

sslstrip

sslstrip is a MITM tool that implements Moxie Marlinspike's SSL stripping attacks.

It requires Python 2.5 or newer, along with the 'twisted' python module.

Installing:

- Unpack: `tar zxvf sslstrip-0.5.tar.gz`
- Install twisted: `sudo apt-get install python-twisted-web`
- (Optionally) run 'python setup.py install' as root to install, or you can just run it out of the directory.

Running:

sslstrip can be run from the source base without installation. Just run 'python sslstrip.py -h' as a non-root user to get the command-line options.

[crayon-6a9d66de19096469838635/]

More Info:

<http://www.thoughtcrime.org/software/sslstrip/>

```
Shell - Start VNC Server
ettercap  etterfilter  etterlog
bt sslstrip-0.2 # sn
snice      snmpconf      snmpinform      snmpptest      snmpwalk
sniff.py    snmpd              snmpkey          snmptranslate  snort
sniffer.py  snmpdelta          snmpnetstat     snmptrap       snortsam
snmpbulkget snmpdf              snmpset          snmptrapd
snmpbulkwalk snmpget            snmpstatus       snmpusm
snmpcheck   snmpgetnext        snmpstable       snmpvacm
bt sslstrip-0.2 # tcpdump -l -n tcp -A -s 128
tcpdump: WARNING: wifi0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wifi0, link-type IEEE802_11 (802.11), capture size 128 bytes

0 packets captured
0 packets received by filter
0 packets dropped by kernel
bt sslstrip-0.2 # tcpdump -l -n tcp -A -s 128
tcpdump: WARNING: wifi0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wifi0, link-type IEEE802_11 (802.11), capture size 128 bytes

0 packets captured
0 packets received by filter
0 packets dropped by kernel
bt sslstrip-0.2 # python sslstrip.py -w hola2q.txt
```

```
Shell - Konsole <2>
^C received, shutting down se
bt sslstrip-0.2 # eth
etherape ethtool
bt sslstrip-0.2 # ett
ettercap  etterfilter  ett
bt sslstrip-0.2 # sn
snice      snmpconf      snmpinform      snmpptest      snmpwalk
sniff.py    snmpd              snmpkey          snmptranslate  snort
sniffer.py  snmpdelta          snmpnetstat     snmptrap       snortsam
snmpbulkget snmpdf              snmpset          snmptrapd
snmpbulkwalk snmpget            snmpstatus       snmpusm
snmpcheck   snmpgetnext        snmpstable       snmpvacm
bt sslstrip-0.2 # tcpdump -l
tcpdump: WARNING: wifi0: no I
tcpdump: verbose output suppl
listening on wifi0, link-type

0 packets captured
0 packets received by filter
0 packets dropped by kernel
bt sslstrip-0.2 # tcpdump -l
tcpdump: WARNING: wifi0: no I
tcpdump: verbose output suppl
listening on wifi0, link-type

[4]+ Killed
bt ~ # arpspoof -i ath0 192.168.1.1
17964 ?      00:00:00 knotify
18007 ?      00:00:00 sshd
18115 pts/2  00:00:00 man
18118 pts/2  00:00:00 sh
18119 pts/2  00:00:00 sh
18124 pts/2  00:00:00 less
18414 pts/2  00:00:00 man
18417 pts/2  00:00:00 sh
18418 pts/2  00:00:00 sh
18428 pts/2  00:00:00 less
18430 pts/2  00:00:00 man
18433 pts/2  00:00:00 sh
18434 pts/2  00:00:00 sh
18444 pts/2  00:00:00 less
18686 ?      00:00:00 scsi_eh_14
18687 ?      00:00:00 usb-storage
18729 ?      00:00:00 hald-addon-stor
19335 ?      00:00:01 konqueror
19380 ?      00:00:00 kio_file
19522 ?      00:00:02 kwrite
19852 ?      00:00:02 kwrite
19889 pts/3  00:00:00 tcpdump
19891 pts/2  00:00:00 ps
bt ~ # arpspoof -i ath0 192.168.1.133
```