Day 8

Exploitation Analyst

Hacking the SSL Network protocol:

Protocol Downgrade Attack:

What is a Protocol?

A protocol is a set of rules or standards that define how data is formatted, transmitted, and interpreted between devices over a network.

What is a Protocol Downgrade Attack?

A Protocol Downgrade Attack is a man-in-the-middle (MitM) attack where an attacker tricks a client and server into using an older, less secure version of a protocol, even though both support a newer, secure version. This weakens encryption, allowing the attacker to intercept, decrypt, or modify sensitive data.

One of the most famous examples is the POODLE attack (Padding Oracle On Downgraded Legacy Encryption), which exploits SSL 3.0 — an outdated and insecure protocol.

How Does This Happen?

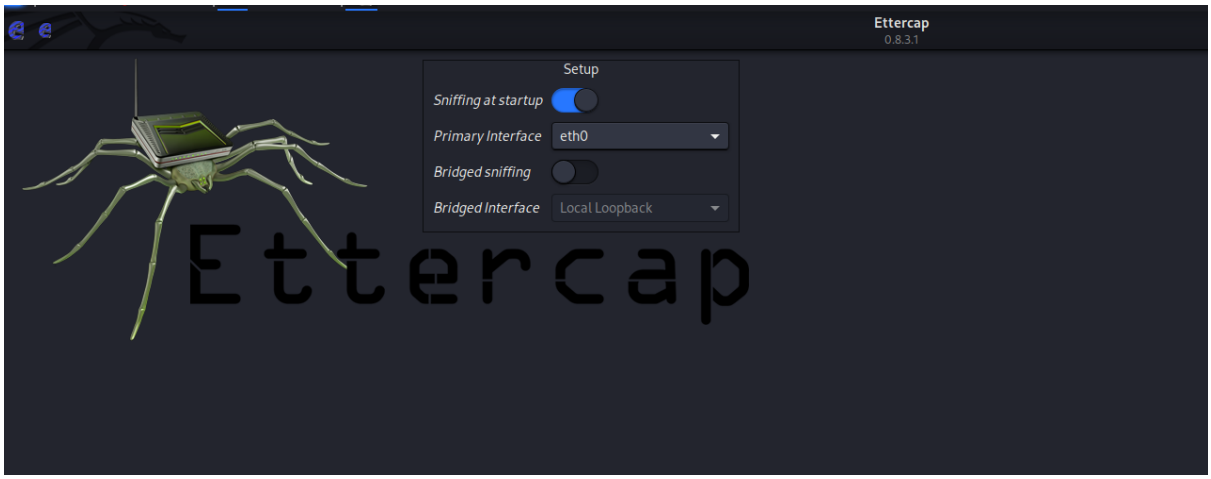
When a client connects to a server (e.g., during HTTPS), both sides negotiate which protocol version to use (called the TLS handshake). If something fails, they may fall back to older versions for compatibility.

Downgrade attacks abuse this fallback behavior by interfering with the handshake (e.g., dropping packets or altering messages) so that both parties "agree" to use SSL 3.0, which has known cryptographic flaws.

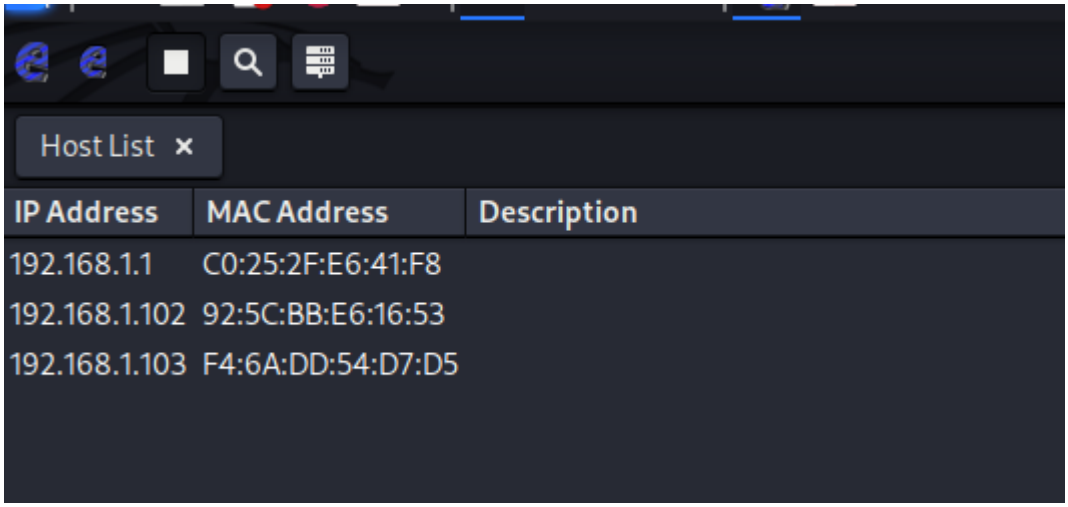
SSL Stripping - Downgrading HTTPS to HTTP to capture plain text passwords:

Steps:

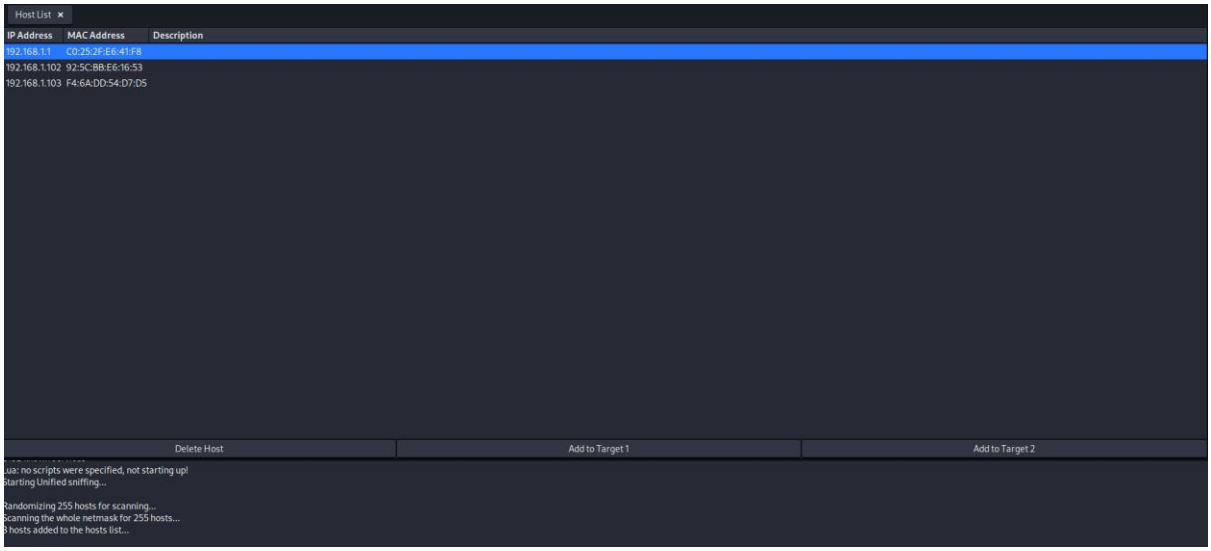
Open the Ettercap:



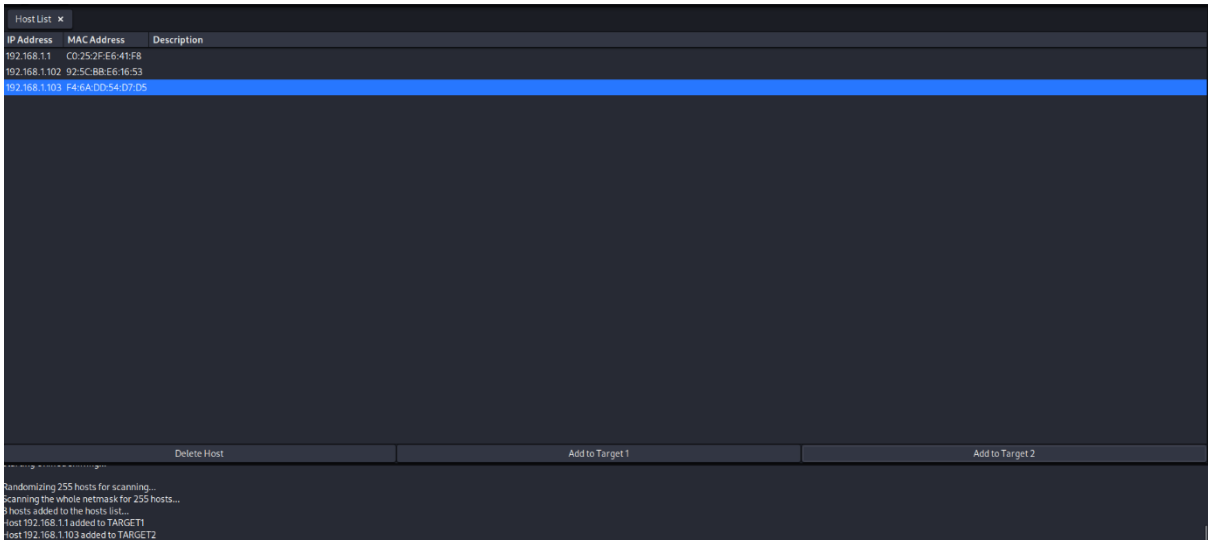
Click on the scan host option:



Then click on the IP of the Router and click on the Add to Target 1 button: here the 192.168.1.1 is the IP of the router.

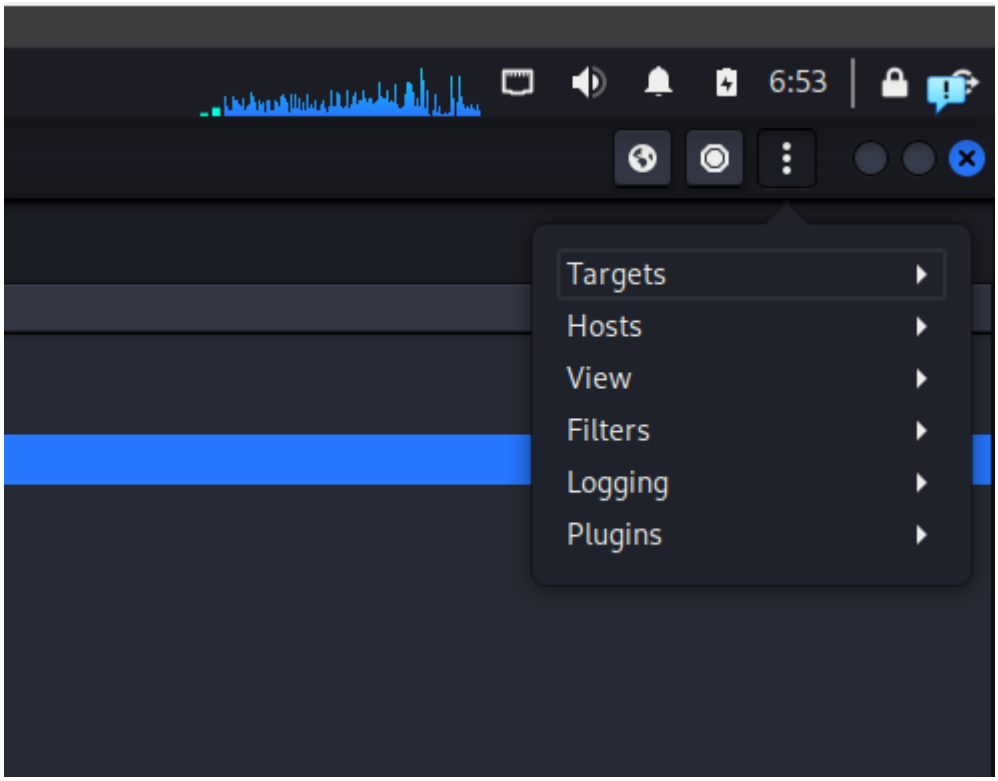


Then click on the target IP, here we selected the IP – 192.168.1.103:

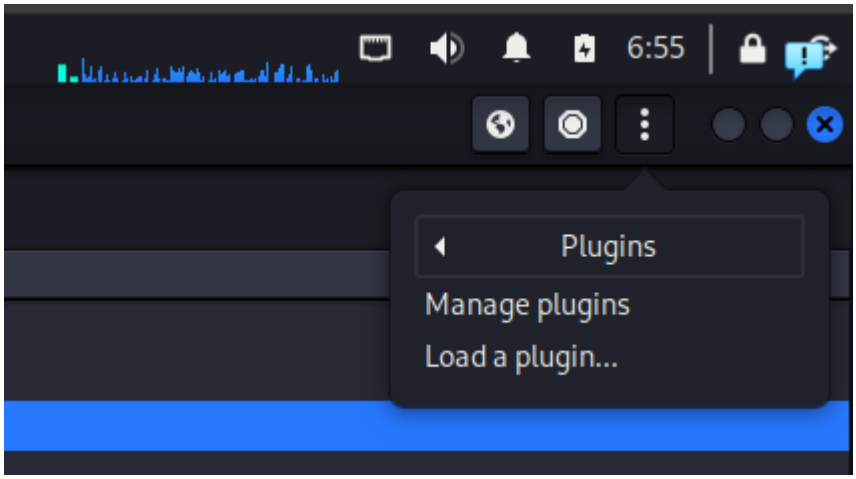


Now, we have selected the target and the machine for MITM.

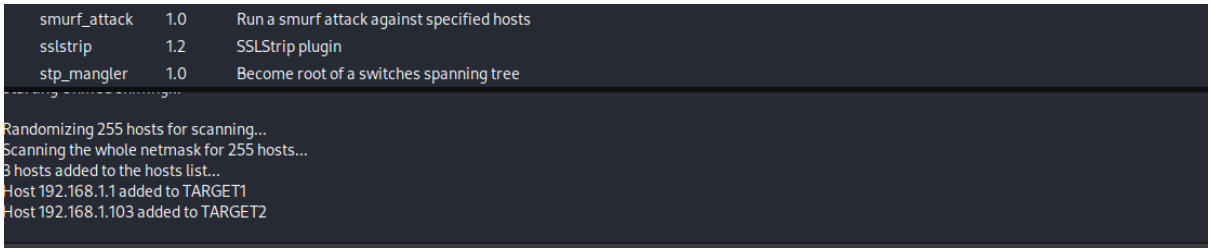
Now, we will go to the three dots, and see the options as shown:

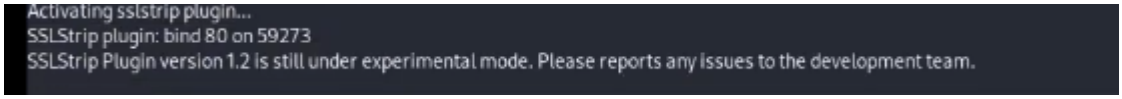


Click on the ‘plugins’ and then select the option of ‘manage plugins’:

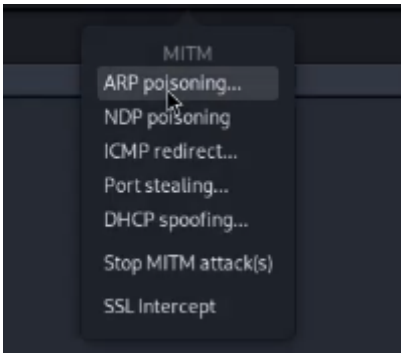


Now, scroll down and select the option of ‘sslstrip’:

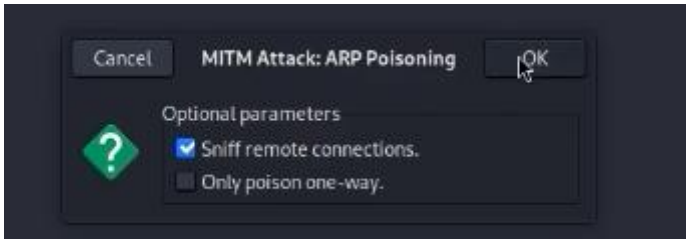




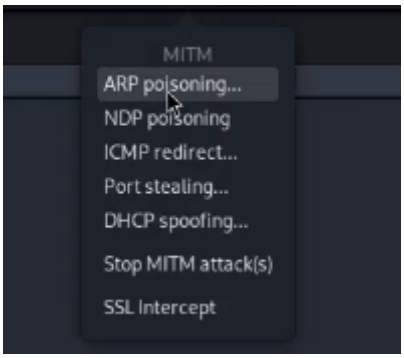
Now, we will go to the MiTM menu: select ARP poisoning.



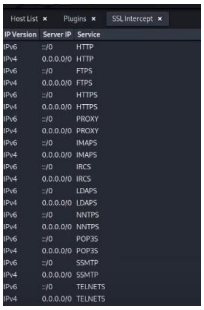
Click on the ‘ok’ button:



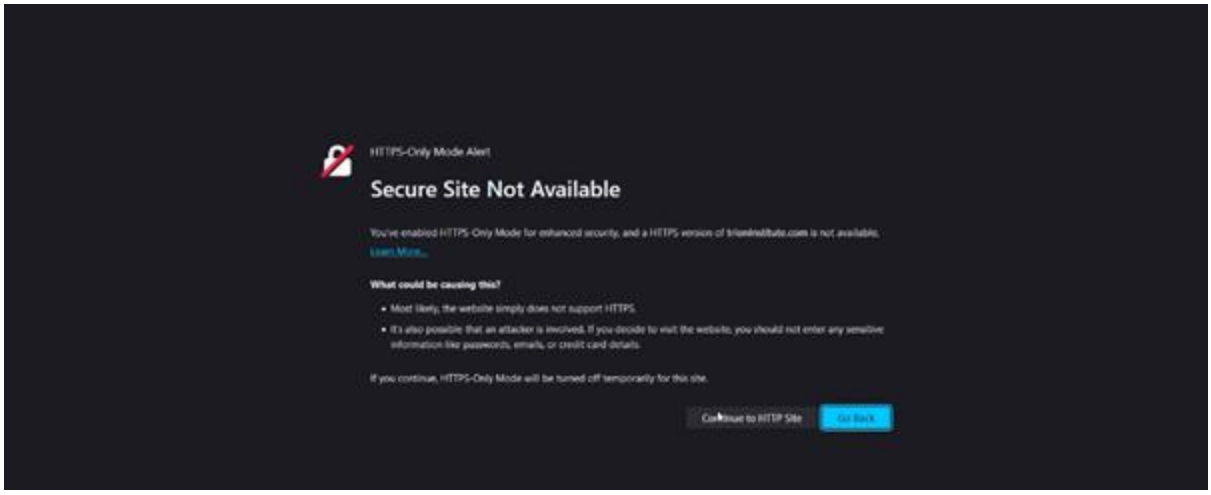
Then again I will go to the MITM menu, and select the ‘SSL Intercept’ option:



Following list will appear:



Then we try to enter any website:



Clearly, we downgraded the website.

Short Defense List – SSL Stripping & Downgrade Protection

- **Enable HSTS**: Enforce HTTPS via HTTP headers.
- **Force HTTPS Redirects**: Redirect all HTTP to HTTPS at server level.
- **Disable Weak Protocols**: Only allow TLS 1.2/1.3.
- **Use Secure Cookies**: Set Secure and HttpOnly flags.
- **Add DNS CAA Records**: Restrict which CAs can issue certs.
- **Enable TLS Pinning**: Validate server certs in apps.
- **Monitor Traffic**: Use IDS/IPS to detect downgrades.
- **Use Valid HTTPS Certs**: Avoid self-signed certs.
- **Educate Users**: Warn against bypassing HTTPS warnings.

--The End--