

Técnicas Avanzadas de Ataque Un Enfoque Práctico



Luis Alejandro Ruiz
Giovanni Cruz

DECLARACIÓN

Todos los conceptos y demostraciones realizadas en esta presentación son para **uso educativo exclusivamente**, Digiware o los miembros de Digisert no se hacen responsables por el uso que se le de a los conceptos emitidos en esta presentación y es responsabilidad de cada usuario las consecuencias que pueda acarrear el uso de estos conocimientos.



Rogue AP - Introducción

- ✓ Hotspot – Es un sitio o lugar publico en el cual se ofrece una conexión a Internet por medio de una red inalámbrica
- ✓ Wireless Internet Service Provider (WISP) – Compañía o operadora que ofrece los servicio de Internet en un hotspot

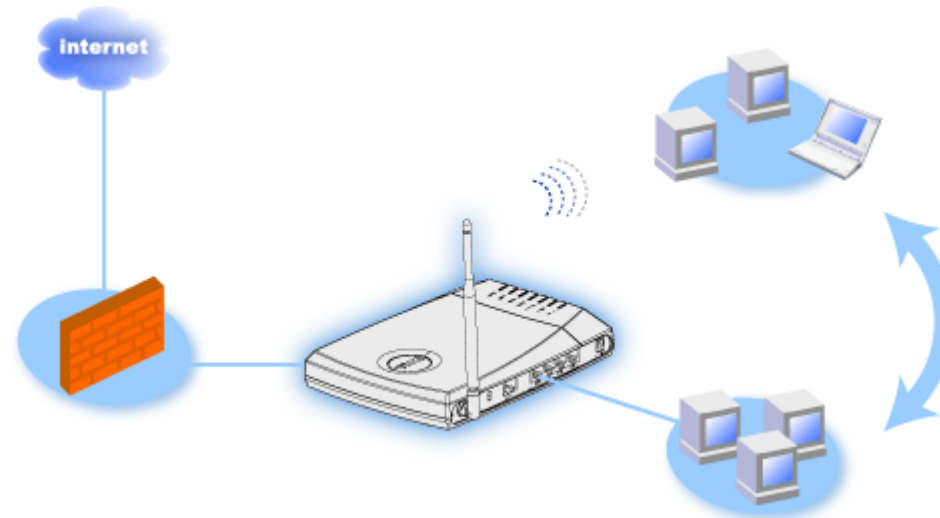
Rogue AP - Seguridad

- ✓ Eavesdropping
- ✓ WEP – Captura de paquetes y ataque estadístico
- ✓ WPA – Robo de paquetes de handshake y ataque de fuerza bruta o diccionario
- ✓ DoS
- ✓ Asociación a Redes Ad – Hoc
- ✓ Man In The Middle
- ✓ Rogue AP



Rogue AP - Acceso

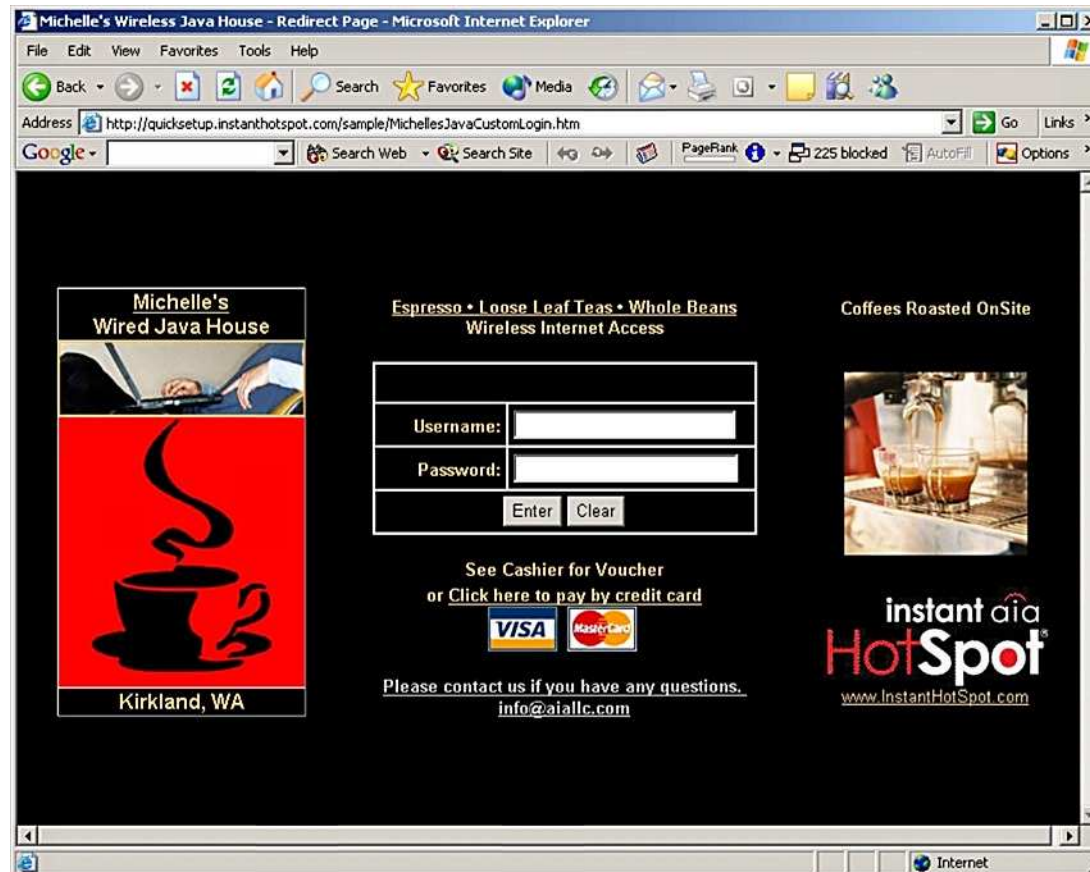
- ✓ Access Point Controller





Rogue AP - Acceso

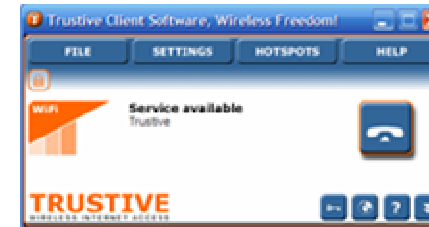
- ✓ Portal Cautivo





Rogue AP – Acceso

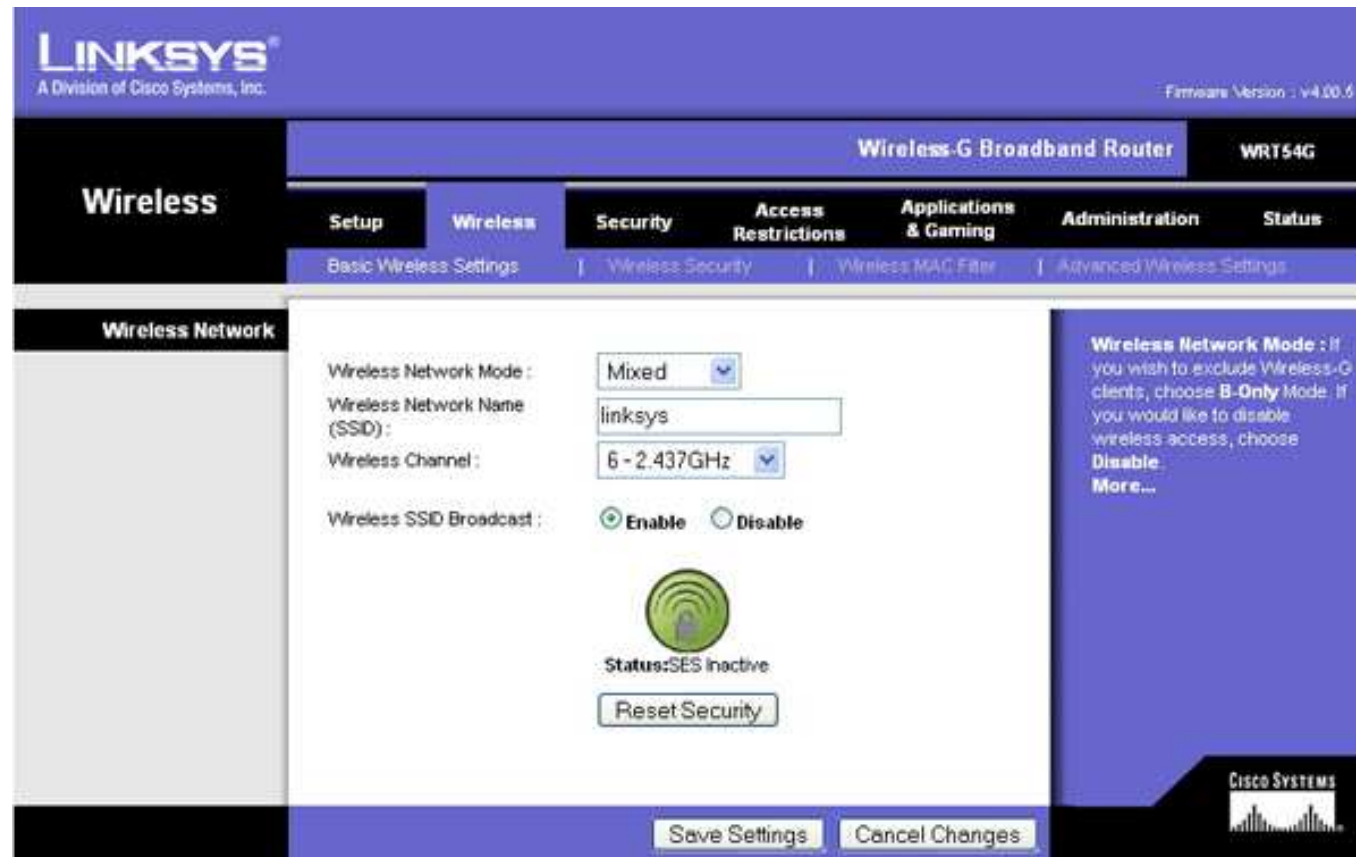
- ✓ Portal Cautivo con Agente de Acceso





Rogue AP - Ataque

- ✓ Actualización del Firmware





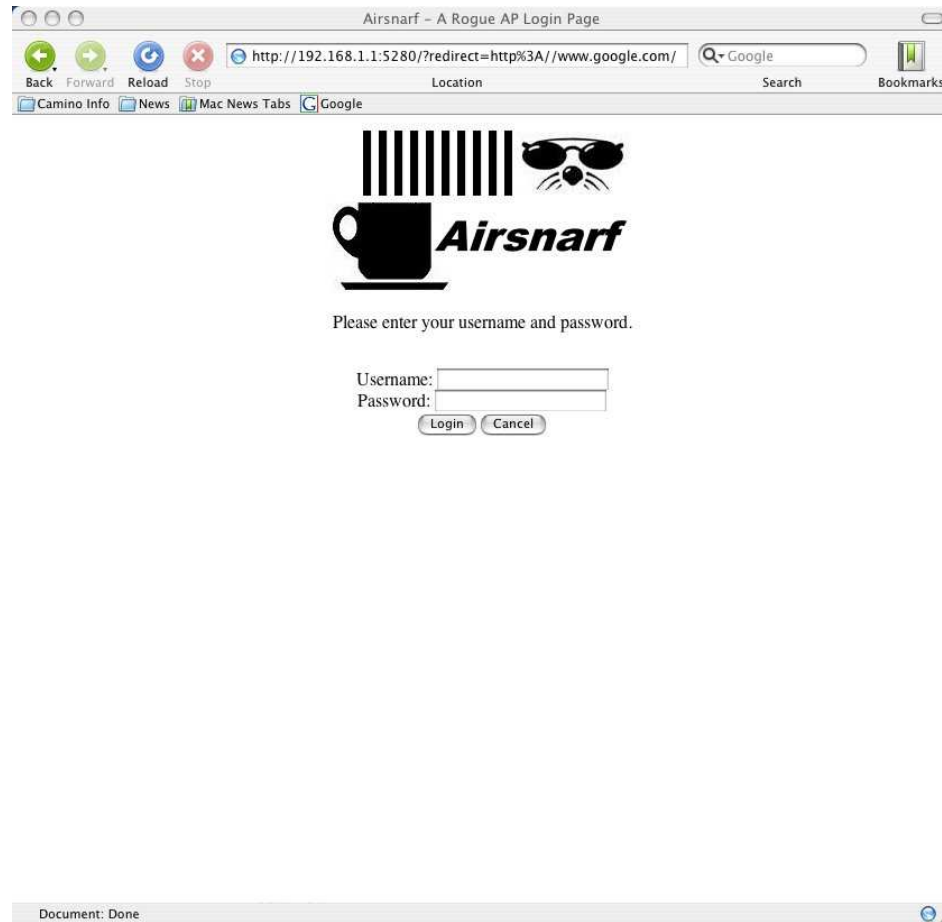
Rogue AP - Ataque

The screenshot shows the web interface of a WRT54G router. The browser address bar shows `http://192.168.1.1/`. The page title is "Setup" and the firmware version is "Rogue Squadron 0.1". The main navigation menu includes "Setup", "Wireless", "Security", "Access Restrictions", "Applications & Gaming", "Administration", and "Status". The "Setup" menu is expanded to show "Basic Setup", "DDNS", "MAC Address Clone", and "Advanced Routing". The "Internet Setup" section is active, showing "Automatic Configuration - DHCP" selected. The "Router IP" section is also visible, showing "Local IP Address" set to 192.168.1.1, "Subnet Mask" set to 255.255.255.0, and "Gateway" set to 0.0.0.0. The "DHCP Server" section is also visible, showing "DHCP Server" set to "Enable", "Starting IP Address" set to 192.168.1.100, "Maximum Number of DHCP Users" set to 50, and "Client Lease Time" set to 0 minutes. The "Static DNS" section is also visible, showing three static DNS addresses set to 0.0.0.0. The "Automatic Configuration - DHCP" section includes fields for "Router Name" (WRT54G), "Host Name", "Domain Name", "MTU" (Auto), and "Size" (1500). The "Automatic Configuration - DHCP" section also includes a "DHCP Server" section with "Starting IP Address" (192.168.1.100), "Maximum Number of DHCP Users" (50), and "Client Lease Time" (0 minutes). The "Automatic Configuration - DHCP" section also includes a "Time Setting" section with "Time Setting" (0 minutes) and "Time Setting" (0 minutes).



Rogue AP - Ataque

- ✓ Cambio del Portal Cautivo





Rogue AP - Ataque

Welcome to Qorvus1!

Search News Weather stock charts Trading Online Banking Misc MarketWatch Yahoo! Finance AccessLine MGA

Welcome to Qorvus1

Login:

Password:

Login

Click below to login in as a guest.

Guest Login

For technical support please contact system administrator.

Host Node Name: QORVUS1
Outside Internet Connection: Active
Operating Mode: Gateway Node

Qnode™ Wireless Access Points Manufactured By:

Qorvus Systems, Inc.
Vancouver, WA 98664
(360) 243-7371
<http://www.qorvus.net/>



Rogue AP - Ataque

✓ Asociación

Access Point



SSID: "goodguy"

AP más cercano o
con más potencia



SSID: "badguy"



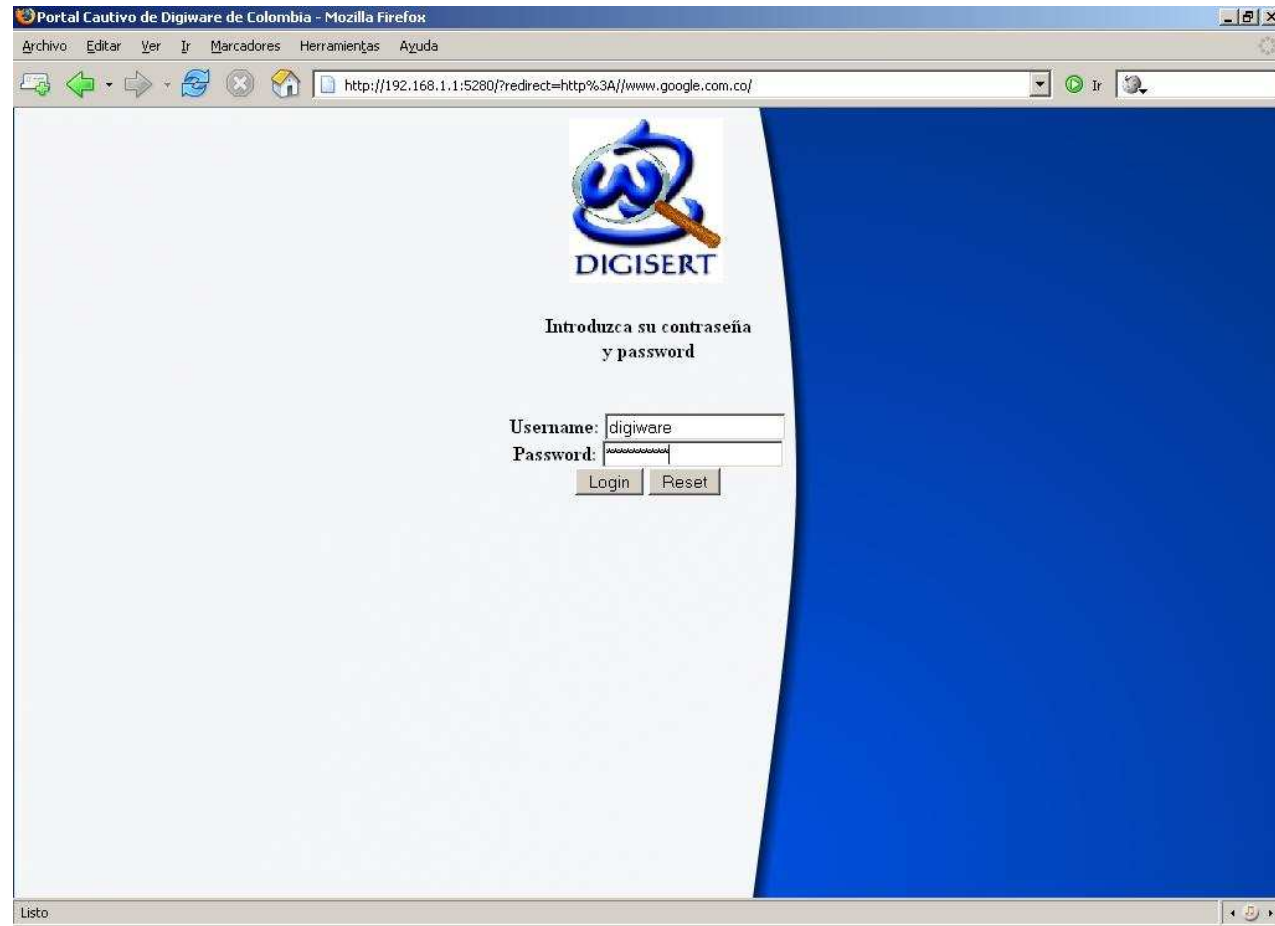
Wi-Fi Card

SSID: "goodguy"



Rogue AP - Ataque

✓ Autenticación





Rogue AP - Ataque

```
192.168.1.1 - PuTTY  
  
username=digiware password=passworddw accept_terms=yes redirect=http://www.googl  
e.com.co/ mode_login>Login  
airsnarf /opt# vi airdsnarfs.txt
```



Rogue AP - Amenazas

- ✓ Robo de credenciales e información
- ✓ Espionaje corporativo
- ✓ Back Door Corporativo
- ✓ DoS
- ✓ Clonación de AP



Bibliografía

- ✓ <http://airsnarf.shmoo.com>
- ✓ <http://www.wrt54g.net/>
- ✓ <https://www.wirelessve.org/entries/show/WVE-2005-0023>
- ✓ <http://hostap.epitest.fi/>
- ✓ <http://www.hotspotlist.com/>



Preguntas



Luis Alejandro Ruiz
e-mail: aruiz@digiware.com.co

Giovanni Cruz
e-mail: gcruz@digiware.com.co

PBX: 57(1) 6232474
www.digiware.com.co
digisert@digiware.com.co

GRACIAS

