Makara Ramoabi

20240045

Security

1.**Scenario analysis**

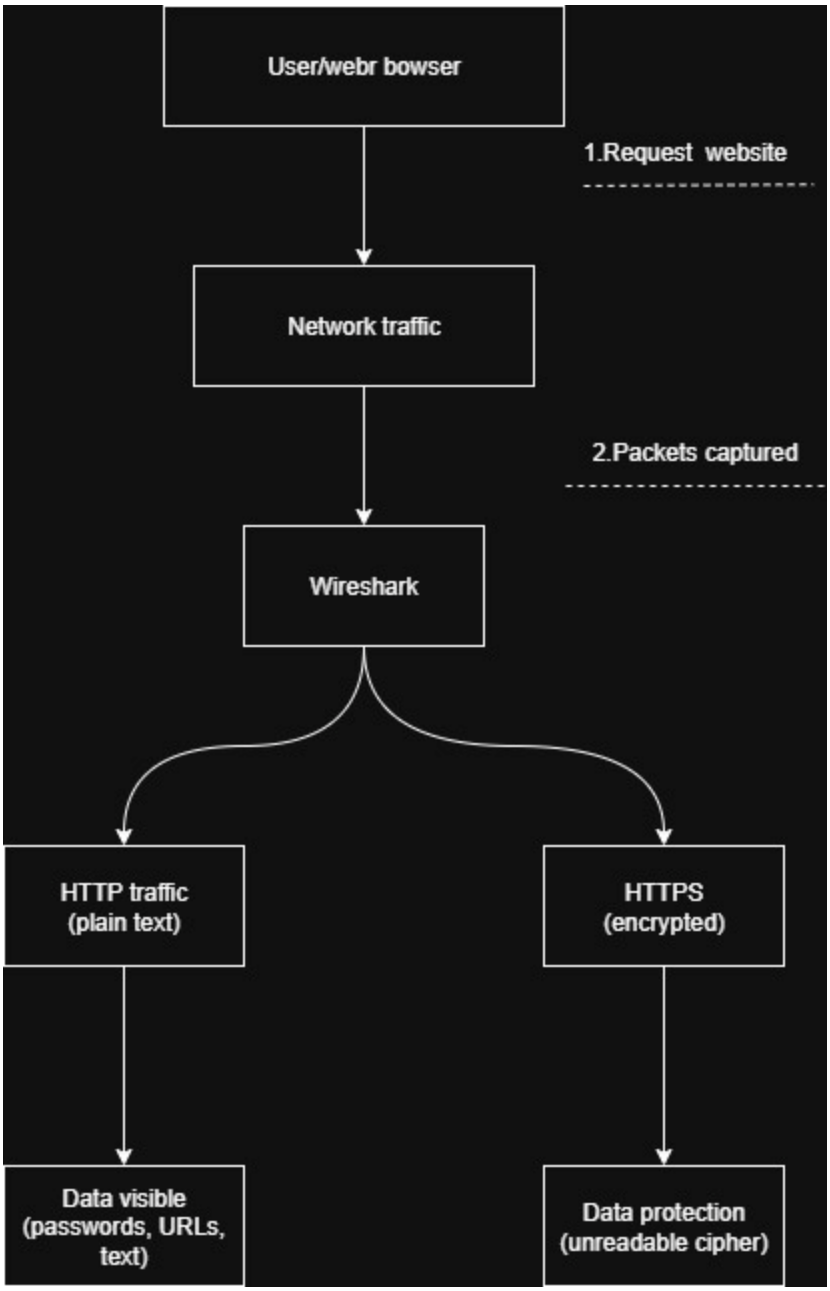
An employee of a marketing company is doing some market research for a product; she goes to a website that claims to have important data in that field. She browses the page and deems it legit. She then decides to download the file (PDF) to study further, and more thoroughly. When she pressed the 'Download' button, the instillation began. When the download reached 100%, she received a message stating "Couldn't download file, we have detected malware and it is unsafe". This is due to a security measure that her company had implemented called checksum. Checksum is a short string of numbers/letters (a hash) that's created from a file's contents. If even one bit is of, the file changes. The checksum has to change. The checksum is usually sent along with the file when downloaded from the website, and during the transfer some tempering might happen. The checksum is supposed to grasp if the file is legit and tempered with.

2.**Concept research**

Confidentiality is a security principle that ensures that data is only accessed by authorized personal only. It prohibits access of sensitive data to unauthorized and outside personal. This is crucial for any system that contains sensitive data. It uses tactical and secure measures to protect data, such as encrypting it. Encryption is converting readable data (text, numbers) into unreadable data (ciphertext). This makes it so that even if there is a small data breach, it is almost impossible to read/use the data. This method can be used on user passwords, user identity, and user data during data transfer or storage.

3.**Tool practice**

Using Wireshark helped me understand how data travels across a network and how security protects it. When capturing HTTP traffic, the information was visible in plain text, which showed how easy it is for attackers to intercept sensitive data. On the other hand, HTTPS traffic appeared encrypted and unreadable, proving the importance of encryption in protecting confidential data. This practical activity made network security concepts more real and easier to understand. It showed that security is not just theoretical but actively protects users from threats such as data theft, tempering, and spying.



4.**Security diagram**

The CIA triad represents the three core principles of information security: Confidentiality, Integrity, and Availability. Confidentiality ensures that data is only accessed by authorized users through mechanisms like encryption and access controls. Integrity ensures that data remains accurate and unaltered by using hashing and checksums to detect changes. Availability ensures that systems and data are accessible when needed through backups, redundancy, and proper

maintenance. Together, these principles help organizations project sensitive information, prevent unauthorized changes, and ensure reliable access to systems and services.