compromise a user’s computer or device and use it to mine cryptocurrencies, such as Bitcoin. Cryptojacking is not as well known as other attack vectors, however, it shouldn’t be underestimated. Organizations don’t have great visibility when it comes to this type of attack, which means that a hacker could be using valuable network resources to mine a cryptocurrency without the organization having any knowledge of it. Of course, leaching resources from a company network is far less problematic than stealing valuable data.

1. Drive-by Attack

A ‘drive-by-download’ attack is where an unsuspecting victim visits a website which in turn infects their device with malware. The website in question could be one that is directly controlled by the attacker or one that has been compromised. In some cases, the malware is served in content such as banners and advertisements. These days, exploit kits are available which allow novice hackers to easily setup malicious websites or distribute malicious content through other means.

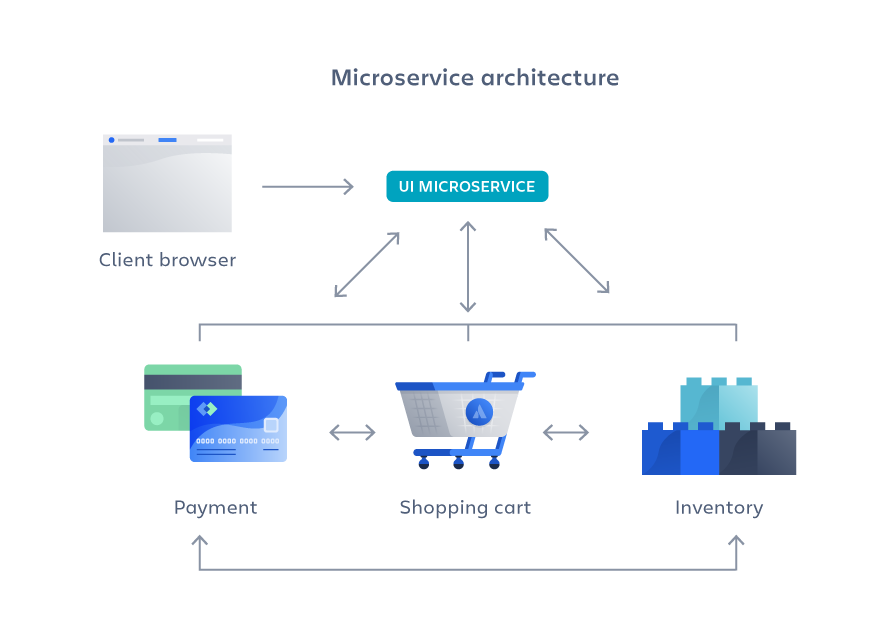
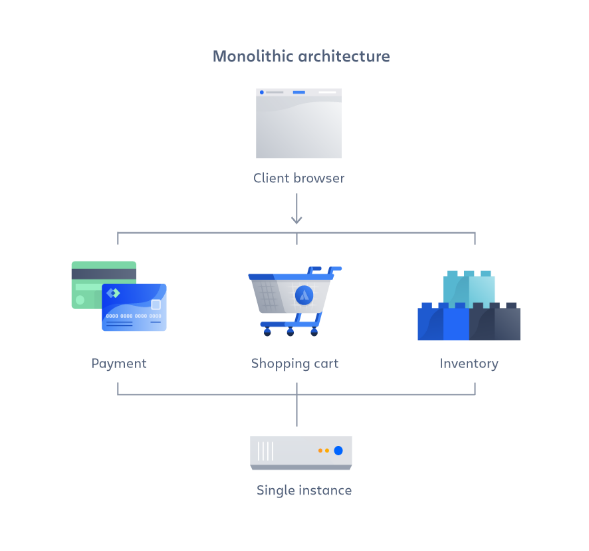
1. **Microservices and Monolithic Architectures**

A **monolithic architecture** is a traditional model of a software program, which is built as a unified unit that is self-contained and independent from other applications.

* The word “monolith” is often attributed to something large and glacial, which isn’t far from the truth of a monolith architecture for software design.
* A monolithic architecture is a singular, large computing network with one code base that couples all of the business concerns together.
* To make a change to this sort of application requires updating the entire stack by accessing the code base and building and deploying an updated version of the service-side interface. This makes updates restrictive and time-consuming.
* Monoliths can be convenient early on in a project's life for ease of code management, cognitive overhead, and deployment. This allows everything in the monolith to be released at once.

A **microservices architecture**, also simply known as microservices, is an architectural method that relies on a series of 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.
* Microservices decouple major business, domain-specific concerns into separate, independent code bases.
* Microservices don’t reduce complexity, but they make any complexity visible and more manageable by separating tasks into smaller processes that function independently of each other and contribute to the overall whole. and deployment. This allows everything in the monolith to be released at once.



1. **Differences between REST API and SOAP API**