

Hijacking Web 2.0 Sites with SSLstrip

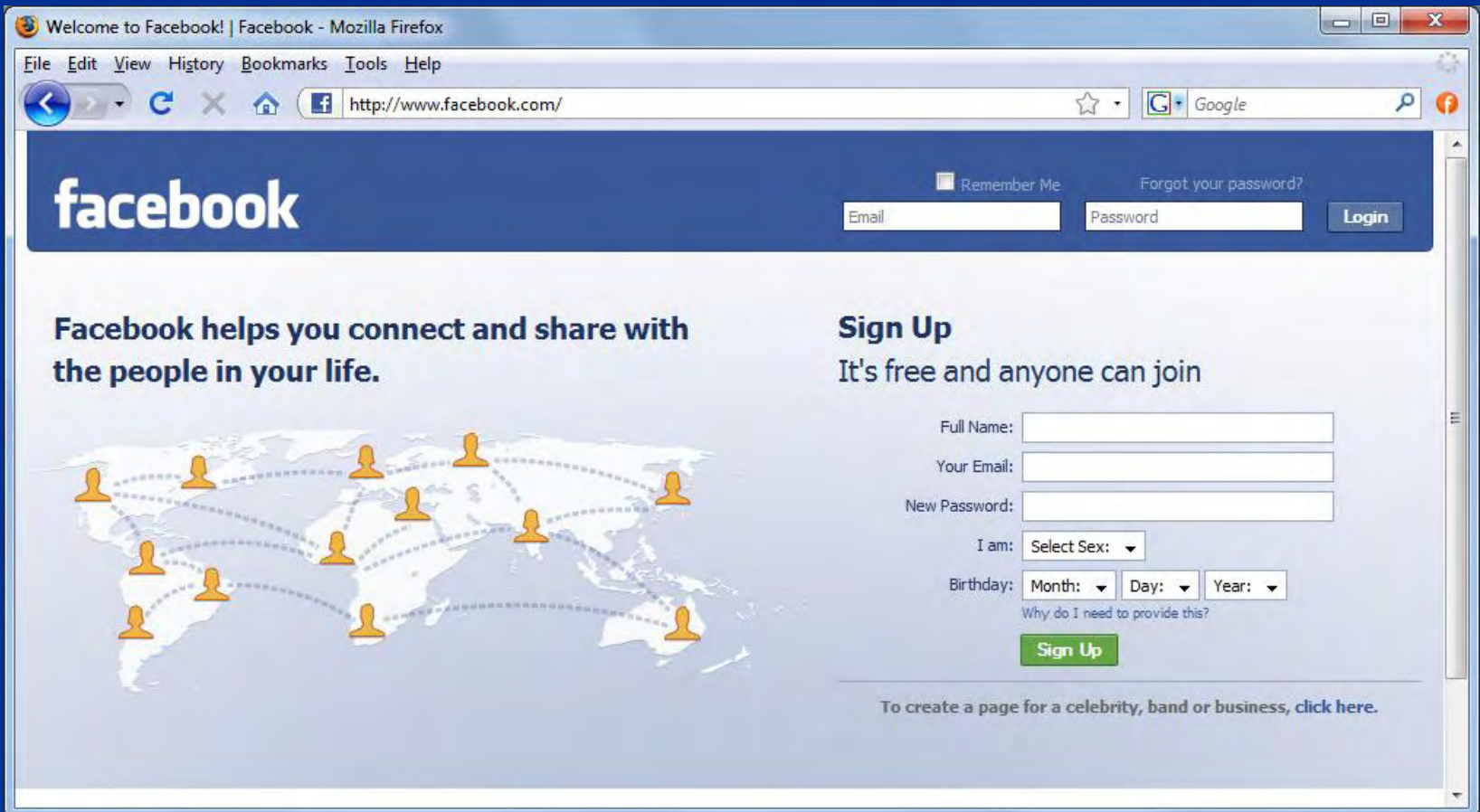
Hands-on Training

Contact

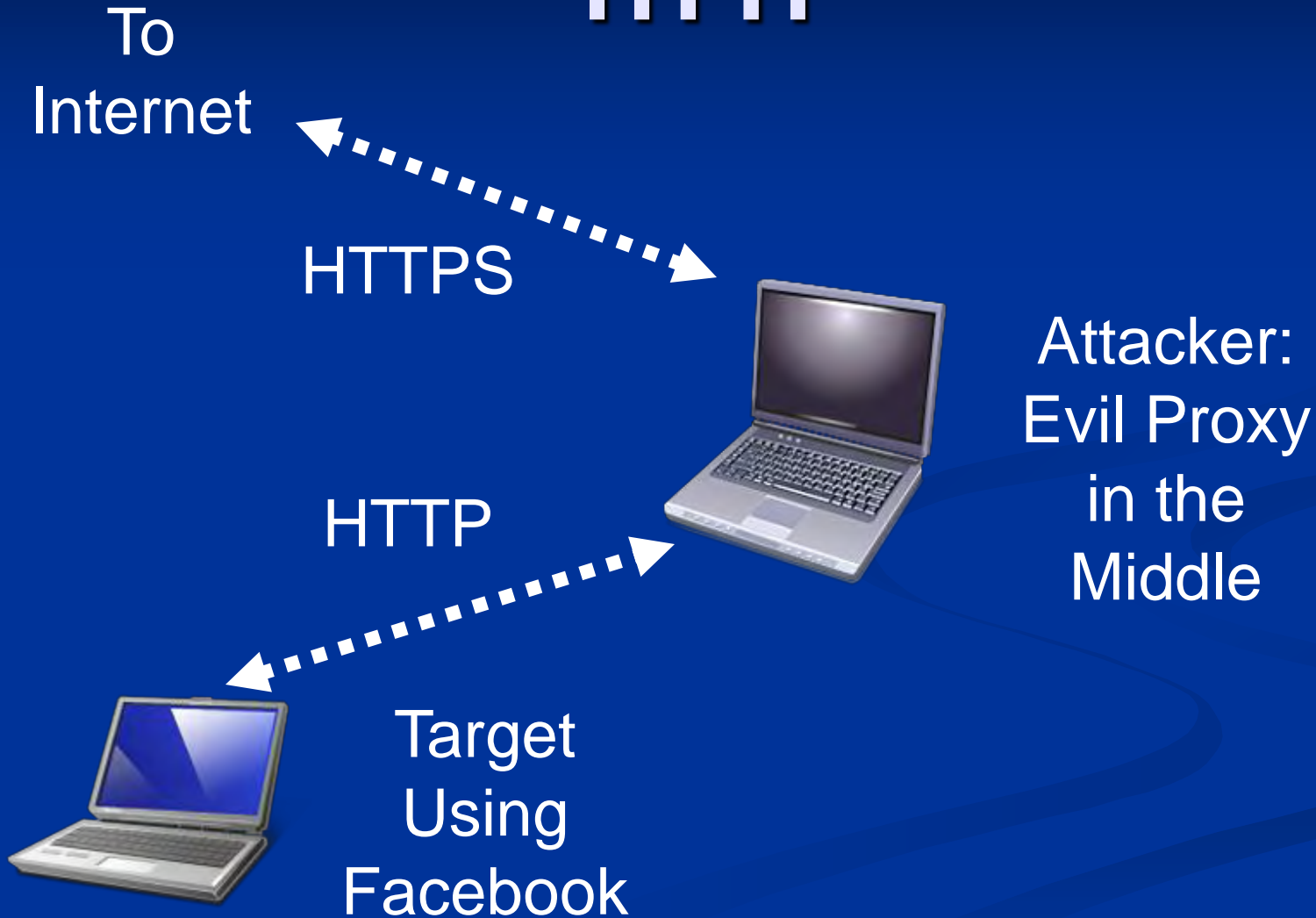
- Sam Bowne
- Computer Networking and Information Technology
- City College San Francisco
- Email: sbowne@ccsf.edu
- Web: samsclass.info

The Problem

- HTTP Page with an HTTPS Logon Button



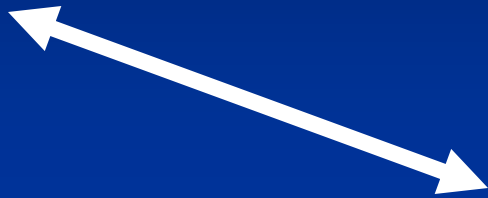
Proxy Changes HTTPS to HTTP



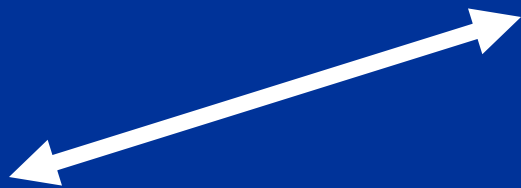
Ways to Get in the Middle

Physical Insertion in a Wired Network

To
Internet

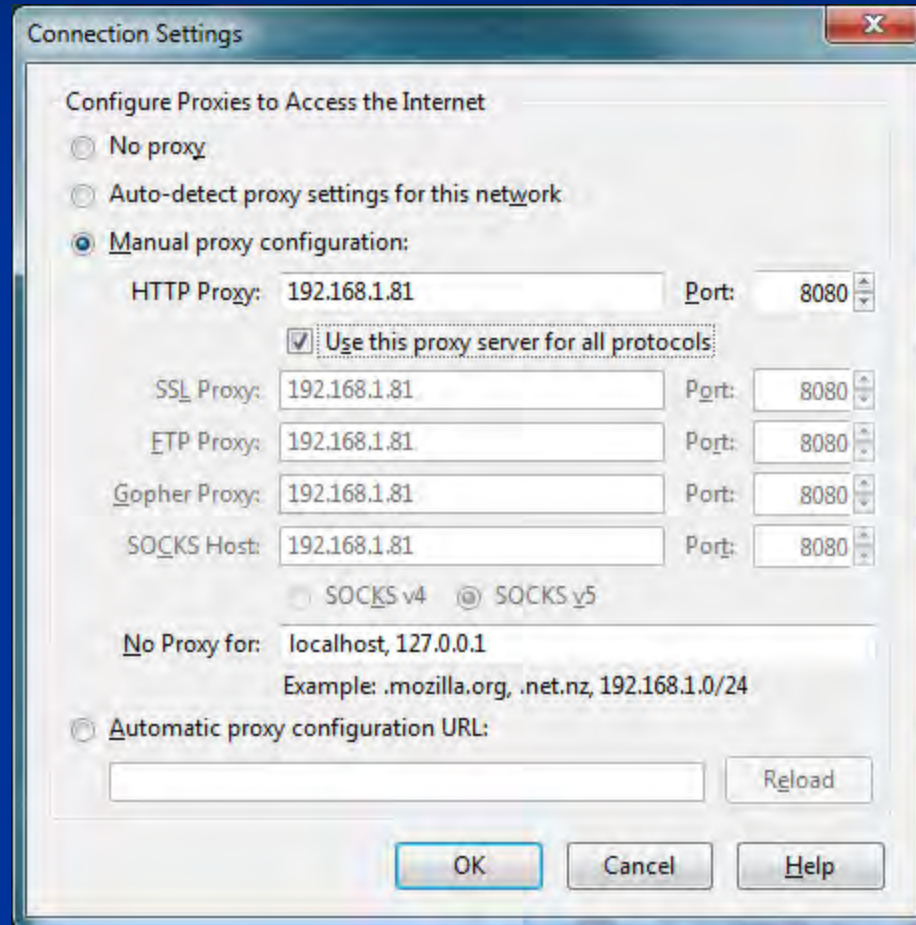


Attacker



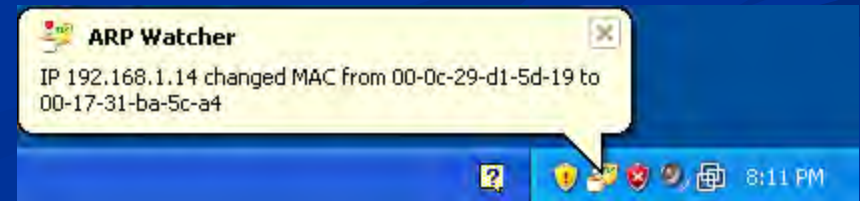
Target

Configuring Proxy Server in the Browser



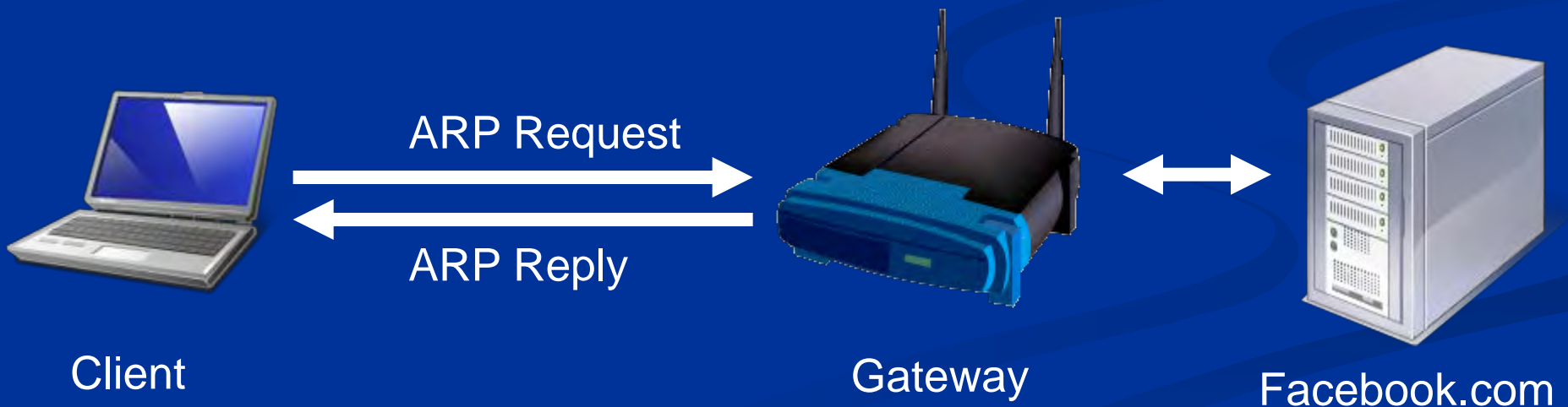
ARP Poisoning

- Redirects Traffic at Layer 2
- Sends a lot of false ARP packets on the LAN
- Can be easily detected
- DeCaffienateID by IronGeek
 - <http://k78.sl.pt>



ARP Request and Reply

- Client wants to find Gateway
- ARP Request: Who has 192.168.2.1?
- ARP Reply:
 - MAC: 00-30-bd-02-ed-7b has 192.168.2.1



ARP Poisoning



Demonstration

The screenshot displays a VMware Workstation interface with two windows open:

- Terminal Window:** Shows a shell prompt `student@student-desktop: ~/Desktop/sslstrip-0.2$`. The user has executed `tail -n 20 -f cap1 | grep pass`, which has captured a log entry from a Facebook login attempt. The log entry includes a timestamp, a security level (SECURE), and a POST request to `login.facebook.com`. The request body contains a `charset_test` parameter with a complex Unicode string and a `password` parameter.
- Firefox Browser Window:** Shows the Facebook homepage. The address bar contains `http://www.facebook.com/home.php?`. The page title is "Welcome to Facebook, Cnit." and the navigation bar includes "Home", "Profile", "Friends", and "Inbox 1".

The terminal output shows the following log entry:

```
2009-06-04 15:06:15,816 POST Data (www.facebook.com): charset_test=%E2%82AC%2C%2B4%2CE2%82AC%2C%2B4%2CE6%B0%B4%2CD0%94%2CD0%84&locale=en_US&email=cnit.target%40gmail.com&pass=P%40ssw0rd&pass_placeholder>Password&charset_test=%E2%82AC%2C%2B4%2CE2%82AC%2C%2B4%2CE6%B0%B4%2CD0%94%2CD0%84
```

Do it Yourself

- You need a laptop with
 - Windows host OS
 - VMware Player or Workstation
 - Linux Virtual Machine (available on the USB Hard Drives in the room)
- Follow the Handout