Hijacking Web 2.0 Sites with SSLstrip

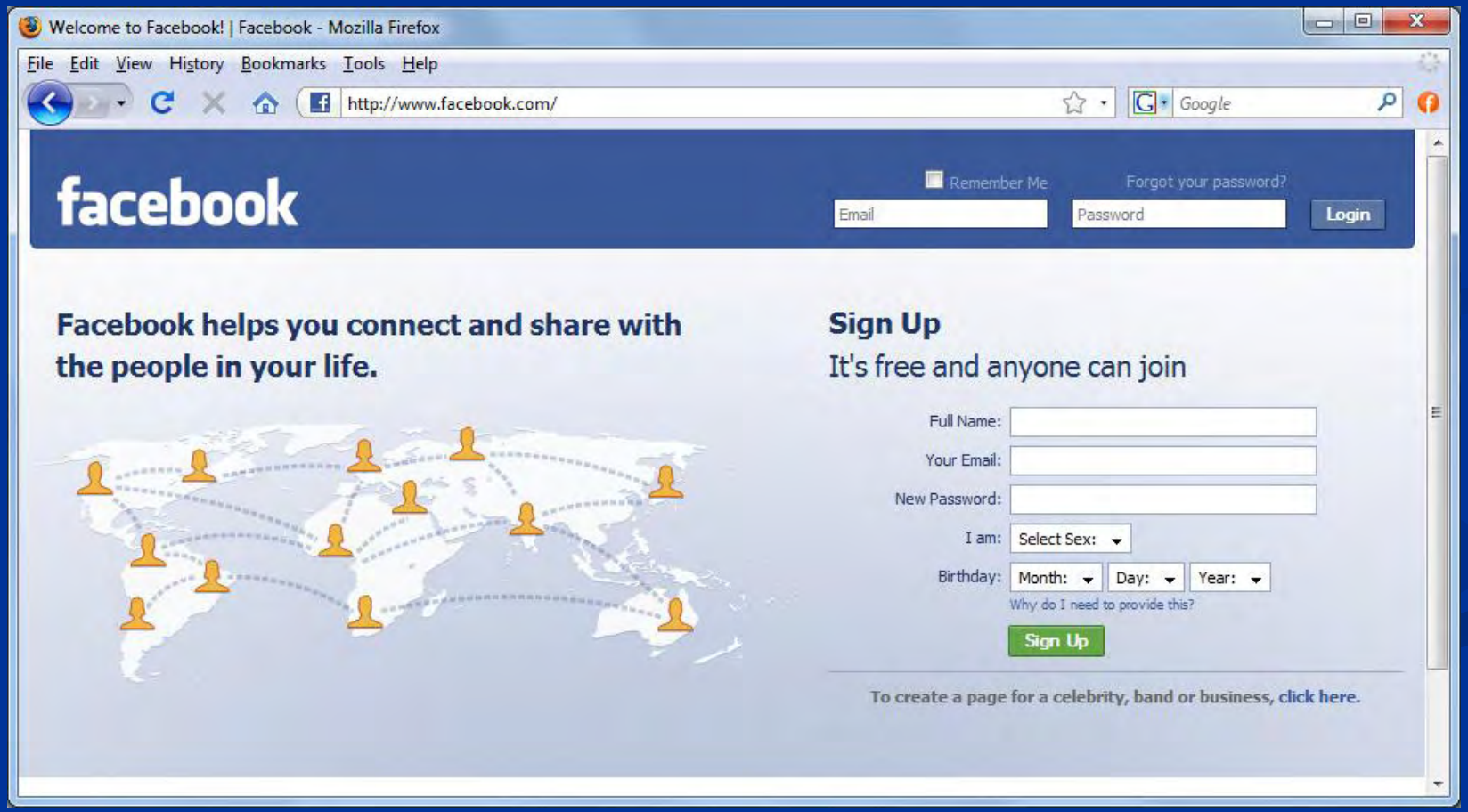
Hands-on Training

Contact

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

The Problem

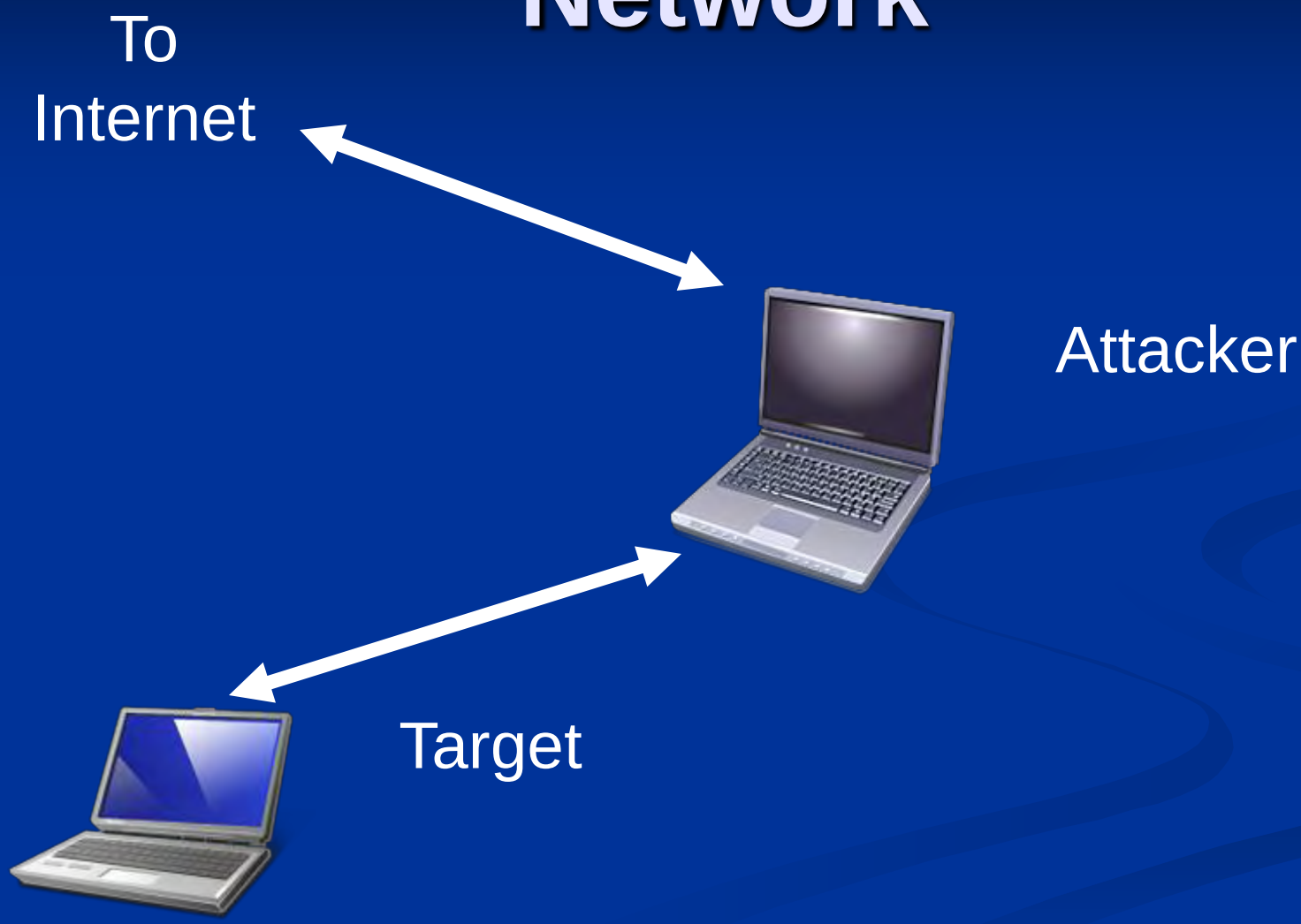
- HTTP Page with an HTTPS Logon Button



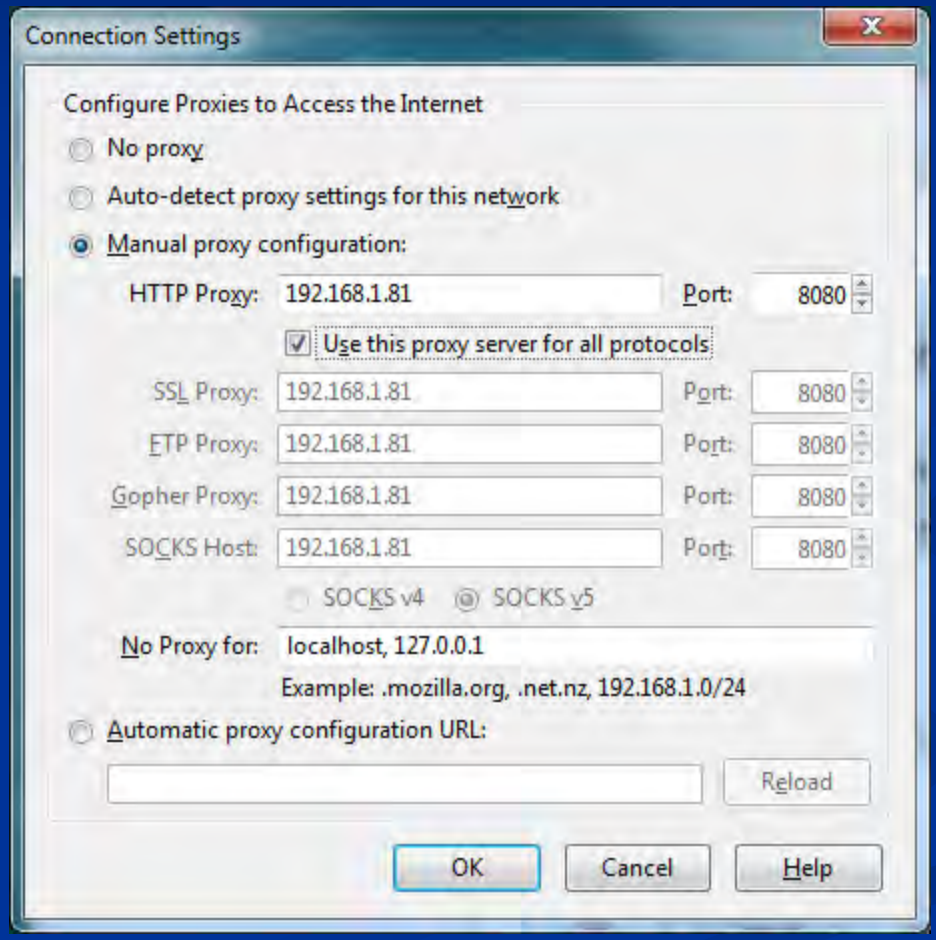
Proxy Changes HTTPS to HTTP

Ways to Get in the Middle

Physical Insertion in a Wired Network

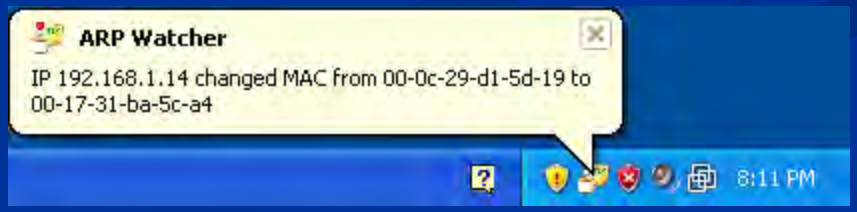


Configuring Proxy Server in the Browser



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

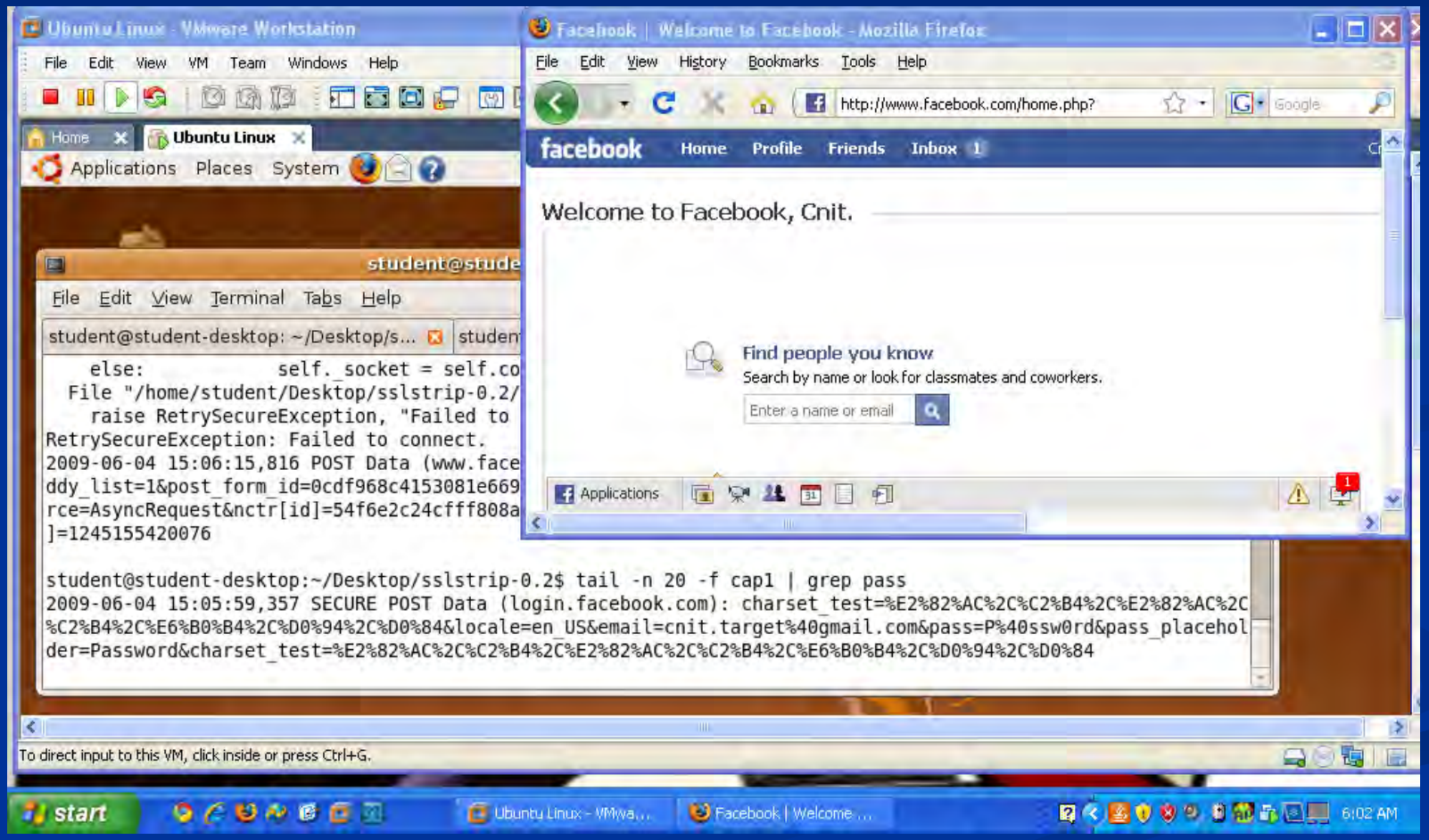


ARP Request and Reply

- 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



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