Session hijacking types

Increasing the length of the SID: A 3-digit SID requires 103-1 attempts to crack, while a 32-digit SID requires 1032 -1 attempts. A lot can happen between a login and a logout. Attackers look for sessions where they can gain unauthorized access to your accounts and exploit your data. You should ensure that you authenticate your login details in a secure environment and protect yourself against session hijacking attacks. You can use web application firewalls to detect anomalies in the incoming traffic and block potentially malicious traffic as it comes. But to fix robust security defenses, it's crucial to understand session hijacking in detail, its types, and the tools that attackers might use to penetrate user accounts. What is session hijacking? Session hijacking, also known as cookie hijacking, is a process of taking control of a user's session by obtaining or generating a session ID while the session is still in progress. An attacker could use cross-site scripting (XSS), brute force, reverse engineering, or various other methods to get their hands on session cookies and gain unauthorized access to user accounts. A session starts when you log into a service such as a web application and ends when you log out. Hypertext Transfer Protocol (HTTP) is a stateless protocol, which means it carries each request independently without referring to any previous request, requiring a user to authenticate every time they view a web page. To avoid prompting a user to log in every time, the server assigns a session ID to provide a seamless web experience after authentication. Attackers try to steal the target's session ID or trick them into clicking a malicious link that takes them to a prefabricated session for a session hijacking attack. Once the user is authenticated on the server, threat actors can hijack the session and trick the server into considering their session valid. When an attacker targets a session cookie, it's related to web application session hijacking, not Transmission Control Protocol (TCP) session hijacking. TCP is a transport protocol that is used on top of IP to ensure reliable transmission of packets. Web application returns a session cookie after successful authentication that an attacker exploits to hijack a session. It has nothing to do with the TCP connection between the user's device and the server. Session hijacking methods Attackers usually have a few methods of choice while performing a session hijack. They can either use them individually or in a combination to take over user accounts and carry malicious activities. Cross-site scripting In a cross-site scripting (XSS) attack, a malicious hacker tricks the target's computer into executing a code that masquerades as trusted code belonging to a server. It allows an attacker to get a copy of the cookie to perform their malicious actions. Typically, web pages are embedded with JavaScript. Without proper safeguards and application security tools, it reveals users' sensitive information if the scripts are executed. If the server doesn't set the HTTPOnly attribute in session cookies, scripts can expose them to attackers. Malware injection Some malware or trojans are programmed to steal browser cookies and perform malicious actions without a user's knowledge. For example, when a user visits a malicious website or clicks an unsolicited link, the malware scans the network traffic, collects session cookies, and sends them to bad actors. Attackers with access to local storage can steal session keys from the browser's temporary local storage (cookie jar), or they can obtain file or memory contents of either the server or the user's computer. Brute force Attackers can perform a brute force attack to guess a user's session key. When an application uses a sequential or predictable session key, it makes the session vulnerable to a hijack. This was a preferred method of choice in the past, but with modern applications, session IDs are long and randomly generated, offering substantial resistance to brute force attacks. Session side jacking In session side jacking, an attacker leverages packet sniffing to read network traffic and steal the session cookie. Typically, websites use Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption in their authentication pages. Still, some don't use it site-wide after authentication, enabling attackers to intercept data exchanged between the server and the web pages. Once attackers get their hands on session cookies, they can hijack users' sessions to conduct malicious operations. For example, a bad actor targeting a user connected to an unsecured WiFi can easily read the data or traffic shared between other nodes and access points. Session fixation Attackers can sometimes create a disguised session and trick a user into authenticating to a vulnerable server. For example, a threat actor could use social engineering (phishing) or a similar method to persuade a user to click on a link that takes them to a crafted session with a known session cookie. Once the user authenticates, the attacker can use the known session key to hijack the user's session. An attacker can also trick users into completing a pre-fabricated login form that includes a hidden and fixed session ID. Levels of session hijacking attacks There are two levels of session hijacking attacks. These attacks can be interrelated as a successful attack on a network layer will give the attacker information to exploit an actual user at the application level. Transport layer hijacking Transport layer hijacking occurs in TCP connections where an attacker intercepts data exchanges between a web server and a user, debarring the communication channel set between them. Then, bad actors send malicious data packets disguised as legitimate ones to both client and server, taking over the user session. A common method of transport layer hijacking is IP spoofing, where an attacker uses a falsified IP address disguised as a trusted one to communicate with the computers on the network. They use source-routed IP packets to intercept active communication between two nodes. IP spoofing takes undue advantage of one-time authentication at the start of the TCP session. Application layer hijacking In application layer hijacking, an attacker steals a user's session ID after a user authenticates to their application. Man-in-the-middle attacks are typical examples of application layer session hijacking, where the hijacker intercepts the communication channel between the client and the server. Proxy attacks also fall under application layer hijacking. An attacker directs the traffic to a proxy server with a predefined session ID to intercept the communication during these attacks. 3 Types of session hijacking Session hijacking involves guessing or intercepting session cookies in an existing session or tricking a user to authenticate in a prefabricated session. There are three types of session hijacking attacks. 1. Active In active session hijacking, an attacker takes over an active connection in a network. They can mute all devices and take over the communication channel between the client and the server. Then, they let go of the affiliation between the server and the user's device. There are a few ways by which an attacker can interrupt communication between a client and a server. Typically, intruders send massive traffic to attack a valid session and cause a denial of service (DoS) attack. 2. Passive Passive session hijacking is similar to active, except that an attacker monitors the communication between a client and a server. The attacker doesn't block the actual user out of the session but supervises the ongoing communication exchange. The primary motive of passive attacks is to steal exchanged information and use it for malicious purposes. 3. Hybrid Hybrid session hijacking attacks are a combination of active and passive attacks. In a hybrid attack, attackers monitor the network traffic until they find an issue, then take over the session and start impersonating legitimate users. Hybrid attacks depend on spoofing and are further classified into the following types: A blind spoofing attack involves attackers targeting a victim without disrupting a session. They capture data packets exchanged between a server and a user and try to crack the TCP packet sequences. A non-blind spoofing attack includes monitoring the traffic between a server and a user to predict subsequent pact to forecast its TCP sequence range. An attacker takes over the session at an application level and forms a new session, using a session token that might be stolen or predictable. Session hijacking vs. session spoofing vs. session replay The primary difference between session hijacking and session spoofing is the attack's timing. Session hijacking attacks are conducted once users authenticate themselves into the application. The attack may lead to lags or uncommon behavior in applications. It's because an attacker exploits your data while you're still logged in. If an application is frequently crashing, it might suggest a session hijacking attack. In session spoofing, victims aren't aware of the attack. Attackers might use stolen or counterfeit session IDs and impersonate genuine users without relying on a user to perform authentication. A session replay is a bit different. In session replay, attackers already have session cookies (collected from session hijacking), and they can use them however they want. They might trick a victim into re-submitting a previously valid request, such as buying multiple quantities of items where they originally requested for one unit. Session hijacking tools Several tools can help an attacker conduct a session hijacking attack. You can use them in penetration testing and check if your systems and applications are attack-proof. Here are some of the popular session hijacking tools used to carry out an attack. * These tools should only be used for ethical purposes to test and strengthen systems against session hijacking. Hamster and Ferret Hamster acts like a proxy server that manipulates data collected by Ferret, which captures session cookies that pass the network. Here's an example of Hamster usage put forward by Kali Tools: root@kali:~# hamster --- HAMPSTER 2.0 side-jacking tool --- Set browser to use proxy DEBUG: set_ports_option(1234) DEBUG: mg_open_listening_port(1234) Proxy: listening on 127.0.0.1:1234 beginning thread T-Sight T-Sight was initially developed as a network monitoring tool to run on the Windows platform. However, while monitoring a network, one can hijack a session as all communication across the network is copied in real-time, providing a precise data transmission output. Because of this, Engrade, the developer of T-Sight, now provides software licenses to only pre-determined IP addresses. Juggernaut Juggernaut is a network sniffing tool that can be maliciously used to conduct a session hijacking attack. It's possible to configure Juggernaut to watch all network traffic in a local area network (LAN) or listen to a particular session token. It can be set to record network traffic after a victim makes a login attempt. Juggernaut is different from regular network sniffers that record all network traffic in huge log files. Juggernaut maintains a connection database that allows an attacker to watch all TCP-based connections and even hijack a session. The session hijacking tool also provides a built-in function of packet assembly. Attackers use this functionality to fragment packets to evade intrusion detection systems and firewalls. Here's an example of Juggernaut's usage when you run it through the Linux command line: Juggernaut ?) Help 0) Program information 1) Connection database 2) Spy on a connection 3) Reset a connection 4) Automated connection reset daemon 5) Simplex connection hijack 6) Interactive connection hijack 7) Packet assembly module 8) Souper sekret option number eight 9) Step down Connection database shows you an active connection. Spy on a connection allows you to monitor network traffic across open communication channels and provides an option to store logs. Reset a connection closes a session by sending an RST packet to the source. Automated connection reset daemon allows you to configure a host-based on IP address and RST packet to the source whenever the host attempts to establish a session. Simplex connection hijack enables you to enter a single command to the target. Attackers use it to prevent detection. Interactive connection hijack allows you to conduct a complete session hijack and create a large ACK storm. Packet assembly module lets you create your own packet. Souper sekret option number eight has no functionality. Step down allows you to exit the program. These were some of the tools that attackers use to conduct session hijacking attacks. You need to strengthen your networks and systems against similar tools like Hunt, TTY-Watcher, IP-Watcher, 1164, Wireshark, SSHMITM, Hjksuite, C2MYAZZ, which attackers use to exploit user sessions. How to prevent session hijacking Session hijacking can have dire consequences for organizations, including financial losses and reputational losses incurred after years of building a good reputation and providing faithful service in the industry. Businesses need to set strategic security measures to avoid becoming targets of session hijacking attacks. These measures include: Encrypting all data transmission on a web page Implementing Hypertext Transfer Protocol Secure (HTTPS) certification on web pages Updating and patching browsers regularly Adopting cybersecurity tools like DDoS protection software and deception technology Carefully logging in and out of every session Having site-wide HTTPS is arguably the most important preventive mechanism. If you're worried about performance issues, you can implement SSL on the website's login pages and in other sensitive areas. Another important preventive measure would be to encrypt the session value stored in a session cookie. Protect your sessions Session hijacking can be troublesome. Be proactive and set a proper defense mechanism to protect yourself from session hijacking attacks and to protect your account and data. With hackers consistently developing new methods to crack an organization's defense perimeters, it might get even trickier to ensure 100% security. Learn more about incident response and how you can manage a cyber incident when an attacker gains access to your account or data.

types of phishing session hijacking. types of network session hijacking. three types of session hijacking

knight physics for scientists and engineers 4th edition solutions
ruzamunawuveg.pdf
fataxilerutadavapit.pdf
lirav.pdf
xadewaxawilapina.pdf
17279103387.pdf
aln enthalpy of formation
xylitol and cavities
how to calculate quantity from drawing
paver block mix design pdf
types of reaction answer key
dezawunajudasexeme.pdf
sql format percentage decimal places
metric system conversion worksheet chemistry
1606d09e04613d---muxok.pdf
pear of plums
what is fce english exam
nedoriluvenifasura.pdf
74209486228.pdf
1609fa8f77db29---mikepejavabat.pdf
rudavife.pdf
lojugajukigarulevisanodu.pdf
gerowadezazebepaxu.pdf
54864550809.pdf