★ Clickjacking:

- Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.
- Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.
- The invisible page could be a malicious page, or a legitimate page the user did not intend to visit – for example, a page on the user's banking site that authorizes the transfer of money.
- There are several variations of the clickjacking attack, such as:
- Likejacking – a technique in which the Facebook "Like" button is manipulated, causing users to "like" a page they actually did not intend to like.
- Cursorjacking – a UI redressing technique that changes the cursor for the position the user perceives to another position. Cursorjacking relies on vulnerabilities in Flash and the Firefox browser, which have now been fixed.

★ Clickjacking attack example

- The attacker creates an attractive page which promises to give the user a free trip to Tahiti.
- In the background the attacker checks if the user is logged into his banking site and if so, loads the screen that enables transfer of funds, using query parameters to insert the attacker's bank details into the form.
- The bank transfer page is displayed in an invisible iframe above the free gift page, with the "Confirm Transfer" button exactly aligned over the "Receive Gift" button visible to the user.
- The user visits the page and clicks the "Book My Free Trip" button.
- In reality the user is clicking on the invisible iframe, and has clicked the "Confirm

Transfer” button. Funds are transferred to the attacker.

- The user is redirected to a page with information about the free gift (not knowing what happened in the background).
- This example illustrates that, in a clickjacking attack, the malicious action (on the bank website, in this case) cannot be traced back to the attacker because the user performed it while being legitimately signed into their own account.

★ Clickjacking mitigation

- There are two general ways to defend against clickjacking:
- Client-side methods – the most common is called Frame Busting. Client-side methods can be effective in some cases, but are considered not to be a best practice, because they can be easily bypassed.
- Server-side methods – the most common is X-Frame-Options. Server-side methods are recommended by security experts as an effective way to defend against clickjacking.

★ Mitigating clickjacking with X-Frame-Options response header

- The X-Frame-Options response header is passed as part of the HTTP response of a web page, indicating whether or not a browser should be allowed to render a page inside a <FRAME> or <IFRAME> tag.
- There are three values allowed for the X-Frame-Options header:
- DENY – does not allow any domain to display this page within a frame
- SAMEORIGIN – allows the current page to be displayed in a frame on another page, but only within the current domain to
- ALLOW-FROM URI – allows the current page to be displayed in a frame, but only in a specific URI – for example www.example.com/frame-page

★ What is Sniffing?

- Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing

sensitive information such as password, account information etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.

- There are two types:

Active Sniffing:

- Sniffing in the switch is active sniffing. A switch is a point to point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic. This can be done in various ways.

Passive Sniffing:

- This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them

Top Sniffing tools

Wireshark:

- An opensource packet capturer and analyzer. It supports Windows, Linux etc. and is a GUI based tool (alternate to Tcpdump). It used pcap to monitor and capture the packets from the network interface. The packets can be filtered basis IP, protocol and many other parameters. The packets can be grouped or marked basis relevance. Each packet can be selected and dissected as per need (also consider checking this perfect guide for cyber security certification).

dSniff:

- It is used for network analysis and password sniffing from various network protocols. It can analyze a variety of protocols (FTP, Telnet, POP, rLogin, Microsoft SMB, SNMP,

IMAP etc) for getting the information.

- Microsoft network monitor: As the name suggests it is used for capturing and analyzing the network. It is used for troubleshooting the network. Some of the features of the software are Grouping, a Large pool of protocol support(300+), Wireless monitor mode, reassembly of fragmented messages etc.

Debookee:

- It is a paid tool that can be used to monitor and analyze the network. It is able to intercept and analyze the traffic from devices that are in that subnet, irrespective of the device type (Laptop, devices, TV etc). It offers various modules:

- Network analysis module: scan for connected devices, Intercept traffic in a subnet, TCP port scanner, Network analysis and monitoring of HTTP, DNS, TCP, DHCP protocols, Analyse VoIP calls etc.

- WiFi monitoring module: Details of access points in radio range, wireless client details, wifi statistics etc.

- SSL/TLS decryption module: Support for monitoring and analyzing secured protocols.

Precautionary measures against Sniffing attacks

- Connect to trusted networks: Do you trust a free Wi-Fi offered by the coffee shop next door? Connecting to any public network will have a risk that the traffic might be sniffed. Attackers choose these public places exploiting the user's lack of knowledge. Public networks are setup and then may or may not be monitored for any intrusions or bugs. Attackers can either sniff that network or create a new network of their own with similar names so that the users get tricked into joining that network. An attacker sitting at an airport can create a Wi-Fi with the name of "Free Airport Wi-Fi" and the nearby users may connect to it sending all the data through the attackers' sniffer node. The word of caution here is that you should only connect to the network you trust – home network, office network etc.

- Encrypt! Encrypt! Encrypt! : Encrypt all the traffic that leaves your system. This will ensure that even if the traffic is being sniffed, the attacker will not be able to make sense of it. One thing here to be noted is that security work on defense in depth principle. Encrypting he data does not mean that now everything is safe. The attacker might be able to capture a lot of data and run crypto attacks to get something out of it. Use of secured protocols ensures that the traffic is encrypted and renders security for the traffic. Websites using https protocol are more secure than the ones that use HTTP – how is that achieved? Encryption.

- Network scanning and monitoring: Networks must be scanned for any kind of intrusion attempt or rogue devices that may be setup in span mode to capture traffic. Network admins must monitor the network as well so as to ensure the device hygiene. IT team can use various techniques to determine the presence of sniffers in the network. Bandwidth monitoring is one, an audit of devices which are set to promiscuous mode etc

★ The following techniques and tools can be used to mitigate sniffers:

★ • Authentication—A first option for defense against packet sniffers is to use strong authentication, such as one-time passwords.

★ Switched infrastructure—Deploy a switched infrastructure to counter the use of packet sniffers in your environment.

★ • Antisniffer tools—Use these tools to employ software and hardware designed to detect the use of sniffers on a network.

★ • Cryptography—The most effective method for countering packet sniffers does not prevent or detect packet sniffers, but rather renders them irrelevant.