What Is Client Side Exploitation?

Introduction:-

Nowadays Server side is getting strong day by day but there are still vulnerabilities present on the client-side and this leads to client-side exploitation. This article will introduce you to various client-side exploitation techniques that can be used in a penetration test. Client-side exploits are very useful to attackers when the client is behind the firewall or any application security layer. In this situation, it is not possible to directly access the client through the network.

The success rate of finding a vulnerability in the client site is directly proportional to the reconnaissance. If you are performing penetration testing on any application to test is there any client-side exploitation is possible or not you must have an understanding of possible attack scenarios to find and prevent the Client-Side Exploitation on your application.

Attack Scenario's In Client-Side Exploitation:

E-Mails with Malicious Attachments-

In this particular attack scenario, the attacker will send the malicious files such as PDF, exe, or mp3 in the hope that the victim would click on the link and download and execute the attachment. Upon execution, the attacker has a Meterpreter session opened on the victim's machine.

This attack can be a bit difficult to accomplish, as the attacker needs to convince the victim to execute their .exe file. Another major hurdle would be the victim's antivirus, which you need to bypass. Luckily, Metasploit has some built-in encoding mechanisms that, when used effectively, can evade some anti viruses, and if used effectively. However, all this is based on trial and error.

Malware Loaded on USB Sticks-

This method can be used by an attacker when he/she have physical access to the victim's machine. The attacker loads up a malicious PDF file or a malicious executable payload via a USB stick. Once the USB stick is inserted, malicious code will automatically be executed and the attacker would get a meterpreter session opened on the victim's machine. Teensy USB is a device that has the capability to emulate a mouse and keyboard.

E-Mails Leading to Malicious Links-

In this particular attack scenario, the attacker will send malicious links in the hope that victims would click on them. The link could be a fake log-in page or a web server hosted with an attacker's malicious code. Considering the attacker is hosting a web server, the code will be executed in the victim's browser and an attacker will have a meterpreter session opened.
In this scenario, the attacker sends the victim a malicious link, and when the victim clicks on it, we will be able to perform various attacks. Here are some examples:

- An attacker can set up a fake log-in page of any particular website, for example, facebook.com, and ask the victim to log in to the fake log-in page actually located at facebookfake.com

- If the attacker is on the same network as the victim, he can launch a DNS spoofing attack, where we can replace the IP of example.com with that of the attacker's fake log-in page, and as soon as the victim visits example.com, he would log in to our fake page instead.

- An attacker can also perform DNS spoofing, where instead of the fake log-in page we can redirect the victim to our malicious webserver that would use relevant browser exploits to compromise the victim's browser.

Browser Exploitation-

Browser-based exploits are one of the most important forms of client-side exploits. Imagine a scenario where you are pen-testing against an organization. If it's an internal pentest, you would already own a box on the LAN. If it's an external pentest you need to somehow gain access to a system. You can set up a malicious web server and ask the victim to visit the server. As soon as he clicks your link, he gets compromised.

Most of the employees of an organization frequently browse on social networking websites like Facebook and Linkedin. We, as penetration testers, can take advantage of this and send malicious links to the employees and compromise them. On an internal network, the attacker could simply use a DNS poisoning attack to redirect victims to his malicious webserver. To sum up, there is a whole lot of attack surface when it comes to browser exploitation.

Compromising Client-Side Update-

In this scenario, an attacker will utilize previously mentioned attack vectors to compromise the client-side updating process. It means that whenever a victim updates a particular software, he will download malicious code instead of updates. In this scenario, the attacker will compromise client-side updates by using a neat tool called Evilgrade, which comes preinstalled with BackTrack. Evilgrade takes advantage of insecure update processes as the user normally does not double-check before an update because they trust that the application is being downloaded from the right place.

Social Engineering Attack-

In a social engineering penetration test, the organization may ask you to attack its users. This is where you use speared phishing attacks and browser exploits to trick a user into doing things they did not intend to do. A social engineering attack can be part of a network penetration test in some cases.
In the current situation of online work and education, social engineering attack is increasing day by day. Almost every person who has an email address and mobile number may get a victim of social engineering attacks for the attacker. In social engineering attack, the attacker fraudulently obtains confidential data from the users.

How To Protect From Client-Side Exploitation:-

1. In client-side exploitation, attackers take advantage of the weakest link that is clients.

2. To protect yourself from client-side attacks you have to be alert during your everyday Internet surfing.

3. Don’t open any link coming from a malicious or unknown person.

4. After opening any email attachment always make sure that the mail is coming from an authorized source.

5. Avoid downloading .exe attachments of a mail.
6. Always check the confidentiality of the domain of the website after filling in confidential information like username, password, card number, bank account number, etc.