

Nick: Cygog
 Milw0rm member: 1808
 Email: Cygog@live.com.ar

 Este es un manual que he diseñado y redactado 100% por mí, espero que ustedes sepan valorar el esfuerzo y el tiempo que he dado al escribir este manual para que llegue a sus manos y así puedan saciar un poco la sed de la sabiduría. Generalmente los usuarios que están leyendo este manual, son usuarios de foros referidos totalmente al mundo del hacking, la tan preciada palabra que todos hayan como criminal, no será tocada en este artículo, ya que no me considero ni mucho menos un "hacker". Espero que sea de su agrado este manual y si poseen dudas no duden en contactarme.



El ordenador no es una máquina inteligente que ayuda a gente estúpida, de hecho, es una estúpida máquina que funciona sólo en manos de gente inteligente.

Cygog@live.com.ar



Wi-Fi, asegurando nuestra red.



- Presentación. Pag.1
- Índice. Pag.2
- Objetivos. Pag.3
- Conceptos Básicos. Pag.4
- Cambiando contraseñas por defecto. Pag.5 y 6
- Encriptado nuestra red. Pag.6 y 7
- El ssid y broadcasting. Pag.8
- Activar el filtrado de MAC'S. Pag.9, 10 y 11
- Adiós y hasta la próxima. Pag.12

"El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada y rodeada por guardias armados"

-Gene Spafford-

Se preguntaran que hace tux vestido de esa manera.. (Quiere asesinar a windows).. (Objetivos).

En esta parte del manual le diré cual es el objetivo principal:

-Proteger lo más posible una red Wi-Fi.

Digo lo más posible ya que nada es 100% seguro, solo se puede mejorar el sistema de seguridad, que protege dicho sistema.

Debe quedarle en claro que no existe un sistema 100% seguro, sino que siempre existirá una falla, y allí nosotros estaremos para encontrarla y arreglarla. Un individuo (atacante), podrá elegir luego de realizar las comprobaciones en un sistemas informático, para luego atacar y así poder vulnerar ese sistema. En cuestion, en redes wi-fi, un atacante podría usar un sniffer y así poder interceptar paquetes y robar información importante sobre la persona o sistema a vulnerar. También si dicho atacante tiene conocimientos básicos, podría ingresar en nuestra red wi-fi, ya que generalmente, usan backtrack (linux) o el wiflasx y otras herramientas para el uso de cracking wap como por ejemplo: AiroPeek, AirSnort, AirMagnet o WEPcrack. Estas herramientas son usadas ya que el protocolo 802.11 implementa encriptación WEP. Bueno, por ese motivo hay que tener en cuenta las siguientes cuestiones que aprenderemos a lo largo del manual. Les enseñare a:



- 1-Cambiar la contraseña por defecto.
- 2-Usar encriptación wep/wpa.
- 3-Cambiar el SSID por defecto.
- 4-Desactivar el broadcasting SSID.
- 5-Activar el filtrado de direcciones MAC
- 6-Establecer el numero de conexiones máximas que puedan conectarse a nuestra red.
- 7-Desactivar DHCP
- 8-Desconectar el AP, cuando no lo uses.
- 9-Cambiar las claves wep regularmente.

Wi-fi es uno de los estándares de redes inalámbricas que se ha adoptado irremplazable, y ha corrido a toda su competencia sin darle ningún espacio a ninguna otra, desde celulares, palms, pcs, etc. incorporan compatibilidades con este tipo de red. En realidad, no hablare mucho sobre los conceptos que deben tener en cuenta en este tutorial ya que intentare hablar con un vocablo no específico, para que así toda persona ya sea novata o experta lo pueda entender. Lo único que creo si sería conveniente escribir en esta parte del manual es una breve descripción sobre la red wi-fi, cabe destacar que no se podría hacer un manual de wi-fi en una o dos páginas, por ese motivo, si no tienen ningún conocimiento sobre redes wi-fi podrían buscar información o consultar en mis otros manuales, siempre es bueno seguir buscando información para que luego ustedes mismos puedan generar su verdad.

Una de las mejores definiciones que he leído fue en la wikipedia: "Wi-Fi es un sistema de envío de datos sobre redes computacionales que utiliza ondas de radio en lugar de cables, además es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11."

El estándar IEEE 802.11 o Wi-Fi de IEEE que define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana. Si desean saber más sobre el modelo de referencia OSI (Open System Interconnection) pueden descargarse mi manual en donde explico este modelo de forma detallada.

Bueno, creo que ya entendiendo esto, se podría intentar a esta altura empezar con las prácticas de obtención de una red wifi segura.

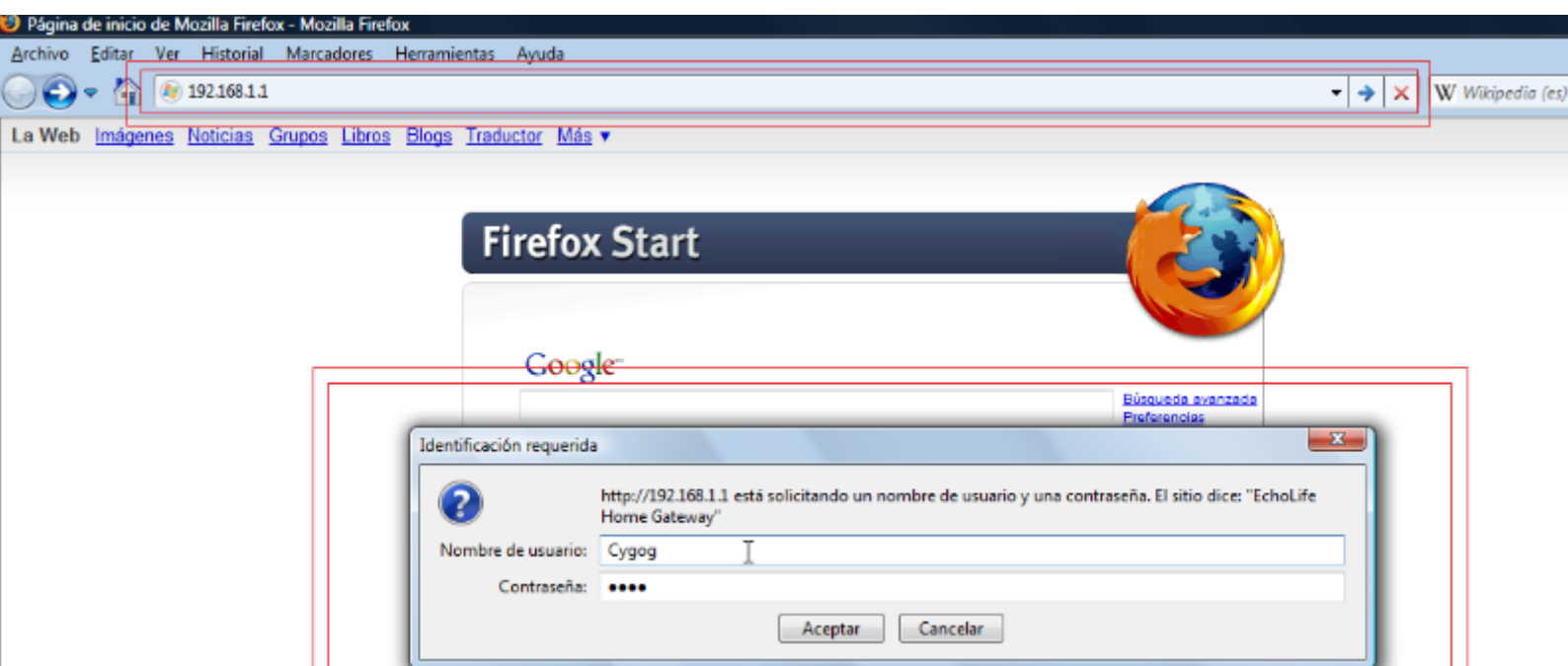
Bueno, lo primero que debemos tener en cuenta, es tener bien asegurado nuestro router. ¿Qué pasaría si una persona malintencionada, coge el router y lo tira contra una pared con todas sus fuerzas? Se rompería. ¿Qué pasaría si esta persona tiene un ordenador y desea romper la conexión wi-fi? Intentaría acceder al router para desconfigurarlo. Para ingresar al router generalmente estos vienen con contraseñas por defecto, una vez dentro modificaría lo que querría...

User: admin	User: admin	User:admin
Pass: admin	Pass:1111	Pass:1234

Ahora les enseñare a ingresar al router desde el navegador web desde windows, para luego cambiar la contraseña de nuestro router y así obtener un poco más de seguridad para nuestra red wi-fi.

1-Abrimos nuestro navegador y en la url pondremos 192.168.1.0 o 192.168.1.1 (generalmente es la 1.1) si desean averíguala pueden verla usando el comando ipconfig o winipcfg.


Veremos que el router nos pide usuario y contraseña:



2- Una vez dentro del router (accedimos a el por el navegador) buscaremos la opción que nos dará la posibilidad de cambiar la contraseña por defecto del router:

Achieving Together

System Management

Username	Privilege	Action(s)
admin	Administrator	
Notice: Click New to creat a new user account.		
<input type="button" value="New"/>		
Username	admin	
Privilege	Administrator	
Old Password	<input type="text"/>	
New Password	<input type="text"/>	
Retype to confirm	<input type="text"/>	
<input type="button" value="Submit"/>		

Esta tabla de formularios de mi router que me da privilegios para que podamos crear usuarios y cambiar contraseñas, para así poder restringir users alrededor de nuestra red que puedan acceder a las configuraciones de nuestro router.

"Comentar el código es como limpiar el cuarto de baño; nadie quiere hacerlo, pero el resultado es siempre una experiencia más agradable para uno mismo y sus invitados"

Ryan Campbell

Nacio wi-fi y agarrado de la mano aparecio wep y luego wpa/2. WEP (“Privacidad Equivalente a Cableado” o “Wired Equivalent Privacy” en inglés, aunque mucha gente lo confunde con “Wireless Encryption Protocol”.) es un protocolo que se invento para redes wireless que no dio un resultado esperado, un detalle a destacar es que 4 años antes de que este protocolo se creara ya habia sido vulnerado... ya que este protocolo usa el algoritmo RC4. Duro poco, unos años más tarde se creo WPA (Wi-Fi Protected Access) como solucion de errores que tenia el protocolo WEP pero hoy en día se sabe con claridad que tampoco es efectiva. En tan solo unos 2 minutos por relog se podria romper la seguridad que brinda WPA. Pero siempre es recomendable tenerla presente en nuestra red. Alrededor de 5/6 años atras, los routers no traian con sigo la encriptacion activada, ya que esto generaria que las personas pagen un extra a las empresas proveedoras de internet wireless para poder usarla.. (timadores), en fin, actualmente todas o casi todas, vienen por defecto con encriptación wpa activa, pero asegurarnos de esto, no estaria nada mal.. Para hacer esto, devemos ingresar al router desde el navegador (como lo hemos echo anteriormente) y buscar alguna opcion que nos permita ver las diferentes variantes que podremos elegir para que nuestra red no este expuesta sin un algoritmo que la proteja.. En mi caso este es el panel que veo:

The screenshot displays the configuration interface for a Huawei EchoLife HG520s router. The left sidebar shows a navigation menu with 'Basic' expanded and 'WAN Setting' selected. The main content area is titled 'WAN Setting' and contains several sections: 'PVC' (with fields for PVC, VPI, VCI, Active, Mode, Encapsulation, and Multiplex), 'Login Information' (with fields for Service Name, Username, and Password), 'IP Address' (with radio buttons for 'Obtain an IP Address Automatically' and 'Static IP Address', and fields for IP Address, Subnet Mask, and Gateway), 'Connection' (with radio buttons for 'Connect on Demand: Max Idle Timeout', 'Nailed-Up Connection', and 'Connect Manually'), and 'TCP MSS Option' (with a field for TCP MSS).

PVC	
PVC	0
VPI	8
VCI	35
Active	Yes
Mode	Routing
Encapsulation	PPPoE
Multiplex	LLC

Login Information	
Service Name	[Redacted]
Username	[Redacted]
Password	*****

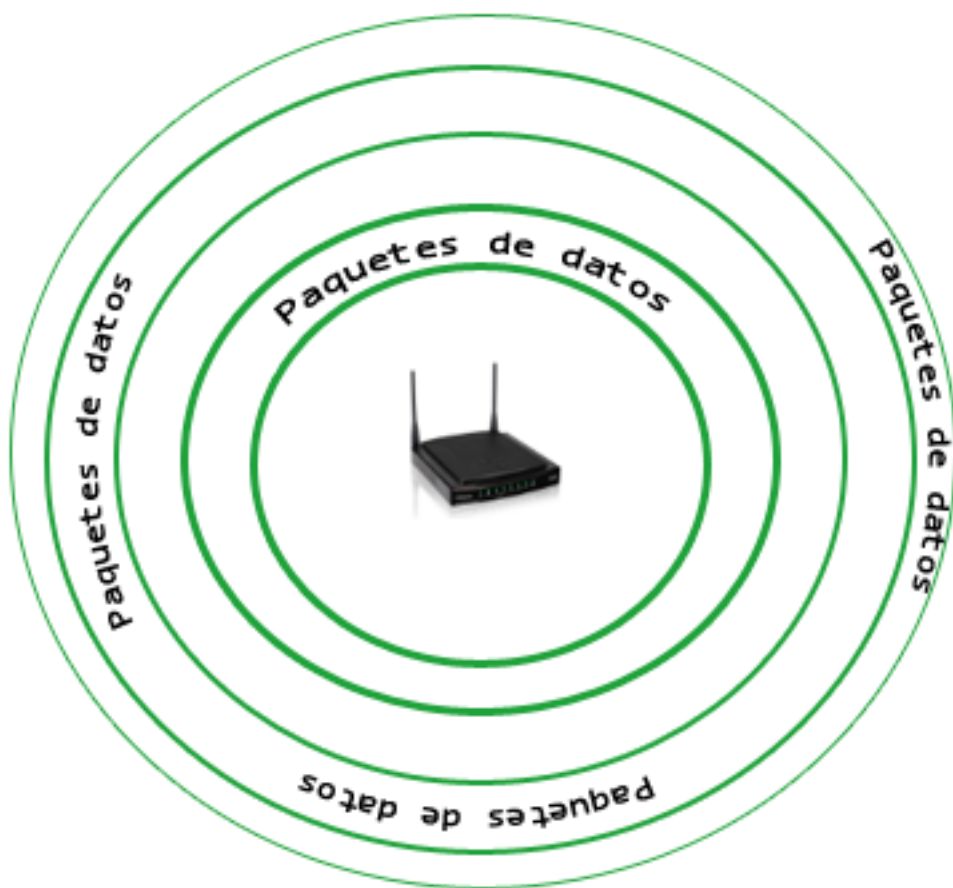
IP Address	
Default Route	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input checked="" type="radio"/> Obtain an IP Address Automatically	<input type="radio"/> Static IP Address
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0

Connection	
<input type="radio"/> Connect on Demand: Max Idle Timeout	0 Minutes
<input checked="" type="radio"/> Nailed-Up Connection	
<input type="radio"/> Connect Manually	

TCP MSS Option	
TCP MSS(0 means use default)	1400 bytes

La configuración más adecuada para wep/wpa es un nivel de encriptación de 128bits.

Bueno, espero que sepan ubicarce y encontrar esta opcion dentro del router. Ante cualquier duda, siempre deven consultar en la empresa proveedora de internet, ya sea via web o manteniendo una comunicacion telefonica.



"Programar sin una arquitectura o diseño en mente es como explorar una gruta sólo con una linterna: no sabes dónde estás, dónde has estado ni hacia dónde vas"

Danny Thorpe

Voy a seguir la estructura que venia haciendo, esta vez les dare otra breve introducción sobre que es el SSID de una red wi-fi y como esconderla.

En realidad Service Set Identifier: identificador de conjunto de servicio (SSID) es un código que se emiten en todos los paquetes que se envian por el router, para identificar nuestra red. Generalmente vienen por defecto los nombres de los routers o empresa proveedora de internet. Lo recomendable es ponerle un nombre que nos permita pasar desapercivido, nombres como “desconectado”, “erronea” etc.. Esto generara que la persona malintencionada no le llame la atención nuestra red y no intente ingresar. Es recomendable tambien desactivar el broadcasting.

Para cambiarla devemos ingresar nuevamente al router, y buscar el panel que nos permita hacerlo. En mi caso:

Wireless Lan

Wireless Setting	
Access Point	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel ID	MEXICO Auto Channel Select Current Channel: 1
SSID Index	1
SSID	Desconectada
Broadcast SSID	<input type="radio"/> Yes <input checked="" type="radio"/> No
Authentication Type	WPA2-PSK

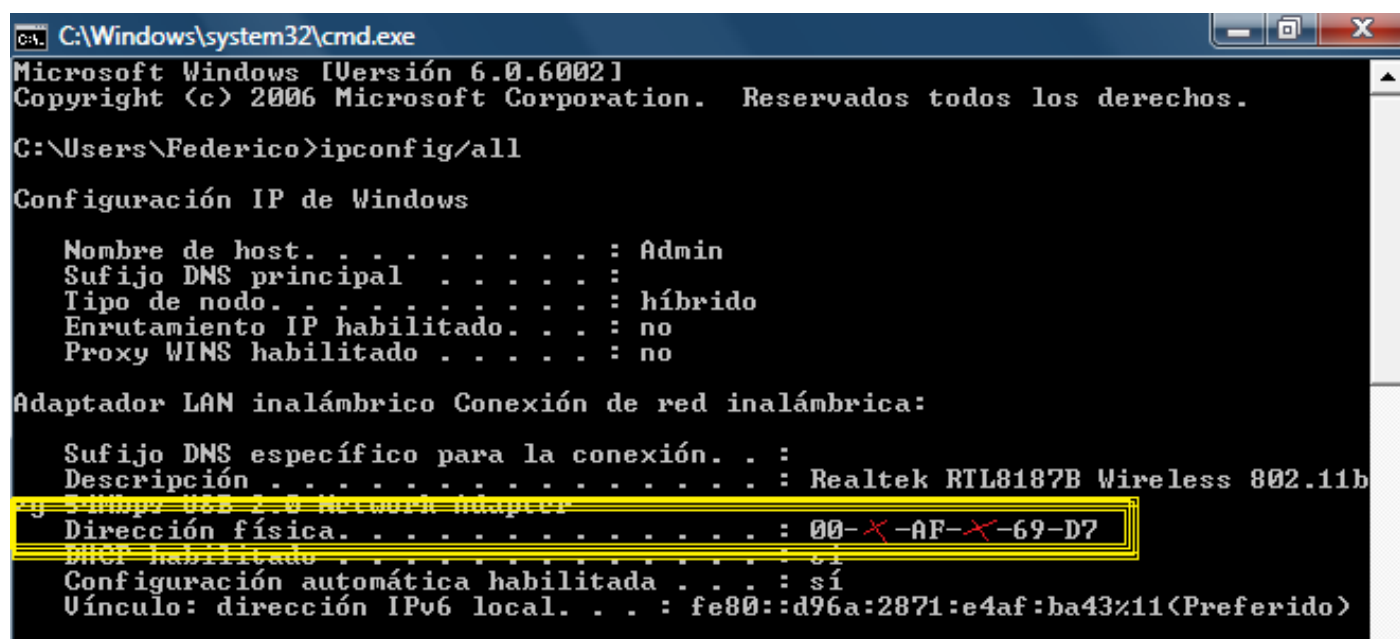
“Veo poco potencial comercial en Internet, al menos durante diez años”

Bill Gates, 1994

Dirección MAC? en si, esta dirección no es dinamica, cada vez que nos conectamos a internet, nuestra mac se registra, las mac se encuentran escritas dentro de los adaptadores de red, (llamadas direcciones físicas por ese motivo) y es por eso que es casi imposible cambiarla o suplantarla, generalmente las personas que suelen hacerlo son ingenieros en informatica, ya que ellos crean sus propias placas receptoras de redes wireless. Si vamos al caso, lo que quiero que aprendan en esta parte del manual es a filtrar mac's, esto significa que nuestra red tendra pcs predisponibles para la conexion. Cuando logramos filtrar las macs, solo las pcs que tengan dicha mac podran conectarse a nuestra red, logrando asi nuestro objetivo: lograr una mayor seguridad en nuestra red.

Antes que nada les voy a enseñar como saber nuestra dirección MAC:

Vamos a la consola de comandos y escribimos IPCONFIG/ALL veremos lo siguiente:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.0.6002.1]
Copyright (c) 2006 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Federico>ipconfig/all

Configuración IP de Windows

Nombre de host. . . . . : Admin
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador LAN inalámbrico Conexión de red inalámbrica:

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Realtek RTL8187B Wireless 802.11b
y g 54Mbps 802.11g Network Adapter
Dirección física. . . . . : 00-xx-af-xx-69-d7
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::d96a:2871:e4af:ba43%11<Preferido>
```

Sabremos al momento de realizar esto, cual es nuestra dirección MAC ya que tienen una forma muy peculiar:

00-xx-af-xx-69-d7

Bueno, ya sabiendo nuestra dirección MAC, seguiremos el siguiente paso que es el filtrar en nuestra red las direcciones MAC'S

En mi caso, mi router tiene una opción llamada "Wireless Lan" en la cual me da la posibilidad de filtrar las macs. Según el router que posean encontrarán esta opción:

Wireless MAC Address Filter	
Active	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Action	Allow Association ▼
#1	00:00:00:00:00:00
#2	00:00:00:00:00:00
#3	00:00:00:00:00:00
#4	00:00:00:00:00:00
#5	00:00:00:00:00:00
#6	00:00:00:00:00:00
#7	00:00:00:00:00:00
#8	00:00:00:00:00:00
<input type="button" value="Submit"/>	

Una vez puestas las macs su router solo dejara conectarse a estas determinadas pc's.

Bueno, hasta aquí, su red será segura, recuerden que ningún sistema informático es 100% seguro pero si se puede mejorar, uno de los pilares de la S.I (Seguridad Informática) es la autenticación en otro de mis manuales describo esto, este pilar es uno en el cual se está avanzando mucho en tecnologías wireless.

Si se quiere mejorar la seguridad, también aparte de lo que les he enseñado, podrán establecer números de conexiones máximas para su red, desactivar DHCP, desactivar el AP (punto de acceso) cuando no uses tu red, y cambiar las claves wep regularmente.



Espero que les haya gustado la primer parte de este manual, ya que en esta les enseñe a asegurar sus redes, en la próxima entrega, lo contrario de esta, les escribiré sobre el como hackear redes con tecnologías inalámbricas.

Como en todo manual, guía, tutorial o como le guste llamarlo, les doy mis saludos a:

Antrax (administrador de E-r00t, Argentina)

Neddih (administrador de hackxcrack, España)

Jaxer (Viejo amigo de Mexico)

Dreo (Viejo amigo de Argentina)

84kur10 (ayudante de enseñanza en foros, Undergroun)

nightwalker (Compañero de foro, Argentina)

Un Gran saludo y abrazo a todos ellos y a todos los que me han acompañado durante todos estos largos años en la gran red de redes. Atte Cygog

Cygog@live.com.ar