Bypassing Authenticated Wireless Networks
Introduction to Authenticated Networks

- An authenticated wireless network is a network which requires a username and password to go online.
- They are increasingly common, although the same security flaws exist now that existed when the technology first became available.
NoCatAuth

- NoCatAuth is an open source wireless authentication system written in perl.
- Widely used
  - Schools
  - Coffee shops
  - Restaurants
  - Community Networks
Login Process

- DHCP
- HTTP requests are redirected to and SSL encrypted login page.
- Once authenticated, the firewall sets a rule that allows data from your IP and MAC address to pass through the gateway.
Bypassing Authentication

- Basically, all that you need to do to bypass the firewall rules is spoof the information of someone who is already authenticated.
- Three things need to be known
  - MAC of target
  - IP of target
  - Location of the gateway
How the pickupline Works

- Creates a database
  - Gateway information
  - Target information
- Creates a thread in the background that sniffs for possible targets and attempts to identify the gateway.
- Once you have some targets, you can try spoofing them with the “spoof” command.
- If the spoofing is successful, you should be able to go on the internet as if you were authenticated.
How to Use the Tool

- **start**
  - starts the background thread that gathers target information etc

- **list**
  - lists all targets gathered

- **spoof**
  - lets you select a target to spoof

- **exit**
  - exits the program
Demonstration