**Downgrade Attacks**

Instead of attacking the more secure later versions of TLS, the target of downgrade attacks is to force a victim to use insecure configurations of TLS. That can either be an older, potentially weaker version of TLS or a flawed cipher suite. After successfully conducting a downgrade attack, an attacker can then focus on breaking the weaker configuration forced upon the client in a second attack step.

More specifically, downgrade vulnerabilities arise when TLS servers support multiple TLS versions to enable older clients that do not support the latest TLS version to communicate with the server as well. This can potentially be exploited by an attacker to force even clients that do support the latest TLS version to downgrade to an older, more insecure TLS version.

**Cipher Suite Rollback**

Cipher suite rollback attacks target SSL 2.0. That is because the list of cipher suites transmitted by the client and server during the handshake is not integrity protected with a MAC. It is therefore possible for a MitM attacker to intercept the ClientHello message and alter the list of cipher suites in such a way that a weak cipher suite is chosen, for instance by providing only export cipher suites. He can then forward the handshake message along and the handshake will proceed as normal. The connection established between the client and server will then use a weak cipher suite that can be broken by the attacker. SSL 3.0 and all TLS versions protect against cipher suite rollback attacks by including the list of cipher suites in the MAC of the final message of the handshake, thereby providing integrity protection. That way, changes made by a MitM attacker are detected before the handshake is concluded, leading to an alert and a failed connection establishment.

**TLS Downgrade Attacks**

The target of TLS downgrade attacks is to force the client into using an older and potentially weak TLS version for the connection with a server. A MitM attacker can achieve downgrade attacks by continuously interfering in the TLS handshake and dropping packets, resulting in a handshake failure. After a few failed handshake attempts for TLS 1.2, browsers may fall back to TLS 1.1 for connection establishment. The attacker can repeat this process until the victim's browser attempts to establish a connection using the desired TLS version. Interestingly, this is undocumented behavior of web browsers, though it was found to work in the past.

Exploits for attacks like POODLE and FREAK utilize a downgrade attack as part of their attack chain to target servers running secure TLS versions that still support older, vulnerable TLS versions such as SSL 3.0. To prevent downgrade attacks entirely, support for old TLS versions should be removed completely.

**Note:** TLS downgrade attacks are different from HTTP downgrading.