**Day 5**

**Exploitation Analyst**

**Hacking the SSL Network protocol:**

**SSL Stripping:**

**YouTube:**

1. [**https://youtu.be/99YNg8UAesI?si=EosGL3bARGJb8hdO**](https://youtu.be/99YNg8UAesI?si=EosGL3bARGJb8hdO)
2. [**https://youtu.be/\_Dnw1ZDVXz8?si=Bf11MdsUEba-WlqC**](https://youtu.be/_Dnw1ZDVXz8?si=Bf11MdsUEba-WlqC)

**How websites manage to connect HTTPS always?**

Websites manage HTTP to HTTPS redirection by issuing a 301/302 redirect from the server, using security headers like HSTS (HTTP Strict Transport Security) to force browsers to use HTTPS, and registering in browser preload lists to block any initial HTTP connection. Frameworks also offer middleware to enforce HTTPS by default.

**Is it true that websites always first try to connect to HTTP?**

Yes, in most cases, the first request from the browser is HTTP if the user types a URL without specifying https://. For example, entering example.com or www.example.com in the address bar typically defaults to:

http://example.com

However, this is only true if:

* The domain is not in the browser’s HSTS preload list, and
* The site has not been visited recently with an HSTS header already cached.

Once a site sends an HSTS header, or if it's preloaded, the browser automatically upgrades future HTTP attempts to HTTPS before making the request.

So:

* Yes, first-time visits to a non-HSTS site typically start as HTTP.
* No, if HSTS is already cached or preloaded, it goes directly to HTTPS.

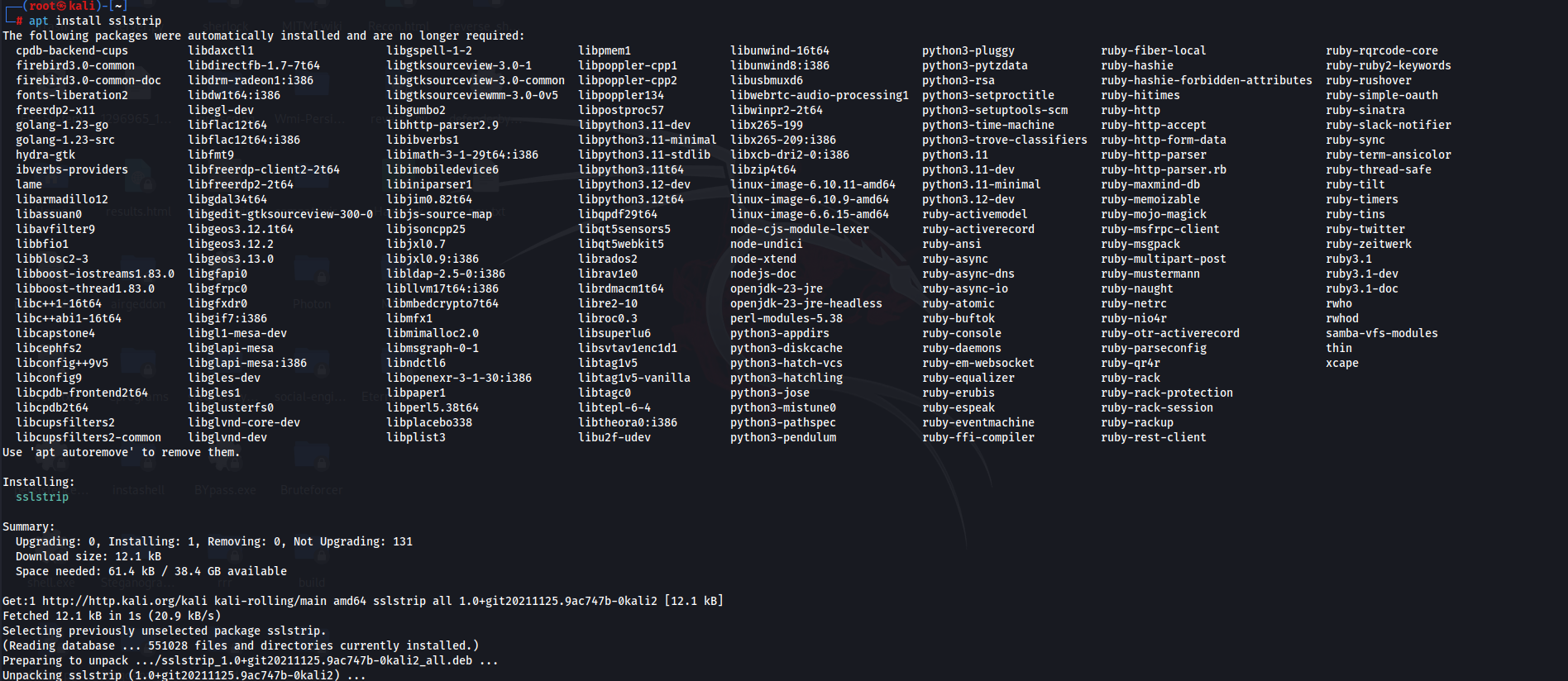
**How to perform SSL stripping:**

**What is SSL Stripping?**

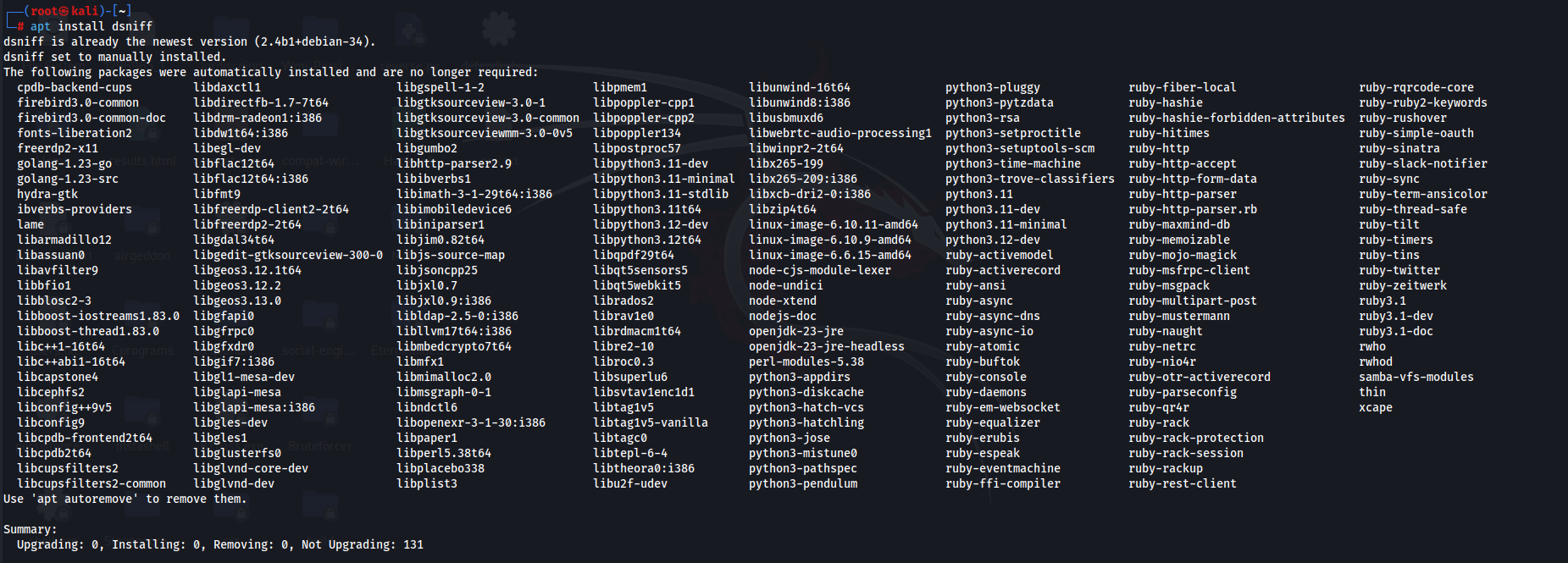
SSL stripping is a type of Man-in-the-Middle (MITM) attack where the attacker intercepts a user's HTTP request and prevents the automatic upgrade to HTTPS by downgrading the connection. Instead of forwarding the user’s request securely over HTTPS, the attacker serves the site over unencrypted HTTP, allowing them to capture sensitive data like login credentials in plain text. This attack exploits the fact that many users or browsers initially connect to websites via HTTP before being redirected to HTTPS.

Steps:

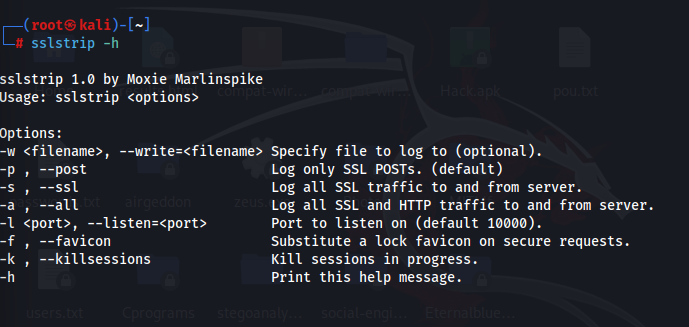
Install ssl strip:

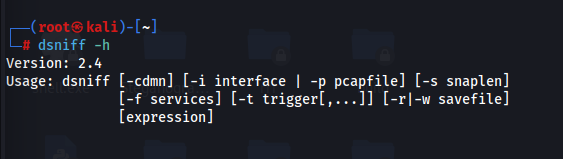


Then install dsniff:

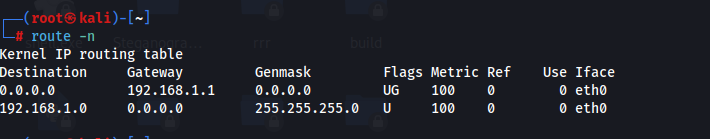


Check if they are properly installed:





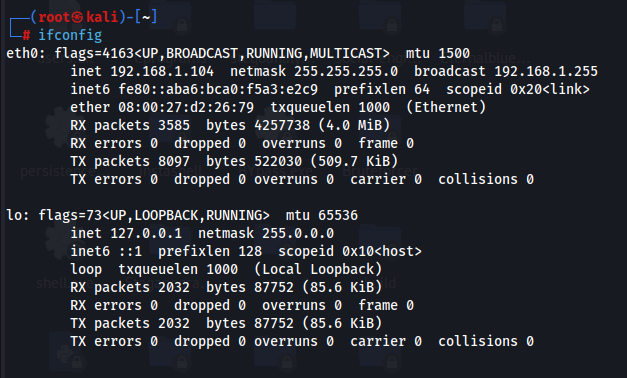
To get the IP address of router use this command: IP of router is 192.168.1.1



Now, to get the IP address of all the devices here on the router: nmap -sS -O 192.168.1.1/24

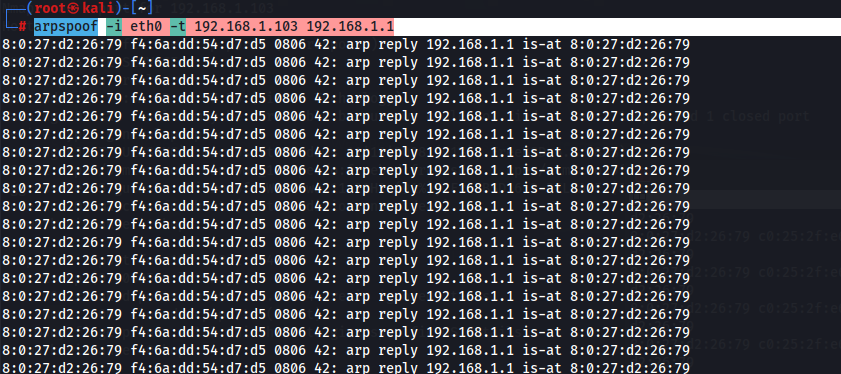


Then we will note our own IP address: it is 192.168.1.104

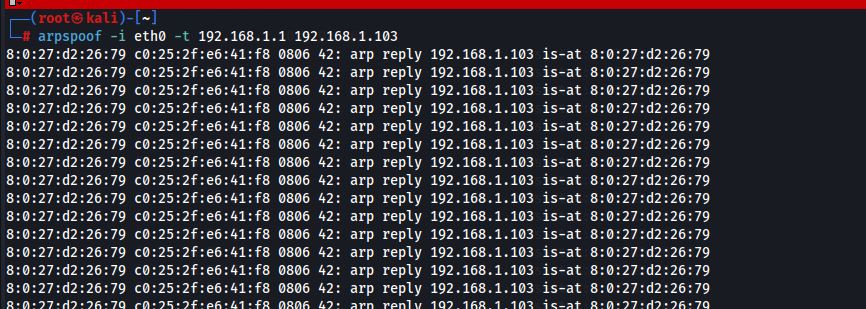


Now, we will open the new terminal window and start out MITM attack: This will tell the target machine that our kali machine is the router.

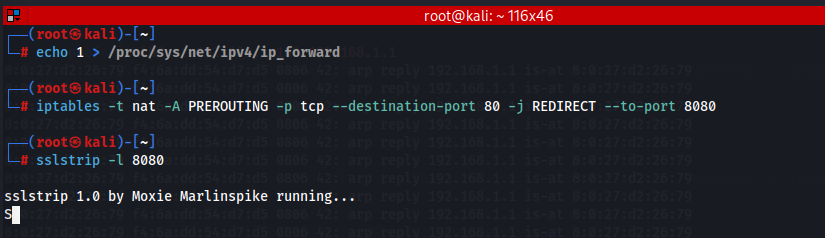
<taget-ip> <router-ip>



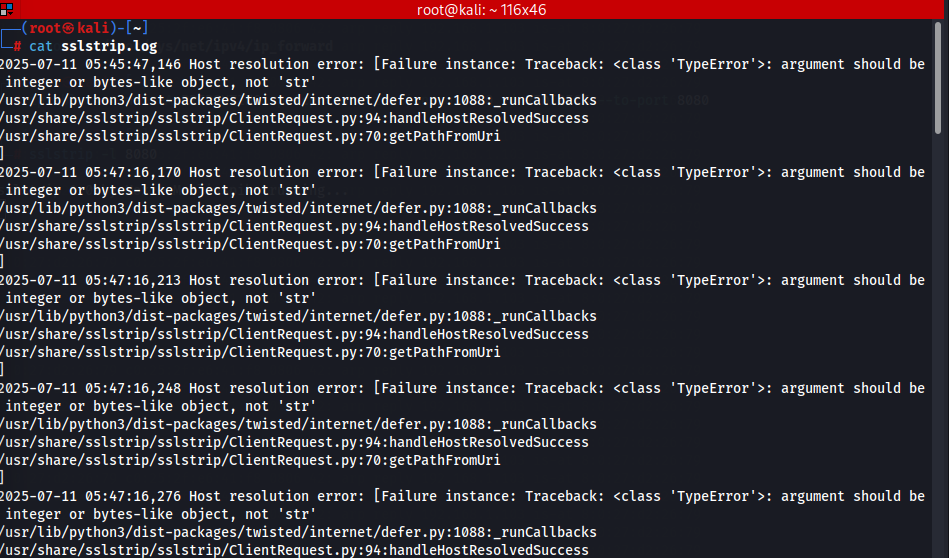
In new terminal swap these ips:

Now, we are in the middle of this network. But still we are not done yet.

Now, open a new terminal and do:



To get the credentials use the sslstrip.log: but since python 2 is downgraded. It will not work.



**To defend against SSL Stripping:**

* Implement HTTP Strict Transport Security (HSTS) to force browsers to use HTTPS only.
* Register your domain in the HSTS preload list to protect even first-time visitors.
* Use 301/302 redirects from HTTP to HTTPS at the server level as a backup.
* Educate users to manually type https:// when visiting websites.
* Use browser extensions like HTTPS Everywhere to auto-upgrade HTTP to HTTPS.
* Avoid using untrusted public Wi-Fi networks without a VPN, as they are common MITM attack points.

--The End--